Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Karbantartás

Verzió 1.0

2024

Tartalomjegyzék

10.1. Szabályzat és eljárásrendek 4
10.2. Szabályozott karbantartás 7
10.3. Rendszeres karbantartás – Automatizált karbantartási tevékenységek 10
10.4. Karbantartási eszközök 12
10.5. Karbantartási eszközök – Eszközök vizsgálata 14
10.6. Karbantartási eszközök – Adathordozók vizsgálata 16
10.7. Karbantartási eszközök – Jogosulatlan elszállítás megakadályozása 18
10.8. Karbantartási eszközök – Korlátozott eszközhasználat 20
10.9. Karbantartási eszközök – Privilegizált jogosultsággal való futtatás 22
10.10. Karbantartási eszközök – Szoftverfrissítések és javítások 24
10.11. Távoli karbantartás 26
10.12. Távoli karbantartás – Naplózás és felülvizsgálat 29
10.13. Távoli karbantartás – Azonos szintű biztonság és adattörlés 31
10.14. Távoli karbantartás – Hitelesítés és a karbantartási munkaszakaszok szétválasztása 33
10.15. Távoli karbantartás – Jóváhagyások és értesítések 36
10.16. Távoli karbantartás – Kriptográfiai védelem 38
10.17. Távoli karbantartás – Kapcsolat megszakításának megerősítése 40
10.18. Karbantartó személyek 42
10.19. Karbantartó személyek – Nem megfelelő ellenőrzöttségű személyek 45
10.20. Karbantartó személyek – Nem rendszer karbantartás 47
10.21. Kellő időben történő karbantartás 49
10.22. Kellő időben történő karbantartás – Megelőző karbantartás 51
10.23. Kellő időben történő karbantartás – Prediktív karbantartás 53

10.24. Kellő időben történő karbantartás – Prediktív karbantartás automatizált támogatása 55
10.25. Terepi karbantartás szabályozása 57

10.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

10.1. A szervezet:

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

10.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó karbantartási szabályzatot, amely

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

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

10.1.1.2. A karbantartási eljárásrendet, amely a karbantartási szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

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

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

MAGYARÁZAT

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

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

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gondoskodnia kell a karbantartási szabályzat és eljárásrendek kidolgozásával, dokumentálásával, jóváhagyásával, kiadásával és megismertetésével kapcsolatos feladatok ellátásáról.
2. A szervezetnek meg kell bizonyosodnia arról, hogy a karbantartási 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 karbantartási 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 karbantartási 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

18.67. Információ kezelése és megőrzése

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

3.3.7.1. Rendszer karbantartási 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.5.37

NIST SP 800-53 REV.5 REFERENCIA

MA-1

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

10.2. SZABÁLYOZOTT KARBANTARTÁS

10.2. A szervezet:

10.2.1. Ütemezi, dokumentálja és felülvizsgálja a rendszerelemek karbantartásának, javításának és cseréjének nyilvántartásait a gyártó vagy szállító specifikációi és a szervezeti követelmények szerint.

10.2.2. Jóváhagyja és ellenőrzi az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik-e, és hogy a rendszert vagy a rendszerelemeket a helyszínen szervizelik-e, vagy más helyszínre szállítják.

10.2.3. Megköveteli, hogy a szervezet által meghatározott személyek vagy szerepkörök egyedileg jóváhagyják a rendszer vagy a rendszerelemek szervezeti létesítményekből történő elszállítását külső karbantartás, javítás vagy csere céljából.

10.2.4. Biztonságosan törli a szervezet által meghatározott besorolású információkat a hozzájuk kapcsolódó adathordozókról, mielőtt azokat a szervezeti létesítményeiből külső karbantartás, javítás vagy csere céljából elszállítanák.

10.2.5. Ellenőrzi a védelmi intézkedések megfelelő működését a karbantartás, javítás vagy csere után.

10.2.6. Rögzíti a szervezet által meghatározott információkat a szervezeti karbantartási nyilvántartásokba.

MAGYARÁZAT

A rendszeres karbantartás meghatározza az EIR karbantartási programját minden rendszerelem és minden karbantartási típus vonatkozásában függetlenül attól, hogy azt maga a szervezet vagy külső szolgáltató végzi (szerződéses, garanciális, házon belüli, szoftver-karbantartási megállapodás). A rendszer karbantartása magában foglalja azokat az elemeket is, amelyek nem vesznek közvetlenül részt az információfeldolgozásban és/vagy az adatok/információk megőrzésében, mint például a szkennerek, másolók és nyomtatók. Annak érdekében, hogy a karbantartási nyilvántartások hatékonyak legyenek, a jegyzőkönyveknek tartalmazniuk kell például a karbantartás dátumát és idejét, a karbantartást végző szervezet, valamint személyek nevét, amennyiben szükséges, úgy a felügyeletet biztosító kísérők nevét, a végrehajtott

karbantartás leírását és az eltávolított vagy kicserélt rendszerelemek, alkatrészek meghatározását, leírását.

Az EIR-ek biztonsági osztálya meghatározza a karbantartási bejegyzések részletességével kapcsolatos elvárásokat. A szervezetek figyelembe veszik az információs rendszerek tartalék alkatrészeinek beszerzésével kapcsolatos szempontokat is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet ütemezi, dokumentálja és felülvizsgálja a rendszerelemek karbantartásának, javításának és cseréjének nyilvántartásait a gyártó vagy szállító specifikációi és az érintett szervezet követelményei szerint.
2. A szervezetnek jóvá kell hagyja és ellenőriznie kell az összes karbantartási tevékenységet, függetlenül attól, hogy azt a helyszínen vagy távolról végzik-e, és hogy az EIR-t vagy a rendszerelemeket a helyszínen szervizelik-e, vagy más helyszínre szállítják.
3. A szervezetnek meg kell követelnie, hogy a meghatározott személyek vagy szerepkörök egyedileg jóváhagyják az EIR vagy a rendszerelemek szervezeti létesítményekből történő elszállítását külső karbantartás, javítás vagy csere céljából.
4. A szervezetnek gondoskodnia kell arról, hogy biztonságosan törli a meghatározott besorolású információkat a hozzájuk kapcsolódó adathordozókról, mielőtt azokat szervezet létesítményeiből külső karbantartás, javítás vagy csere céljából elszállítanák.
5. A szervezetnek ellenőriznie kell a biztonsági intézkedések megfelelő működését a karbantartás, javítás vagy csere után.
6. A szervezetnek biztosítania kell, hogy rögzíti a meghatározott információkat a karbantartási jegyzőkönyvekbe.
7. A szervezetnek a tulajdonában álló EIR-ek biztonsági osztálya alapján meg kell határoznia a karbantartási jegyzőkönyvek részletességével kapcsolatos elvárásokat.
8. A szervezet figyelembe veszi az információs rendszerek tartalék alkatrészeinek beszerzésével kapcsolatos szempontokat is.

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

10.11. Távoli karbantartás

11.8. Adathordozók törlése

12.42. Be- és kiszállítás

18.2. Hibajavítás

19.4. Ellátási láncra vonatkozó követelmények és folyamatok

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

3.3.7.2. Rendszeres karbantartás

ISO/IEC 27001:2023 REFERENCIA

A.7.10; A.7.13; A.8.10

NIST SP 800-53 REV.5 REFERENCIA

MA-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

10.3. Rendszeres karbantartás – Automatizált karbantartási tevékenységek

10.3.1. A szervezet automatizált mechanizmusokat alkalmaz a karbantartások és javítások ütemezésére, lefolytatására és dokumentálására.

10.3.2. Naprakész, pontos és teljes nyilvántartást vezet minden igényelt, ütemezett, folyamatban lévő és befejezett karbantartási és javítási tevékenységről.

Magyarázat

A szervezet:

automatizáltan megszervezi a karbantartások és javítások ütemezését, végrehajtását és dokumentálását; továbbá

(b) a megrendelt, ütemezett, folyamatban lévő és befejezett valamennyi karbantartásról és javításról naprakész, pontos és teljes nyilvántartást vezet.

A követelmény alkalmazásának lépései

1. A szervezetnek automatizált mechanizmusokat kell alkalmaznia, amelyek segítségével ütemezheti, elvégezheti és dokumentálhatja a karbantartási és javítási tevékenységeket az EIR-en.

2. A szervezetnek naprakész, pontos és teljes nyilvántartást kell vezetnie minden igényelt, ütemezett, folyamatban lévő és befejezett karbantartási és javítási tevékenységről. Ez magában foglalja az EIR-en végzett munka minden részletét, beleértve a munka típusát, az elvégzett munka időpontját, a munkát végző személyt vagy csapatot, és a munka eredményét.

3. A szervezetnek rendszeresen ellenőriznie kell a nyilvántartást, hogy biztosítsa annak naprakészségét és pontosságát. Ez magában foglalja a befejezett munka, illetve az ahhoz kapcsolódó dokumentáció ellenőrzését.

4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén módosítania kell frissítenie kell a karbantartási és javítási tevékenységekhez köthető automatizált mechanizmusokat annak érdekében, hogy biztosítsa az EIR folyamatos működését és biztonságát.

5. A szervezetnek biztosítania kell, hogy a karbantartási és javítási tevékenységek megfelelnek a kiberbiztonsági követelményeknek, és hogy ezek a tevékenységek nem veszélyeztetik az EIR biztonságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

10.4. Karbantartási eszközök

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

3.3.7.2. Rendszeres karbantartás

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

MA-2(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

10.4. KARBANTARTÁSI ESZKÖZÖK

10.4. A szervezet:

10.4.1. Jóváhagyja, nyilvántartásba veszi és ellenőrzi az EIR-hez kapcsolódó karbantartási eszközöket.

10.4.2. A nyilvántartásokat a szervezet az általa meghatározott időközönként felülvizsgálja.

MAGYARÁZAT

E követelménypont a szervezet információs rendszereinek karbantartása során használt vizsgálati és javítási eszközökkel kapcsolatos biztonsági problémákkal foglalkozik. A karbantartási eszközök lehetnek hardver, szoftver és firmware eszközök. A szervezet információs rendszereire nézve a karbantartási eszközök potenciális veszélyt jelentenek, mert ezen eszközökön keresztül kártékony kód kerülhet a rendszerekbe. A karbantartási eszközök lehetnek például hardver/szoftver diagnosztikai eszközök és hardver/szoftver hálózatfelügyeleti megoldások. Ez a követelménypont nem terjed ki olyan elemekre, melyek az információs rendszer szerves részét képezik, viszont a karbantartási munkát segíthetik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet jóváhagyja, nyilvántartásba veszi és ellenőrzi az EIR-hez kapcsolódó karbantartási eszközöket. Ez magában foglalja a hardver, szoftver és firmware eszközöket.
2. A szervezet gondoskodik a karbantartási eszközök jóváhagyásával kapcsolatos felelősségekről és annak dokumentálásáról.
3. A szervezet rendszeresen felülvizsgálja a karbantartási eszközöket. Ez lehetővé teszi az elavult, nem támogatott, irreleváns vagy már nem használt eszközök jóváhagyásának visszavonását és az ilyen típusú karbantartási eszközök kivezetését/selejtezését.
4. A szervezetnek figyelembe kell vennie, hogy a karbantartási eszközökön keresztül kártékony kódok juttathatók a szervezet EIR-jeibe.
5. A szervezetnek tudatában kell lennie annak, hogy a karbantartást támogató hardver- és szoftverelemek, amelyek az EIR részét képezik pl.: ping, ls, ipconfig, vagy az Ethernet switch monitorozó portját implementáló hardver és szoftver) nem tartoznak a karbantartási eszközök hatálya alá.

Kapcsolódó intézkedések

10.2. Szabályozott karbantartás

12.42. Be- és kiszállítás

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

3.3.7.3. Karbantartási eszközök

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

MA-3

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

10.5. KARBANTARTÁSI ESZKÖZÖK – ESZKÖZÖK VIZSGÁLATA

10.5. A szervezet ellenőrzi a karbantartó személyzet által használt eszközöket, a nem megfelelő, vagy nem engedélyezett módosítások észlelése érdekében.

MAGYARÁZAT

A karbantartó eszközöket a karbantartó személyzet közvetlenül behozhatja a létesítménybe, vagy letöltheti a gyártó weboldaláról. Ha a karbantartási eszközök ellenőrzése során a szervezetek megállapítják, hogy az eszközöket nem megfelelő módon módosították, vagy az eszközök rosszindulatú kódot tartalmaznak, a biztonsági eseményt a biztonsági események kezelésére vonatkozó szervezeti szabályzatokkal és eljárásrendekkel összhangban kezelik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy a karbantartó személyzet által használt eszközök ellenőrzése rutinszerűen megtörténjen. Ez magában foglalhatja a fizikai eszközök ellenőrzését, valamint a szoftvereszközök, például a karbantartási programok és alkalmazások ellenőrzését is.
2. A szervezetnek meg kell határoznia egy szabályt vagy irányelvet, amely meghatározza, milyen módosítások tekinthetők megfelelőnek az EIR-en. Ez magában foglalhatja a szoftverfrissítéseket, a hardvercseréket és más, a karbantartás során végrehajtott változtatásokat.
3. A szervezetnek implementálnia kell egy naplózási rendszert, amely nyomon követi az összes módosítást, amelyet a karbantartó személyzet végrehajt az EIR-en. Ez lehetővé teszi az érintett szervezet számára, hogy gyorsan észlelje a nem megfelelő vagy nem engedélyezett módosításokat.
4. Ha a naplózás során nem megfelelő vagy nem engedélyezett módosítást észlelnek, az érintett szervezetnek azonnal cselekednie kell. Ez magában foglalhatja a módosítás visszavonását, a karbantartó személyzet értesítését a problémáról, és szükség esetén a karbantartási protokollok felülvizsgálatát.

5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a karbantartási eszközök ellenőrzésének protokolljait, hogy biztosítsa azok hatékonyságát és naprakészségét az EIR aktuális állapotához képest.

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

MA-3(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

10.6. KARBANTARTÁSI ESZKÖZÖK – ADATHORDOZÓK VIZSGÁLATA

10.6. A szervezet az EIR-ben történő felhasználást megelőzően ellenőrizi a diagnosztikai és tesztprogramok adathordozóit, hogy tartalmaznak-e kártékony kódot.

MAGYARÁZAT

Ha a karbantartási- diagnosztikai- és tesztprogramokat tartalmazó adathordozók vizsgálata során megállapításra kerül, hogy valamely adathordozó kártékony kódot tartalmaz, a biztonsági esemény kezelése a szervezeti eseménykezelési szabályzatokkal és eljárásrendekkel összhangban történik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és be kell szereznie azokat a karbantartási- diagnosztikai- és tesztprogramokat, amelyeket az EIR vonatkozásában használni kíván.
2. A karbantartási- diagnosztikai- és tesztprogramokat tartalmazó adathordozókat az érintett szervezetnek alaposan meg kell vizsgálnia, annak érdekében, hogy található-e rajtuk kártékony kód.
3. Ha a vizsgálat során az érintett szervezet kártékony kódot talál az adathordozókon, azonnal el kell távolítania azt, és meg kell akadályoznia annak terjedését az EIR-ben. Ez biztonsági eseménynek minősül, melyet a szervezeti eseménykezelési szabályzatokkal és eljárásrendekkel összhangban kell kezelni.
4. A szervezetnek dokumentálnia kell minden ellenőrzést, beleértve annak eredményét is.
5. A szervezetnek rendszeresen frissítenie kell a kártékony kód ellenőrzésére használt eszközeit annak érdekében, hogy azok naprakészek legyenek és felismerjék a legújabb fenyegetéseket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

18.8. Kártékony kódok elleni védelem

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

3.3.7.3. Karbantartási eszközök

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

MA-3(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

10.7. KARBANTARTÁSI ESZKÖZÖK – JOGOSULATLAN ELSZÁLLÍTÁS MEGAKADÁLYOZÁSA

10.7. A szervezet megakadályozza a szervezeti információkat tartalmazó karbantartó eszközök elszállítását az alábbiak szerint:

10.7.1. Ellenőrzi, hogy a berendezésen van-e szervezeti információ.

10.7.2. Megsemmisíti a berendezést vagy biztonságosan törli annak tartalmát.

10.7.3. A berendezést a létesítményben tartja és megőrzi;

10.7.4. kivéve, ha a szervezet által meghatározott személyek vagy szerepkörök egyike kifejezetten engedélyezi a berendezésnek a létesítményből történő elszállítását.

MAGYARÁZAT

A szervezeti információk magukban foglalják az érintett szervezetek tulajdonában lévő összes információt, valamint minden olyan információt, amelyet az érintett szervezetek részére bocsátottak rendelkezésre és amelyeknek az érintett szervezetek az adatgazdái.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek a karbantartó eszközök elszállítását megelőzően ellenőriznie kell, hogy azok tartalmaznak-e szervezeti információt.
2. Ha az elszállítandó karbantartó eszköz tartalmaz szervezeti információt, az érintett szervezetnek meg kell semmisítenie az eszközt vagy biztonságosan törölnie kell annak tartalmát.
3. A szervezetnek a karbantartó eszközt a létesítményben kell tartania és meg kell őriznie, kivéve, ha a szervezet által meghatározott személyek vagy szerepkörök egyike kifejezetten engedélyezi a berendezésnek a létesítményből történő elszállítását.
4. A szervezetnek folyamatosan felül kell vizsgálnia és szükség esetén frissítenie kell a jogosulatlan elszállítással kapcsolatos szabályzatait és eljárásrendjeit annak érdekében, hogy biztosítsa az EIR és a benne tárolt információk biztonságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

11.8. Adathordozók törlése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.10

NIST SP 800-53 REV.5 REFERENCIA

MA-3(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

10.8. KARBANTARTÁSI ESZKÖZÖK – KORLÁTOZOTT ESZKÖZHASZNÁLAT

10.8. A szervezet a karbantartási eszközök használatát csak a megfelelő engedéllyel rendelkező személyek számára teszi lehetővé.

MAGYARÁZAT

A karbantartási eszközök használata csak a megfelelő engedéllyel rendelkező személyek számára engedélyezett. Ez a megkötés azokra a rendszerekre vonatkozik, melyek karbantartási funkciókat látnak el.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely személyek rendelkeznek a megfelelő engedéllyel a karbantartási eszközök használatához.
2. A szervezetnek létre kell hoznia egy szabályzatot, amely magában foglalja az engedélyezési folyamatot és a karbantartási eszközök használatának feltételeit.
3. A szervezetnek be kell vezetnie egy rendszert, amely képes ellenőrizni és nyomon követni, hogy ki használja a karbantartási eszközöket az egyes EIR-eken belül. Ez magában foglalhatja a felhasználói hitelesítést és a naplózást.
4. A szervezetnek rendszeresen ellenőriznie kell a naplókat, hogy megbizonyosodjon a karbantartási eszközök megfelelő használatáról és azonnal cselekednie kell, ha szabálytalanságot észlel.
5. A szervezetnek biztosítania kell a karbantartási eszközök megfelelő tárolását és kezelését annak érdekében, hogy megakadályozza az illetéktelen hozzáférést.
6. A szervezetnek rendszeresen képeznie kell a személyzetet a karbantartási eszközök megfelelő használatával és a kiberbiztonsági előírásokkal összefüggésben.
7. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a szabályzatokat és az ahhoz kapcsolódó eljárásrendeket, annak érdekében, hogy hatékonyak és naprakészek legyenek.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

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

MA-3(4)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

10.9. Karbantartási eszközök – Privilegizált jogosultsággal való futtatás

10.9. A szervezet monitorozza a privilegizált jogosultsággal futtatott karbantartási eszközök használatát.

Magyarázat

A privilegizált jogosultsággal futtatott karbantartó eszközök jogosulatlan hozzáférést eredményezhetnek olyan szervezeti információkhoz és eszközökhöz, amelyek egyébként nem lennének hozzáférhetők.

A követelmény alkalmazásának lépései

1. A szervezetnek azonosítania és nyilvántartásba kell vennie azokat a karbantartási eszközöket, amelyek privilegizált jogosultsággal futnak.
2. A szervezetnek alkalmaznia kell egy naplózási és monitorozó rendszert, amely képes nyomon követni és rögzíteni a privilegizált jogosultsággal futó karbantartási eszközök használatát.
3. A szervezetnek úgy kell beállítania a naplózási és monitorozó rendszert, hogy az riasztásokat küldjön az érintett szervezet által kijelölt szervezeti egységnek, amennyiben a privilegizált jogosultsággal futó karbantartási eszközök szokatlan vagy gyanús tevékenységet végeznek.
4. A szervezetnek rendszeresen ellenőriznie kell a naplókat, hogy azonosítsa a potenciális biztonsági problémákat, és gyorsan reagáljon a riasztásokra.
5. A szervezetnek rendszeresen felül kell vizsgálnia és és szükség esetén frissítenie kell a naplózási és monitorozó rendszer beállításait annak érdekében, hogy biztosítsa a rendszer hatékonyságát és a privilegizált jogosultsággal futó karbantartási eszközök megfelelő felügyeletét.
6. A szervezetnek képzést kell biztosítania a személyzet számára a privilegizált jogosultsággal futó karbantartási eszközök megfelelő használatáról és a potenciális biztonsági kockázatokról.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése
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

MA-3(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

10.10. Karbantartási eszközök – Szoftverfrissítések és javítások

10.10. A szervezet ellenőrzi a karbantartási eszközöket, hogy megbizonyosodjon arról, hogy azokon a legújabb szoftverfrissítések és javítások telepítésre kerültek.

Magyarázat

Az elavult és/vagy javítás nélküli szoftvert használó karbantartói eszközök esetleges gyengeségeit kihasználhatják a támadók, mely az érintett szervezet számára jelentős sérülékenységet jelenthet.

A követelmény alkalmazásának lépései

1. A szervezetnek fel kell mérnie, milyen karbantartási eszközöket használnak.
2. A szervezetnek ellenőriznie kell, hogy a karbantartási eszközökön a legújabb szoftverfrissítések és javítások telepítésre kerültek-e.
3. A szervezetnek rendszeresen dokumentálnia kell a karbantartási eszközök frissítéseiről. Ez magában foglalja a frissítések dátumát, időpontját, a frissített eszközök listáját és a frissítések eredményét.
4. A szervezetnek biztosítania kell, hogy a karbantartási eszközök frissítéseit a lehető leggyorsabban telepítsék, miután azok elérhetővé válnak. Ez minimalizálja az elavult és/vagy javítás nélküli szoftvert használó karbantartási eszközök potenciális sérülékenységét.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése
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

MA-3(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

10.11. TÁVOLI KARBANTARTÁS

10.11. A szervezet:

10.11.1. Jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket.

10.11.2. Csak akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, amennyiben az összhangban áll a szervezeti szabályokkal és az EIR rendszerbiztonsági tervében dokumentált.

10.11.3. Erős hitelesítési eljárásokat alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásakor.

10.11.4. Nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről.

10.11.5. Lezárja a munkaszakaszokat és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik.

MAGYARÁZAT

Távoli karbantartásnak nevezzük azt, amikor egy személy hálózat segítségével végez karbantartási munkát, függetlenül attól, hogy az külső vagy belső hálózaton történik. Az egyének által hálózat igénybevétele nélkül, információs rendszer vagy rendszerelem mellett történő fizikai jelenlét során zajló tevékenységeket helyszíni karbantartásnak tekintjük. Az erős hitelesítési megoldások általában többfaktoros hitelesítést használnak és védelmet nyújtanak a visszajátszásos támadások ellen. Megfelelő hitelesítő eszköz lehet például a nyilvános kulcsú infrastruktúra (PKI), ahol a tanúsítványok egy token-en kerülnek tárolásra és jelszóval, jelmondattal vagy biometrikusan védettek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet jóváhagyja, nyomon követi és ellenőrzi a távoli karbantartási és diagnosztikai tevékenységeket. Ez azt jelenti, hogy az érintett szervezetnek rendszeresen ellenőriznie kell a távoli karbantartási és diagnosztikai tevékenységeket, és biztosítania kell, hogy ezek megfelelnek a szervezeti szabályoknak és a rendszerbiztonsági tervnek.

2. A szervezet csak akkor engedélyezi a távoli karbantartási és diagnosztikai eszközök használatát, amennyiben az összhangban áll a szervezeti szabályokkal és az EIR rendszerbiztonsági tervében dokumentált.
3. A szervezet erős hitelesítési eljárásokat alkalmaz a távoli karbantartási és diagnosztikai munkaszakaszok létrehozásakor. Ez azt jelenti, hogy az érintett szervezetnek biztosítania kell, hogy a távoli karbantartási és diagnosztikai munkaszakaszok létrehozása során erős hitelesítési eljárásokat alkalmaznak, például többtényezős hitelesítést vagy PKI-t, ahol a tanúsítványokat jelszóval, jelmondattal vagy biometrikus adatokkal védett token-en tárolják.
4. A szervezet nyilvántartást vezet a távoli karbantartási és diagnosztikai tevékenységekről. Ez azt jelenti, hogy az érintett szervezetnek dokumentálnia kell a távoli karbantartási és diagnosztikai tevékenységeket annak érdekében, hogy nyomon követhető legyen milyen tevékenységek történtek és ki végezte azokat.
5. A szervezet lezárja a munkaszakaszokat és a hálózati kapcsolatokat, amikor a távoli karbantartás befejeződik.

Kapcsolódó intézkedések

2.2. Fiókkezelés
2.15. Hozzáférés-ellenőrzés érvényesítése
2.60. Legkisebb jogosultság elve
2.100. Távoli hozzáférés
4.2. Naplózható események
4.3. Naplóbejegyzések tartalma
8.2. Azonosítás és hitelesítés
8.14. Azonosító kezelés
8.21. A hitelesítésre szolgáló eszközök kezelése
8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

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

3.3.7.4. Távoli karbantartás

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

MA-4

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

10.12. TÁVOLI KARBANTARTÁS – NAPLÓZÁS ÉS FELÜLVIZSGÁLAT

10.12. A szervezet:

10.12.1. Naplózza azokat a távoli karbantartási és diagnosztikai munkaszakaszokat, amelyeket a szervezet meghatározott naplózási eseményként definiál.

10.12.2. felülvizsgálja és elemzi a karbantartási és diagnosztikai munkaszakaszok naplóbejegyzéseit, a rendellenességek észlelése céljából.

MAGYARÁZAT

Az érintett szervezet naplózza azokat a távoli karbantartási és diagnosztikai munkaszakaszokat, amelyeket a szervezet meghatározott naplózási eseményként definiál. Ez azt jelenti, hogy minden olyan művelet, amely a távoli karbantartás vagy diagnosztika során történik, rögzítésre kerül egy naplóban. Ez magában foglalhatja a műveleteket, amelyeket a karbantartási személyzet végzett, az időpontokat, amikor a műveletek megtörténtek, és a műveletek eredményét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a távoli karbantartási és diagnosztikai munkaszakaszokat, amelyeket naplózási eseményként definiál. Ez magában foglalhatja a rendszerbe való bejelentkezést, a rendszer módosításait, a rendszerleállításokat és újraindításokat, valamint a hibaelhárítási tevékenységeket.
2. Miután a szervezet meghatározta a naplózási eseményeket, implementálnia kell a naplózási mechanizmust. Ez magában foglalhatja a naplózási szoftver telepítését, a naplózási paraméterek beállítását, és a naplófájlok helyének meghatározását.
3. A szervezetnek rendszeresen felül kell vizsgálnia és elemeznie a naplóbejegyzéseket, hogy észlelje a rendellenességeket. Ez magában foglalhatja a naplóbejegyzések automatikus elemzését, illetve manuális áttekintését.

Kapcsolódó intézkedések

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.40. Naplóbejegyzések létrehozása

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.8.16

NIST SP 800-53 rev.5 referencia

MA-4(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

10.13. TÁVOLI KARBANTARTÁS – AZONOS SZINTŰ BIZTONSÁG ÉS ADATTÖRLÉS

10.13. A szervezet:

10.13.1. megköveteli, hogy a távoli karbantartási és diagnosztikai javítások olyan EIR-ből legyenek végrehajtva, amelyben a biztonsági képességek azonos szintűek a karbantartott rendszer biztonsági képességeivel, vagy amennyiben ez nem biztosított,

10.13.2. megköveteli, hogy a karbantartandó elemet az EIR-ből eltávolítsák, a karbantartást megelőzően minden szervezeti információt biztonságosan töröljenek az érintett rendszerelemről. A karbantartási folyamat végrehajtását követően az érintett elemet átvizsgálják a potenciálisan kártékony szoftverek észlelése érdekében, mielőtt az EIR-hez csatlakoztatnák.

MAGYARÁZAT

Az információs rendszerek, diagnosztikai eszközök és a karbantartási szolgáltatásokat nyújtó berendezések azonos biztonsági képessége azt jelenti, hogy az említett rendszerek, eszközök és berendezések alkalmazott biztonsági követelményei megfelelnek legalább a karbantartott információs rendszer biztonsági követelményeinek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először biztosítania kell, hogy a távoli karbantartási és diagnosztikai javításokat végző EIR biztonsági képességei azonos szintűek a karbantartott EIR biztonsági képességeivel. Ez azt jelenti, hogy azokon az EIR-eken, eszközökön és berendezéseken, amelyek a karbantartási szolgáltatásokat nyújtják, legalább olyan szintű a biztonság, mint az éppen karbantartott EIR-en.
2. Ha legalább az azonos szintű biztonság nem biztosított, az érintett szervezetnek meg kell követelnie a karbantartandó elem eltávolítását az EIR-ből. Emellett a karbantartás megkezdése előtt minden szervezeti információt biztonságosan töröljenek az érintett rendszerelemről.
3. A karbantartási folyamat végrehajtását követően az érintett szervezetnek át kell vizsgálnia az érintett elemet a potenciálisan kártékony szoftverek észlelése érdekében. Csak ezt követően csatlakoztathatják az érintett elemet az EIR-hez.

4. A szervezetnek dokumentálnia kell a távoli karbantartással kapcsolatos tevékenységeket annak érdekében, hogy nyomon követhető legyen milyen tevékenységek történtek és ki végezte azokat.

Kapcsolódó intézkedések

11.8. Adathordozók törlése
18.8. Kártékony kódok elleni védelem
18.42. Szoftver- és információsértetlenség

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

3.3.7.4. Távoli karbantartás

ISO/IEC 27001:2023 referencia

A.8.10

NIST SP 800-53 rev.5 referencia

MA-4(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

10.14. TÁVOLI KARBANTARTÁS – HITELESÍTÉS ÉS A KARBANTARTÁSI MUNKASZAKASZOK SZÉTVÁLASZTÁSA

10.14. A szervezet az alábbi intézkedésekkel védi a munkaszakaszokat a távoli karbantartás során:

10.14.1. olyan hitelesítő eszközöket kell alkalmazni, amelyek ellenállnak a visszajátszásos támadásoknak.

10.14.2. A karbantartási munkaszakaszok el kell különíteni a rendszer többi hálózati munkaszakaszától a következő módokon:

10.14.2.1. fizikailag elkülönített kommunikációs útvonalak használatával; vagy

10.14.2.2. logikailag elkülönített kommunikációs útvonalak használatával.

MAGYARÁZAT

Az érintett szervezet olyan hitelesítő eszközöket használ, amelyek képesek megakadályozni a visszajátszásos támadásokat. A visszajátszásos támadások során a támadók ellopják a hitelesítő adatokat, majd ezeket az adatokat felhasználva próbálnak hozzáférni az EIR-hez. Az ellenálló hitelesítő eszközök olyan technológiákat használnak, mint például a kéttényezős hitelesítés, amelyek megnehezítik a visszajátszásos támadásokat.

Az érintett szervezetnek biztosítania kell, hogy a karbantartási munkaszakaszok kommunikációs csatornái elkülönüljenek. Ez megakadályozza, hogy a karbantartás során esetlegesen felmerülő biztonsági problémák kihatással legyenek az EIR többi részére. Az elkülönítés történhet fizikai és logikai módon. Fizikai elkülönítés esetén a karbantartási munkaszakaszoknak saját, fizikailag elkülönített kommunikációs útvonalai vannak, amelyek nem érintkeznek az EIR többi részével. A logikai elkülönítés esetén a karbantartási munkaszakaszok kommunikációs útvonalai logikailag elkülönül az EIR többi részétől. Ez gyakran titkosítás segítségével történik, amely biztosítja, hogy csak a megfelelő személyek férjenek hozzá a karbantartási munkaszakaszokhoz.

Ezek az intézkedések segítenek az érintett szervezetnek megvédeni az EIR munkaszakaszait a távoli karbantartás során, és minimalizálni a potenciális kiberbiztonsági kockázatokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek olyan hitelesítő eszközöket kell alkalmaznia, amelyek ellenállnak a visszajátszásos támadásoknak.
2. A karbantartási munkaszakaszokat el kell különíteni az EIR többi hálózati munkaszakaszától. Ez az elkülönítés kétféleképpen történhet:
a) Fizikailag elkülönített kommunikációs útvonalak használatával: Ez azt jelenti, hogy a karbantartási munkaszakaszoknak saját, különálló kommunikációs útvonalai vannak, amelyek nem érintkeznek az EIR többi részével.
b) Logikailag elkülönített kommunikációs útvonalak használatával: Ez azt jelenti, hogy a karbantartási munkaszakaszok kommunikációs útvonalai ugyanazon a fizikai hálózaton vannak, mint az EIR többi része, de a hálózati forgalmat úgy szabályozzák, hogy a karbantartási munkaszakaszok és az EIR többi része között nincs közvetlen kommunikáció.
3. A szervezetnek dokumentálnia kell a távoli karbantartással kapcsolatos tevékenységeket annak érdekében, hogy nyomon követhető legyen milyen tevékenységek történtek és ki végezte azokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

MA-4(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

10.15. TÁVOLI KARBANTARTÁS – JÓVÁHAGYÁSOK ÉS ÉRTESÍTÉSEK

10.15. A szervezet:
10.15.1. megköveteli a minden távoli karbantartási munkaszakasz meghatározott személyek vagy szerepkörök által történő jóváhagyását, és
10.15.2. értesíti a meghatározott személyeket vagy szerepköröket a tervezett távoli karbantartás időpontjáról.

MAGYARÁZAT

Távoli karbantartás jóváhagyását, a karbantartás megfelelőségének megállapításához elegendő információbiztonsági és rendszerismerettel rendelkező személy végezheti. Az ilyen műveletek esetében szükséges az érintett szervezet által meghatározott szereplők értesítése.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek szabályzatba és/vagy eljárásrendbe kell foglalnia, hogy mely személyek vagy szerepkörök jogosultak a távoli karbantartási munkaszakaszok jóváhagyására. A szabályzat és/vagy eljárásrend tartalmazza a jóváhagyási folyamatot, a szükséges dokumentációt és az esetleges kivételeket.
2. A szervezetnek meg kell bizonyosodnia arról, hogy a távoli karbantartási munkaszakaszokat végző személyek tisztában vannak a vonatkozó szabályzattal és/vagy eljárásrenddel és azt/azokat be is tartják.
3. A szervezetnek létre kell hoznia egy értesítési rendszert, amely tájékoztatja a meghatározott személyeket vagy szerepköröket a tervezett távoli karbantartás időpontjáról pl.: e-mail vagy egy belső kommunikációs platform.
4. A szervezetnek dokumentálnia kell a távoli karbantartással kapcsolatos tevékenységeket annak érdekében, hogy nyomon követhető legyen milyen tevékenységek történtek és ki végezte azokat.
5. A szervezetnek rendszeresen felül kell vizsgálnia és és szükség esetén frissítenie kell a távoli karbantartási munkaszakaszok jóváhagyási és értesítési folyamatát, hogy biztosítsa azok hatékonyságát és naprakészségét.

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

MA-4(5)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

10.16. TÁVOLI KARBANTARTÁS – KRIPTOGRÁFIAI VÉDELEM

10.16. A szervezet meghatározott kriptográfiai mechanizmusokat alkalmaz a távoli karbantartási és diagnosztikai tevékenységhez használt kommunikáció sértetlenségének és bizalmasságának védelme érdekében.

MAGYARÁZAT

Távoli karbantartási és diagnosztikai feladatok végzése esetén a kommunikáció védelmének nem megfelelő beállítása azt eredményezheti, hogy illetéktelen személyek hozzáférhetnek a szervezeti információkhoz a távoli karbantartási vagy diagnosztikai folyamat során. Az ilyen jellegű jogosulatlan hozzáférés számos kockázattal jár, beleértve a rosszindulatú kódok beillesztését, a rendszerparaméterek jogosulatlan módosítását és a szervezeti információk kiszivárgását. Az érintett szervezet olyan kriptográfiai védelemmel ellátott megoldást kell alkalmazzon, mely szavatolja az információk biztonságát a folyamat végzése alatt.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a távoli karbantartási és diagnosztikai tevékenységekhez használt kommunikációs csatornákat.
2. A szervezetnek meg kell határoznia a megfelelő kriptográfiai mechanizmusokat, amelyeket a távoli karbantartási és diagnosztikai tevékenységekhez használni fog, azért, hogy biztosítsa a kommunikáció sértetlenségét és bizalmasságát.
3. A szervezetnek alkalmaznia kell a kiválasztott kriptográfiai mechanizmusokat a távoli karbantartási és diagnosztikai tevékenységek során.
4. A szervezetnek tesztelnie kell a kriptográfiai mechanizmusok működését, hogy biztosítsa a távoli karbantartási és diagnosztikai tevékenységekhez használt kommunikáció sértetlenségét és bizalmasságát.
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén módosítania kell a kriptográfiai mechanizmusokat annak érdekében, hogy biztosítsa a távoli karbantartási és diagnosztikai tevékenységekhez használt kommunikáció sértetlenségét és bizalmasságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.40. Az adatátvitel bizalmassága és sértetlensége

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

MA-4(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kriptográfiai mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

10.17. TÁVOLI KARBANTARTÁS – KAPCSOLAT MEGSZAKÍTÁSÁNAK MEGERŐSÍTÉSE

10.17. A szervezet ellenőrzi a munkaszakaszok és a hálózati kapcsolatok megszűnését a távoli karbantartási és diagnosztikai munkaszakasz befejezése után.

MAGYARÁZAT

Az érintett szervezet a távoli karbantartási és diagnosztikai tevékenység befejezése után megszünteti az azt támogató munkaszakaszokat és hálózati kapcsolatokat, ezzel meggátolva azok jogosulatlan használatát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek szabályzatban és/vagy eljárásrendben definiálnia kell, hogy a távoli karbantartási és diagnosztikai tevékenység befejezése után megszünteti az azt támogató munkaszakaszokat és hálózati kapcsolatokat.
2. A távoli karbantartási és diagnosztikai tevékenység befejezése után az érintett szervezetnek ellenőriznie kell, hogy a tevékenységet támogató munkaszakaszok és hálózati kapcsolatok valóban megszűntek-e.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.84. A munkaszakasz lezárása

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

MA-4(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

10.18. KARBANTARTÓ SZEMÉLYEK

10.18. A szervezet:

10.18.1. Kialakít egy folyamatot a karbantartási munkákhoz szükséges hozzáférési jogosultságok kezelésére, és nyilvántartást vezet a hozzáférési jogosultsággal rendelkező karbantartó szervezetekről vagy személyekről.

10.18.2. Ellenőrzi az EIR-en kíséret nélkül karbantartást végző személyek hozzáférési jogosultságait.

10.18.3. Kijelöli a szervezethez tartozó és a kívánt hozzáférési jogosultságokkal, valamint a megfelelő műszaki szakértelemmel rendelkező személyeket arra, hogy felügyeljék a szükséges jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

MAGYARÁZAT

A karbantartó személyzet olyan személyekre utal, akik hardveres vagy szoftveres karbantartást végeznek az érintett szervezet EIR-jén. Azok a személyek, akiket korábban nem azonosítottak jogosult karbantartó személyzetként - mint például a gyártók, szolgáltatók, rendszerintegrátorok és tanácsadók - előfordulhat, hogy privilegizált hozzáférést igényelnek a szervezet EIR-jéhez. Ez például akkor fordulhat elő, amikor rövid határidővel vagy azonnal kell karbantartási tevékenységeket végezniük. A szervezet kockázatelemzése alapján ideiglenes hozzáférési jogosultságot adhat ezeknek a személyeknek. Az ideiglenes hozzáférési jogosultságok egyszeri használatra vagy korlátozott időszakra szólhatnak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet kialakít egy folyamatot a karbantartási munkákhoz szükséges hozzáférési jogosultságok kezelésére.
2. A szervezet nyilvántartást vezet a hozzáférési jogosultsággal rendelkező karbantartó szervezetekről vagy személyekről.
3. A szervezetnek ellenőriznie kell az EIR-en kíséret nélkül karbantartást végző személyek hozzáférési jogosultságait.
4. A szervezet gondoskodik arról, hogy a szervezethez tartozó és a kívánt hozzáférési jogosultságokkal, valamint a megfelelő műszaki szakértelemmel rendelkező személyek

felügyeljék a szükséges jogosultságokkal nem rendelkező személyek karbantartási tevékenységeit.

5. A szervezet ideiglenes hozzáférési jogosultságot adhat a karbantartást végző személyeknek, azonban ennek kockázatát a kockázatelemzésben értékelnie kell. Az ideiglenes hozzáférési jogosultságok egyszeri használatra vagy korlátozott időszakra szólhatnak.

Kapcsolódó intézkedések

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

2.59. Felelősségek szétválasztása

2.60. Legkisebb jogosultság elve

8.2. Azonosítás és hitelesítés

8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

10.11. Távoli karbantartás

11.2. Hozzáférés az adathordozókhoz

12.2. A fizikai belépési engedélyek

12.6. A fizikai belépés ellenőrzése

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

3.2.1.19. Karbantartók

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

MA-5

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

10.19. KARBANTARTÓ SZEMÉLYEK – NEM MEGFELELŐ ELLENŐRZÖTTSÉGŰ SZEMÉLYEK

10.19. A szervezet:

10.19.1. Eljárásokat dolgoz ki a nem megfelelő biztonsági ellenőrzöttségű karbantartó személyzet tevékenységének szabályozására.

10.19.1.1. Azokat a karbantartó személyeket, akik nem rendelkeznek a szükséges hozzáférési jogosultságokkal, a szervezet által jóváhagyott, megfelelő hozzáférési jogosultsággal és szaktudással rendelkező személyek kísérik és felügyelik őket a karbantartási és diagnosztikai tevékenységek során.

10.19.1.2. A karbantartási és diagnosztikai tevékenységek megkezdése előtt minden volatilis adattároló eszközt biztonságosan töröl, a nem volatilis eszközök esetében gondoskodik az adattároló eltávolításáról vagy fizikailag leválasztja a rendszerről.

10.19.2. Alternatív biztonsági folyamatot alakít ki arra az esetre, ha egy rendszerelemet nem lehet törölni, eltávolítani vagy a rendszerről leválasztani.

MAGYARÁZAT

Az érintett szervezet olyan eljárásrendet alakít ki, mely a nem megfelelő ellenőrzöttségű személyek számára nem teszi lehetővé az érintett szervezet területére történő belépést és az érintett szervezet tulajdonában álló EIR-ekhez történő hozzáférést.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először eljárásokat kell kidolgoznia a nem megfelelő ellenőrzöttségű karbantartó személyzet tevékenységének szabályozására.
2. A szervezetnek biztosítania kell, hogy a nem megfelelő hozzáférési jogosultságokkal rendelkező karbantartó személyeket megfelelő hozzáférési jogosultsággal és szaktudással rendelkező személyek kísérjék és felügyeljék a karbantartási és diagnosztikai tevékenységek során.
3. A szervezetnek minden volatilis adattároló eszközt biztonságosan törölnie kell a karbantartási és diagnosztikai tevékenységek megkezdése előtt. A nem volatilis eszközök esetében az érintett

szervezetnek gondoskodnia kell az adattároló eltávolításáról vagy fizikailag leválasztani az EIR-ről.

4. A szervezetnek alternatív biztonsági folyamatot kell kialakítania arra az esetre, ha egy rendszerelemet nem lehet törölni, eltávolítani vagy az EIR-ről leválasztani.

5. A szervezetnek dokumentálnia kell a távoli karbantartással kapcsolatos tevékenységeket annak érdekében, hogy nyomon követhető legyen milyen tevékenységek történtek és ki végezte azokat.

6. A szervezetnek rendszeresen felül kell vizsgálnia és és szükség esetén frissítenie kell a nem megfelelő biztonsági ellenőrzöttségű karbantartó személyzet tevékenységével kapcsolatos szabályzatokat és/vagy eljárásrendeket annak érdekében, hogy azok hatékonyan működjenek és naprakészek legyenek.

Kapcsolódó intézkedések

11.8. Adathordozók törlése

13.2. Rendszerbiztonsági terv

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

3.2.1.19. Karbantartók

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

MA-5(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

10.20. KARBANTARTÓ SZEMÉLYEK – NEM RENDSZER KARBANTARTÁS

10.20. A szervezet biztosítja, hogy a rendszerhez közvetlenül nem kapcsolódó, de a rendszer fizikai közelében tartózkodó, kísérettel nem rendelkező karbantartási tevékenységeket végző személyzet rendelkezzen a szükséges hozzáférési engedélyekkel.

MAGYARÁZAT

Az érintett szervezet biztosítja, hogy az EIR-hez közvetlenül nem kapcsolódó, de az EIR fizikai közelében tartózkodó, kísérettel nem rendelkező karbantartási tevékenységeket végző személyzet rendelkezzen a szükséges hozzáférési engedélyekkel. Ez a követelmény magában foglalja a fizikai létesítményeket kezelő személyzetet és a takarító személyzetet is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell azokat a személyeket, akik karbantartási tevékenységeket végeznek az EIR fizikai közelében, de nem közvetlenül kapcsolódnak hozzá.
2. A szervezetnek az említett személyek hozzáférésének engedélyezésére ki kell alakítania egy folyamatot, melyet szabályzatba és/vagy eljárásrendbe kell foglalnia, amely meghatározza, hogy milyen hozzáférési jogosultságokkal és eszközökkel rendelkezhetnek ezek a személyek. Ez magában foglalhatja a belépési kódokat, belépőkártyákat vagy biometrikus azonosítókat.
3. A szervezetnek biztosítania kell, hogy ezek a személyek megkapják a szükséges hozzáférési engedélyeket, és tisztában vannak azzal, hogy mikor és hogyan használhatják azokat.
4. A szervezetnek rendszeresen ellenőriznie kell a hozzáférési engedélyeket, ezáltal biztosítja, hogy csak a megfelelő személyek rendelkezzenek hozzáféréssel.
5. A szervezetnek dokumentálnia kell a hozzáférési engedélyek kiosztását, módosítását és visszavételét, így nyomon követhető hogy ki milyen jogosultsággal rendelkezik. Ez segíthet a jogosulatlan hozzáférési kísérletek azonosításában és megelőzésében. Az érintett szervezetnek emellett naplóznia kell a hozzáférési engedélyekkel kapcsolatos tevékenységeket, így nyomon követhető, hogy ki, mikor és milyen cselekményt hajtott végre.

6. A szervezetnek rendszeres biztonságtudatossági képzéseket és tájékoztatókat kell biztosítania a személyzet számára a hozzáférési engedélyek használatáról és az azzal kapcsolatos biztonsági előírásokról, így csökkenthető a jogosulatlan hozzáférés kockázata.

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

MA-5(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

10.21. KELLŐ IDŐBEN TÖRTÉNŐ KARBANTARTÁS

10.21. A szervezet meghatározza, hogy mely rendszerelemek esetén, milyen időtartamon belül szükséges karbantartási támogatást vagy pótalkatrészt biztosítani hiba esetén.

MAGYARÁZAT

Az érintett szervezet meghatározza azokat a rendszerelemeket, amelyek ha nem működnek megfelelően, kockázatot jelentenek a szervezet működésére és eszközeire nézve. Az érintett szervezet gondoskodik arról, hogy ezen rendszerelemek vonatkozásában rendelkezzen szerződésben rögzített karbantartási támogatással.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell azokat a rendszerelemeket, amelyek ha nem működnek megfelelően kockázatot jelentenek a szervezet működésére és eszközeire nézve.
2. A szervezet értékeli a rendszerelemek kritikusságát és priorizálja őket a karbantartási támogatás szükségessége alapján. Ez magában foglalhatja a rendszer kiesése esetén bekövetkező hatás elemzését, valamint a rendszer helyreállítási idejének becslését.
3. A szervezet meghatározza, hogy mely rendszerelemek esetén, milyen időtartamon belül szükséges karbantartási támogatást vagy pótalkatrészt biztosítani hiba esetén.
4. A szervezet az említett rendszerelemek vonatkozásában megállapodásokat köt a karbantartási támogatásra, illetve pótalkatrész biztosítására.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.36. Rendszerelem leltár
7.2. Üzletmenet-folytonossági terv
7.23. Alternatív feldolgozási helyszín
15.20. Kockázatokra adott válasz
16.76.1. Fejlesztési folyamat, szabványok és eszközök
18.68. Előrelátható meghibásodás megelőzése
19.2. Ellátási láncra vonatkozó kockázatkezelési szabályzat
19.4. Ellátási láncra vonatkozó követelmények és folyamatok

19.8. Rendszerelemek és kapcsolódó adatok eredetisége

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

3.2.1.19. Karbantartók

ISO/IEC 27001:2023 REFERENCIA

A.7.13

NIST SP 800-53 REV.5 REFERENCIA

MA-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek illetve az idő intervallum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

10.22. Kellő időben történő karbantartás – Megelőző karbantartás

10.22. A szervezet meghatározott gyakorisággal megelőző karbantartást végez a kijelölt rendszerelemeken.

Magyarázat

A megelőző karbantartás a rendszerelemek proaktív szervizelését jelenti. Ezáltal az érintett szervezet berendezései és létesítményei kielégítő állapotban működhetnek. Ez a típusú karbantartás biztosítja a rendszeres ellenőrzést, teszteket, méréseket, beállításokat, alkatrészek cseréjét, illetve a kezdeti hibák észlelését és korrekcióját mielőtt azok ténylegesen bekövetkeznének vagy mielőtt nagyobb gondot okoznának. A megelőző karbantartás elsődleges célja a berendezések meghibásodásával járó következmények elkerülése vagy enyhítése. Emellett a megelőző karbantartás célja a berendezések megbízhatóságának megőrzése és helyreállítása a kopott alkatrészek cseréjével, mielőtt azok hibát okoznának. A megelőző hibakezelési szabályzatok alkalmazásának meghatározására szolgáló módszerek közé tartoznak a gyártó ajánlásai; meghibásodási statisztikák; a szakértői vélemények; már elvégzett karbantartás hasonló berendezéseken; a jogszabályok, törvények vagy követelményei, vagy a mért értékek és teljesítményjelzők.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a megelőző karbantartás gyakoriságát a rendszerelemeken.
2. A szervezetnek rendszeresen ellenőriznie kell a rendszerelemeket annak érdekében, hogy időben észrevegye a meghibásodásokat.
3. A szervezetnek ki kell cserélnie az elhasználódott rendszerelemeket, mielőtt azok meghibásodnának.
4. A szervezetnek szabályoznia kell a megelőző karbantartást és eljárásrendet kell kialakítania a megelőző karbantarást érintően.
5. A szervezetnek dokumentálnia kell a megelőző karbantartást, így nyomon követheti a karbantartást, illetve annak hatékonyságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

MA-6(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

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

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

10.23. Kellő időben történő karbantartás – Prediktív karbantartás

10.23. A szervezet meghatározott gyakorisággal prediktív karbantartást végez a kijelölt rendszerelemeken.

Magyarázat

A prediktív karbantartás az eszközök állapotának értékelését végzi el, periodikus vagy folyamatos eszközállapot-monitorozás segítségével. A prediktív karbantartás célja, hogy a karbantartást olyan időpontban végezzék el, amikor az a legköltséghatékonyabb, illetve mielőtt az EIR teljesítménye egy adott küszöbérték alá esne. A prediktív karbantartás célja az EIR jövőbeli állapotához köthető trendek előrejelzése. A prediktív karbantartás jelentős költségmegtakarítást és megbízhatóbb EIR-t eredményezhet.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia azokat a rendszerelemeket, amelyeken prediktív karbantartást kíván végezni.
2. A szervezetnek meg kell határoznia a prediktív karbantartás gyakoriságát.
3. A szervezetnek implementálnia kell egy rendszert vagy eszközt, amely képes monitorozni és elemezni a rendszerelemek állapotát. Ennek az eszköznek vagy rendszernek képesnek kell lennie arra, hogy figyelmeztesse a szervezethez köthető személyeket, ha egy rendszerelem állapota eléri a karbantartási küszöbértéket.
4. A szervezetnek rendszeresen el kell végeznie a prediktív karbantartást a kijelölt rendszerelemeken a meghatározott gyakorisággal.
5. A szervezetnek dokumentálnia kell a prediktív karbantartási tevékenységeket.
6. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a prediktív karbantartási tevékenységekre vonatkozó szabályzatokat és eljárásrendeket, így biztosítva azok hatékonyságát és naprakészségét.

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

MA-6(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

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

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

10.24. Kellő időben történő karbantartás – Prediktív karbantartás automatizált támogatása

10.24. A szervezet meghatározott automatizált mechanizmusok segítségével végzi el a prediktív karbantartási adatok átvitelét egy karbantartáskezelő rendszerbe.

Magyarázat

Az érintett szervezet egy karbantartáskezelő rendszert használ, amely egy adatbázisban tárolja a karbantartási műveletekkel kapcsolatos információkat, és automatizálja az eszközök állapotára vonatkozó adatok feldolgozását, hogy elősegítse a karbantartás tervezését, végrehajtását és az azzal kapcsolatos jelentéseket.

A követelmény alkalmazásának lépései

1. A szervezetnek rendelkeznie kell egy automatizált karbantartáskezelő rendszerrel, amely képes feldolgozni a prediktív karbantartási adatokat.
2. A szervezetnek be kell állítania az automatizált mechanizmusokat, amelyek képesek gyűjteni a prediktív karbantartási adatokat, illetve képesek a begyűjtött adatokat továbbítani a karbantartáskezelő rendszernek.
3. A szervezetnek biztosítania kell, hogy az adatok átvitele a karbantartáskezelő rendszerbe biztonságos és védett legyen.
4. A szervezetnek rendszeresen ellenőriznie kell a karbantartáskezelő rendszer működését és a benne tárolt adatok pontosságát.
5. A szervezetnek biztosítania kell, hogy a karbantartási tevékenységek megfelelően végrehajtásra kerülnek a karbantartáskezelő rendszer által szolgáltatott adatok alapján. Ez magában foglalhatja a karbantartási ütemterv betartását, a szükséges alkatrészek beszerzését, valamint a karbantartási munkák dokumentálását.
6. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a prediktív karbantartási tevékenységekre vonatkozó szabályzatokat és eljárásrendeket, illetve a karbantartáskezelő EIR beállításait, így biztosítva azok hatékonyságát és naprakészségét.

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

MA-6(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

10.25. TEREPI KARBANTARTÁS SZABÁLYOZÁSA

10.25. A szervezet korlátozza vagy megtiltja a meghatározott EIR-ek vagy rendszerelemek terepen végzett karbantartását, vagy azt kizárólag a meghatározott, megbízható karbantartó létesítményekben engedélyezi.

MAGYARÁZAT

A terepen végzett karbantartás olyan karbantartási típus, amelyet egy EIR-en vagy rendszerelemen végeznek, miután az EIR-t vagy a rendszerelemet egy adott helyszínre telepítették. Bizonyos esetekben előfordulhat, hogy a terepen végzett karbantartást (azaz a helyszínen végzett karbantartást) nem végzik olyan szigorúan vagy ugyanolyan minőségben, mint ha azt egy megbízható karbantartó létesítményben végzenék. Az érintett szervezet által kritikusnak minősített EIR-ek esetében szükséges lehet korlátozni vagy megtiltani a terepen végzett karbantartást a helyszínen és előírni, hogy ilyen jellegű karbantartást kizárólag megbízható létesítményekben, további biztonsági követelmények betartásával lehet végrehajtani.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell azokat az EIR-eket vagy rendszerelemeket, amelyek esetében korlátozza vagy megtiltja a terepen végzett karbantartást.
2. A szervezetnek meg kell határoznia azt is, hogy melyek azok az EIR-ek vagy rendszerelemek amelyeket korlátozottan ugyan, de karban lehet tartani terepen is, illetve melyek azok az EIR-ek vagy rendszerelemek, melyek esetében kizárólag a meghatározott, megbízható karbantartó létesítményekben engedélyezett a karbantartás.
3. A szervezetnek a korlátozásról vagy tiltásról értesítenie kell az összes érintett személyt és csoportot a változásról és biztosítania kell, hogy mindenki megértse és betartsa a szabályokat.
4. Ha az érintett szervezet úgy dönt, hogy a karbantartás meghatározott, megbízható karbantartó létesítményekben engedélyezett akkor az érintett szervezetnek meg kell bizonyosodnia arról, hogy ezek a létesítmények megbízhatóak és megfelelően ellenőrzöttek.
5. A szervezetnek dokumentálnia kell minden karbantartási munkát, beleértve a karbantartás helyét, időpontját, a végzett munka részleteit és az érintett EIR-eket vagy rendszerelemeket.

6. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a terepi karbantartási tevékenységekre vonatkozó szabályzatokat és eljárásrendeket, így biztosítva azok hatékonyságát és naprakészségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

10.2. Szabályozott karbantartás
10.11. Távoli karbantartás
10.18. Karbantartó személyek

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

MA-7

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek illetve a megbízható karbantartó létesítmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024