Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Készenléti tervezés

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

7.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

7.1. A szervezet:

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

7.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó üzletmenet-folytonosságra vonatkozó szabályzatot, amely

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

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

7.1.1.2. Az üzletmenet-folytonosságra vonatkozó eljárásrendet, amely az üzletmenet-folytonosságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

7.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki az üzletmenet-folytonosságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

7.1.3. Felülvizsgálja és frissíti az aktuális üzletmenet-folytonosságra vonatkozó szabályzatot és az üzletmenet-folytonosságra vonatkozó eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

MAGYARÁZAT

A szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó üzletmenet-folytonossági szabályzat és üzletmenet-folytonossági eljárásrend megfelelő szintű kidolgozása alapvető fontosságú a szervezet és az EIR-ek üzletmenet-folytonosságának biztosítása érdekében. A két dokumentum - mint keretrendszer - tartalmazza a szervezet elvárásait az üzletmenet-folytonosságra vonatkozóan, melyek megállapításánál figyelembe szükséges venni az érdekelt felek által támasztott, üzletmenet-folytonosságra vonatkozó elvárásokat is. Fontos, hogy a dokumentumok összhangban legyenek a szervezet információbiztonsági környezetével, kockázatkezelési stratégiájával. A szabályokat be lehet illeszteni az általános biztonsági

szabályzatokba, vagy több szabályzatban is megjelenhetnek (amennyiben a szervezet felépítése ezt indokolttá teszi), azonban javasolt külön kezelni őket. Az üzletmenet-folytonossági szabályzó dokumentumokat és eljárásokat javasolt a nemzetközi sztenderdekkel összhangban (pl.: ISO 22301) megalkotni. A megfelelő működés megteremtése és az elszámoltathatóság biztosítása érdekében kompetens személyek kijelölése szükséges a szabályzó dokumentumok megalkotásához és karbantartásához.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia és dokumentálnia kell egy üzletmenet-folytonossági szabályzatot, amely tartalmazza a szervezeti-, folyamat és rendszerszintű követelményeket. Ez a szabályzat meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az érintett szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat.
2. A szabályzatnak összhangban kell lennie a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.
3. A szervezetnek ki kell dolgoznia egy üzletmenet-folytonossági eljárásrendet, amely segíti az üzletmenet-folytonossági szabályzatban foglaltak és az ahhoz kapcsolódó ellenőrzések megvalósítását.
4. A szervezetnek ki kell jelölnie egy személyt, aki felelős az üzletmenet-folytonossági szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért.
5. A szervezetnek felül kell vizsgálnia és frissítenie kell az aktuális üzletmenet-folytonossági szabályzatot és az üzletmenet-folytonossági eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és 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

3.1.4.1. Üzletmenet-folytonosságra vonatkozó eljárásrend

ISO/IEC 27001:2023 REFERENCIA

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

NIST SP 800-53 REV.5 REFERENCIA

CP-1

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

7.2. ÜZLETMENET-FOLYTONOSSÁGI TERV

7.2. A szervezet:

7.2.1. Kidolgozza az EIR-re vonatkozó üzletmenet-folytonossági tervet, amely:

7.2.1.1. meghatározza az alapfeladatokat (biztosítandó szolgáltatásokat) és alapfunkciókat, valamint az ezekhez kapcsolódó vészhelyzeti követelményeket;

7.2.1.2. tartalmazza a helyreállítási célokat, a helyreállítási prioritásokat és metrikákat;

7.2.1.3. kijelöli a vészhelyzeti szerepköröket, felelősségeket, a kapcsolattartó személyeket és azok elérhetőségeit;

7.2.1.4. meghatározza az EIR összeomlása, kompromittálódása vagy hibája ellenére is biztosítandó szolgáltatásokat;

7.2.1.5. tartalmazza az EIR végleges, teljeskörű helyreállításának tervét, mely garantálja, hogy az eredetileg tervezett és megvalósított védelmi intézkedések a helyreállítás után ne sérüljenek;

7.2.1.6. szabályozza az üzletmenet-folytonossági információk megosztását; és

7.2.1.7. a szervezet által meghatározott személyek vagy szerepkörök által felülvizsgált és jóváhagyott.

7.2.2. Megfogalmazza, és a szervezetre érvényes követelmények szerint dokumentálja, valamint A szervezeten belül kizárólag a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyek és szervezeti egységek számára kihirdeti az EIR-ekre vonatkozó üzletmenet-folytonossági tervet.

7.2.3. Összehangolja a folyamatos működés tervezésére vonatkozó tevékenységeket a biztonsági események kezelésével;

7.2.4. Meghatározott gyakorisággal felülvizsgálja az EIR-hez kapcsolódó üzletmenet-folytonossági tervet.

7.2.5. Az EIR vagy a működési környezet változásainak, az üzletmenet-folytonossági terv megvalósítása, végrehajtása vagy tesztelése során felmerülő problémáknak megfelelően aktualizálja az üzletmenet-folytonossági tervet.

7.2.6. Tájékoztatja az üzletmenet-folytonossági terv változásairól a folyamatos működés szempontjából kulcsfontosságú, névvel vagy szerepkörrel azonosított személyeket és szervezeti egységeket.

7.2.7. Az üzletmenet-folytonossági terv tesztelése, gyakorlata vagy tényleges alkalmazása során levont tanulságokat beépíti a tesztelési és gyakorlati folyamatokba.

7.2.8. Gondoskodik arról, hogy az üzletmenet-folytonossági terv jogosulatlanok számára ne legyen megismerhető és módosítható.

MAGYARÁZAT

Az üzletmenet-folytonossági tervezés egy átfogó koncepció része, a folyamatos működés elérésére, a szervezeti és üzleti célok érdekében. Az üzletmenet-folytonossági tervezés a rendszer-visszaállítással és az alternatív folyamatok életbe léptetésével foglalkozik, amennyiben a rendszer üzemszerű működése nem biztosított. Ez az EIR tervezésének és fejlesztési életciklusának is szerves részét kell képezze. A üzletmenet-folytonossági tervek leírják az EIR-ek helyreállíthatóságának szintjét, ugyanis nem minden rendszernek kell teljes mértékben helyreállnia a működés folytonosságához. A rendszer-helyreállítási céloknak tükrözni szükséges az alkalmazandó törvényeket, végrehajtási rendeleteket, egyéb rendeleteket, irányelveket, szabványokat, ajánlásokat, a szervezeti kockázattűrés mértékét és a rendszer esetleges kiesésének hatását. Az üzletmenet-folytonossági tervben szereplő intézkedések magukban foglalják a rendszer elavulását, leállítását, a manuális üzemmódba való visszaállást, az alternatív információáramlást és a rendszerek támadása esetére fenntartott üzemmódokban való működést. A vészhelyzeti tervezés és a biztonsági események kezelési tevékenységeinek összehangolásával a szervezetek biztosítják, hogy a szükséges tervezési tevékenységek elvégzésre kerülnek és biztonsági esemény esetén végrehajtásra kerüljenek. Az üzletmenet-folytonossági tervezés során javasolt olyan nemzetközi szabványok szerint felépíteni az érintett szervezet folyamatait, mint pl. az ISO 22301.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az üzletmenet-folytonossági terv összhangban kell, hogy legyen a szervezet kockázatmenedzsment stratégiájával.

2. A terv készítése során fel kell becsülni a rendszer helyreállítási idejét és az adatvesztés toleranciáját, szem előtt tartva a rendszer kiesésének hatását, figyelembe véve a jogi és szabályozási követelményeket, szabványokat és ajánlásokat.

3. Meg kell állapítani azt a minimális szolgáltatási szintet, amely a működés folytonosságának fenntartása érdekében szükséges, és fel kell készülni az esetleges redundáns rendszerek és biztonsági mentések használatára.
4. Fel kell készülni a rendszerek manuális működésére, az alternatív információáramlásra és a rendszer támadása esetén alkalmazandó vészüzemre.
5. Meg kell határozni, hogy milyen szinten kell helyreállni a rendszereknek a működés folytonossága érdekében.
6. Rendszeres gyakorlatokat és teszteket kell végezni, hogy biztosítsák a terv hatékonyságát és a személyzet felkészültségét.
7. Felülvizsgálatokat és aktualizálásokat kell végrehajtani a terven, hogy biztosítsák annak relevanciáját és hatékony működését, figyelembe véve a változó üzleti, technológiai és fenyegetési környezetet.

Kapcsolódó intézkedések

7.10. A folyamatos működésre felkészítő képzés
7.13. Üzletmenet-folytonossági terv tesztelése
7.19. Biztonsági tárolási helyszín
7.23. Alternatív feldolgozási helyszín
7.29. Telekommunikációs szolgáltatások
7.35. Az elektronikus információs rendszer mentései
7.43. Az elektronikus információs rendszer helyreállítása és újraindítása
7.47. Alternatív kommunikációs protokollok
7.49. Alternatív biztonsági mechanizmusok alkalmazása
9.9.1. Biztonsági események kezelése

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

3.1.4.2. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

ISO/IEC 27001:2023 referencia

7.5.1; 7.5.2; 7.5.3; A.5.2; A.5.29; A.8.14

NIST SP 800-53 rev.5 referencia

CP-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

7.3. Üzletmenet-folytonossági terv – Összehangolás a kapcsolódó tervekkel

7.3. A szervezet egyezteti az üzletmenet-folytonossági tervet a kapcsolódó tervekért felelős szervezeti egységekkel.

Magyarázat

Az érintett szervezetnek számos kapcsolódó tervvel kell összehangolnia az üzletmenet-folytonossági tervét. Ezek közé tartoznak a katasztrófa-helyreállítási tervek, a kritikus infrastruktúra tervek, a működés folytonosságának tervei, a válságkommunikációs tervek, a belső fenyegetésekhez kapcsolódó, valamint a kockázatmenedzsmenthez kapcsolódó tervek, továbbá a különböző vészhelyzeti tervek. A szervezetnek biztosítania kell, hogy az üzletmenet-folytonossági terv összhangban legyen ezekkel a kapcsolódó tervekkel, hogy a váratlan események esetén is megfelelő szinten tudja kezelni a folyamatait, és biztosítani tudja a működés megfelelő szintű folytonosságát.

A követelmény alkalmazásának lépései

1. A szervezetnek fel kell mérnie, mely szervezeti egységek felelnek a kapcsolódó tervekért, mint például az üzletmenet-folytonossági terv, a katasztrófa helyreállítási terv, a kritikus infrastruktúra terv, a működés folytonossági terv, a válságkommunikációs terv, stb.
2. A szervezetnek biztosítania kell a készítéskori, ill. a periodikus egyeztetéseket ezekkel a szervezeti egységekkel, hogy megvitassák és elfogadják az üzletmenet-folytonossági tervet, és az alkalmazkodjon a kapcsolódó tervekhez.
3. Biztosítani kell, hogy az EIR képes legyen támogatni a tervben leírtakat.
4. A szervezetnek dokumentálnia kell az egyeztetési folyamatot, hogy nyomon követhető legyen a folyamat és a fejlődés.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az üzletmenet-folytonossági tervet, hogy biztosítsa annak relevanciáját és hatékonyságát.
6.Az szervezetnek biztosítania kell, hogy a szervezeti egységek tisztában legyenek a tervvel, és képesek legyenek végrehajtani a szükséges lépéseket egy esetleges kiberbiztonsági esemény esetén.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.1.4.2. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

ISO/IEC 27001:2023 referencia

A.5.30

NIST SP 800-53 rev.5 referencia

CP-2(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

7.4. Üzletmenet-folytonossági terv – Kapacitás tervezése

7.4. A szervezet megtervezi a folyamatos működéshez szükséges információfeldolgozó, infokommunikációs és környezeti képességek biztosításához szükséges kapacitást.

Magyarázat

Az érintett szervezetnek meg kell terveznie a folyamatos működéshez szükséges, valamint az információfeldolgozó, infokommunikációs és környezeti képességek biztosításához szükséges kapacitást. Ez magában foglalja az EIR-ek kapacitásának tervezését, hogy azok képesek legyenek kezelni a normál és vészhelyzeti terhelést, valamint a környezeti támogatás megtervezését, hogy az EIR-ek továbbra is működjenek, még akkor is, ha a környezeti feltételek romlanak. A kapacitás monitorozás fontos szerepet játszik ebben a folyamatban, mivel segít az érintett szervezetnek nyomon követni és értékelni az EIR-k teljesítményét és kapacitását, valamint azonosítani a potenciális problémákat és kockázatokat.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia az EIR kapacitásának jelenlegi állapotát, beleértve az információfeldolgozó, infokommunikációs és környezeti képességeket.
2. Meg kell határozni a jövőbeni igényeket, figyelembe véve a vállalat növekedési terveit, a technológiai fejlődést és a piaci trendeket.
3. A szervezetnek össze kell hasonlítania a jelenlegi kapacitást a jövőbeni igényekkel, és meg kell határoznia a szükséges változtatásokat.
4. A szervezetnek meg kell terveznie a szükséges kapacitásbővítést, beleértve az új berendezések beszerzését, a meglévő berendezések frissítését vagy a kapacitás bérbeadását.
5. Végre kell hajtani a kapacitásbővítési tervet, és naplózni kell a változásokat a rendszerben.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kapacitásbővítési tervet, hogy biztosítsa az EIR képességeinek megfelelő működését.
7. A szervezetnek biztosítania kell a kapacitásbővítési tervet támogató szabályok és eljárások meglétét, és rögzíteni kell a terv végrehajtását és a kapacitás változásait.

Kapcsolódó intézkedések

12.28. Vészhelyzeti tápellátás

12.31. Vészvilágítás

12.33. Tűzvédelem

12.37. Környezeti védelmi intézkedések

12.44. Az információs rendszer elemeinek elhelyezése

17.12. Szolgáltatásmegtagadással járó támadások elleni védelem

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

3.1.4.2. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

ISO/IEC 27001:2023 referencia

A.8.6

NIST SP 800-53 rev.5 referencia

CP-2(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

7.5. Üzletmenet-folytonossági terv – Üzleti (ügymeneti) funkciók visszaállítása

7.5. A szervezet meghatározza az alapfunkciók újrakezdésének időpontját az üzletmenet-folytonossági terv aktiválását követően.

Magyarázat

Az érintett szervezetnek meg kell határoznia az alapfunkciók újrakezdésének időpontját az üzletmenet-folytonossági terv aktiválását követően. Ez az időpont lehet azonnali, rövid távú, középtávú vagy hosszú távú, attól függően, hogy milyen gyorsan kell az EIR alapfunkcióit újraindítani a működés folytonosságának biztosítása érdekében.

A szervezetnek dokumentálnia kell az alapfunkciók újrakezdésének időpontját, hogy nyomon követhesse a folyamatot és értékelje a teljesítményt. Ez segíthet azonosítani a problémákat és javítani a folyamatokat a jövőben.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia az üzletmenet-folytonossági terv aktiválásának időpontját.
2. A szervezetnek prioritást kell rendelnie az alapfunkciók újrakezdéséhez.
3. A szervezetnek figyelembe kell vennie az üzemzavarok súlyosságát és mértékét az EIR-ben és annak támogató infrastruktúrájában, amikor meghatározza az alapfunkciók újrakezdésének időpontját.
4. A szervezetnek dokumentációt kell vezetnie a folyamatról, hogy később felülvizsgálhassa és szükség esetén módosíthassa azt.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.1.4.2. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-2(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az idő intervallum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

7.6. Üzletmenet-folytonossági terv – Alapfeladatok és alapfunkciók folyamatossága

7.6. A szervezet az alapfeladatok és alapfunkciók folyamatosságát úgy tervezi meg, hogy azok üzemelési folyamatosságában semmilyen, vagy csak csekély veszteség álljon elő. Fenntartható legyen a folyamatosság az EIR elsődleges feldolgozó vagy tárolási helyszínén történő teljes helyreállításáig.

Magyarázat

A szervezeteknek gondoskodniuk kell arról, hogy a működés folyamatossága fenntartható legyen az EIR elsődleges feldolgozó vagy tárolási helyszínén történő teljes helyreállításáig, még akkor is, ha a vészhelyzet miatt az elsődleges feldolgozó vagy tárolási helyszínek változnak. Ez azt jelenti, hogy az EIR-nek képesnek kell lennie arra, hogy folyamatosan működjön, minimálisan vagy veszteség nélkül, egészen az EIR teljes helyreállításig.

A követelmény alkalmazásának lépései

1. A szervezet először végezzen üzletmenet-folytonossági tervezést vagy üzleti hatáselemzést, amelyben meghatározza az alapfeladatok és alapfunkciók folyamatossági kritériumait.
2. A szervezet határozza meg az EIR elsődleges feldolgozó és/vagy tárolási helyszíneit, amelyek a vészhelyzeti tervezés részét képezik.
3. Fel kell készülni arra, hogy a vészhelyzeti tervezés során meghatározott elsődleges feldolgozó és/vagy tárolási helyszínek a vészhelyzettől függően változhatnak.
4. A szervezetnek biztosítania kell, hogy az EIR folyamatosan működjön (minimális veszteséggel, vagy veszteség nélkül) a teljes helyreállításig.
5. A szervezetnek dokumentálnia szükséges a teljes folyamatot, hogy nyomon követhető legyen a folyamatosság fenntartása és a helyreállítási folyamat.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a vészhelyzeti terveket, hogy biztosítsa az EIR folyamatos működését minden körülmények között.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.1.4.2. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-2(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

7.7. ÜZLETMENET-FOLYTONOSSÁGI TERV – ALTERNATÍV FELDOLGOZÁSI ÉS TÁROLÁSI HELYSZÍNEK

7.7. A szervezet a folytonosság fenntartása érdekében megtervezi az alapfeladatok vagy alapfunkciók minimális, vagy akár veszteség nélküli átirányítását alternatív feldolgozási vagy tárolási helyszínekre, amíg az EIR vissza nem állítható az elsődleges feldolgozási vagy tárolási helyszínen.

MAGYARÁZAT

Megfelelő módon biztosítani szükséges az alapfeladatok vagy alapfunkciók minimális, vagy akár veszteség nélküli átirányítását alternatív feldolgozási vagy tárolási helyszínekre, amíg az EIR vissza nem állítható az elsődleges feldolgozási vagy tárolási helyszínen. A szervezetek által a vészhelyzeti tervezés részeként meghatározott elsődleges feldolgozási és/vagy tárolási helyszínek változhatnak a vészhelyzettel összefüggő körülményektől függően. Az EIR átirányításának tervezése során az érintett szervezetnek meg kell határoznia azokat az alapfeladatokat vagy alapfunkciókat, amelyeket minimális vagy akár veszteség nélkül át kell irányítani az alternatív feldolgozási vagy tárolási helyszínekre. Ez magában foglalja az EIR működésének megértését, az alapfeladatok vagy alapfunkciók azonosítását, valamint azoknak a stratégiáknak és módszereknek a kidolgozását, amelyek segítségével ezeket az alapfeladatokat vagy alapfunkciókat át lehet irányítani.

Az EIR átirányításának tervezése során dokumentálni kell a tervezési folyamatot, beleértve a kockázatelemzést, a stratégiai tervezést, a végrehajtást és a tesztelést, mely segíthet azonosítani a tervezési folyamat során felmerülő problémákat, és lehetővé teszi a folyamat javítását a jövőben.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia azokat az alapfeladatokat vagy alapfunkciókat, amelyek folytonossága kritikus a szervezet működése szempontjából.
2. Fel kell mérni, hogy melyek azok az alternatív feldolgozási vagy tárolási helyszínek, amelyek alkalmasak lehetnek az alapfeladatok vagy alapfunkciók átirányítására.

3. Meg kell tervezni az alapfeladatok vagy alapfunkciók átirányításának folyamatát, beleértve a szükséges erőforrásokat, az időkeretet, és a kommunikációs tervet.
4. Tesztelni kell az átirányítási tervet, hogy biztosítva legyen annak hatékonysága és megbízhatósága.
5. Dokumentálni szükséges az átirányítási tervvel kapcsolatos tevékenységeket, beleértve a tesztelés eredményeit és az esetleges változtatásokat.
6. Rendszeresen felül kell vizsgálni és frissíteni kell az átirányítási tervet, hogy biztosítva legyen annak relevanciája és hatékonysága.
7. Amikor az EIR visszaállítható az elsődleges feldolgozási vagy tárolási helyszínen, a szervezetnek gondoskodnia kell az alapfeladatok vagy alapfunkciók zökkenőmentes visszaállításáról.

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

CP-2(6)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

7.8. Üzletmenet-folytonossági terv – Együttműködés külső szolgáltatókkal

7.8. A szervezet összehangolja saját üzletmenet-folytonossági tervét a külső szolgáltatókkal, hogy a folyamatos működéshez szükséges követelmények teljesíthetők legyenek.

Magyarázat

Az érintett szervezetnek szorosan együtt kell működnie a releváns külső szolgáltatókkal, hogy biztosítsa az EIR folyamatos működését. Ez magában foglalja a vészhelyzeti tervekben, így az üzletmenet-folytonossági tervben szereplő követelmények megértését és azoknak a külső szolgáltatók által történő teljesítését. Az érintett szervezetnek biztosítania kell, hogy a külső szolgáltatók megértsék és teljesítsék az EIR működéséhez szükséges követelményeket.

A követelmény alkalmazásának lépései

1. A szervezetnek először fel kell mérnie, mely üzletmenet-folytonossági feladatok függenek külső szolgáltatóktól. Ez magában foglalhatja az EIR-eket, a kommunikációs csatornákat, a logisztikai támogatást és más, a működéshez szükséges szolgáltatásokat.
2. Meg kell határozni a külső szolgáltatókkal szemben támasztott követelményeket, beleértve az EIR-ek rendelkezésre állását, a válaszidőket, a helyreállítási célokat és más, a folyamatos működéshez szükséges tényezőket.
3. Össze kell hangolni a szervezet üzletmenet-folytonossági tervét a külső szolgáltatókkal. Ez magában foglalhatja a közös gyakorlatokat, a dokumentálási folyamatokat és a rendszeres tesztelést, hogy biztosítsák az EIR-ek és a szolgáltatások rendelkezésre állását a vészhelyzetek során.
4. Felül kell vizsgálni és frissíteni kell az üzletmenet-folytonossági tervet, hogy biztosítva legyen a külső szolgáltatókkal való összhang és a folyamatos működéshez szükséges követelmények teljesítése.
5. A szervezetnek biztosítania kell, hogy a külső szolgáltatók is megfeleljenek a kiberbiztonsági követelményeknek, és képesek legyenek fenntartani az EIR-ek biztonságát és rendelkezésre állását a vészhelyzetek során. Ez magában foglalhatja a szolgáltatók naplózását, a biztonsági események kezelését és a helyreállítási tervek tesztelését.

Kapcsolódó intézkedések

16.49. Külső elektronikus információs rendszerek szolgáltatásai

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

CP-2(7)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

7.9. Üzletmenet-folytonossági terv – Kritikus erőforrások meghatározása

7.9. A szervezet meghatározza az összes szervezet működése szempontjából kritikus erőforrást, amelyek az alapfeladatok vagy az alapvető üzleti folyamatok működéséhez szükségesek.

Magyarázat

Az érintett szervezetnek meg kell határozni az alapfeladatok, ill. alapfunkciók működéséhez szükséges kritikus erőforrásokat. Erre a szervezeteknek lehetőségük van önálló, kritikussági szint meghatározására irányuló elemzés keretében, vagy az üzletmenet-folytonossági tervezés, ill. az üzleti hatáselemzések részeként. Ahhoz, hogy az érintett szervezet alapfeladatai és alapfunkciói a vészhelyzeti műveletek során is folytatódhassanak, a kritikus erőforrások meghatározása elengedhetetlen. A kritikus információs erőforrások azonosítása megkönnyíti továbbá az érintett szervezeti erőforrások prioritizálását. A kritikus erőforrások technikai és működési aspektusokat is tartalmaznak. A technikai aspektusok közé tartoznak a rendszerelemek, az információs technológiai szolgáltatások, az információs technológiai termékek és mechanizmusok. A működési aspektusok közé tartoznak az eljárások (azaz a manuálisan végrehajtott műveletek) és a személyzet (azaz azok a személyek, akik technikai ellenőrzéseket működtetnek és/vagy manuális eljárásokat hajtanak végre).

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia az összes kritikus erőforrást, amelyek az alapfeladatok vagy az alapvető funkciók működéséhez szükségesek. Ez magában foglalhatja az önálló, kritikussági szint meghatározására irányuló elemzést, az üzletmenet-folytonossági tervezést vagy az üzleti hatáselemzést.
2. Azonosítani kell az EIR kritikus eszközeit, hogy további ellenőrzéseket lehessen alkalmazni annak biztosítása érdekében, hogy az érintett szervezet alapfeladatai és üzleti funkciói a vészhelyzeti műveletek során is folytatódhassanak.
3. Prioritást kell adni az erőforrásoknak az EIR kritikus eszközeinek azonosítása révén. Az EIR kritikus eszközei magukban foglalják a technikai és működési szempontokat. A technikai szempontok közé tartoznak a rendszerelemek, az informatikai szolgáltatások, az informatikai

termékek és mechanizmusok. A működési szempontok közé tartoznak az eljárások (azaz a manuálisan végrehajtott műveletek) és a személyzet (azaz azok a személyek, akik működtetik a technikai ellenőrzéseket és/vagy végrehajtják a manuális eljárásokat).

4. Dokumentálni szükséges az összes lépést, amelyet a kritikus erőforrások azonosítása érdekében tettek, hogy biztosítva legyen a folyamat átláthatósága és ellenőrizhetősége.

Kapcsolódó intézkedések

6.36. Rendszerelem leltár

15.21. Rendszerelemek kritikusságának elemzése

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

3.1.4.2. Üzletmenet-folytonossági terv informatikai erőforrás kiesésekre

ISO/IEC 27001:2023 referencia

A.5.30

NIST SP 800-53 rev.5 referencia

CP-2(8)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

7.10. A FOLYAMATOS MŰKÖDÉSRE FELKÉSZÍTŐ KÉPZÉS

7.10. A szervezet:

7.10.1. Az EIR felhasználói számára szerepkörüknek vagy felelősségi körüknek megfelelő folyamatos működésre felkészítő képzést tart:

7.10.1.1. szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül;

7.10.1.2. amikor az EIR változásai ezt szükségessé teszik;

7.10.1.3. a szervezet által meghatározott gyakorisággal.

7.10.2. Meghatározott gyakorisággal vagy meghatározott eseményeket követően felülvizsgálja és frissíti a folyamatos működésre felkészítő képzés tartalmát.

MAGYARÁZAT

A folyamatos működésre felkészítő képzést az érintett szervezet a személyzet szerepkörének és felelősségi körének megfelelően szervezi meg, hogy a képzés tartalma és részletessége megfelelő legyen. Például, néhány személynek csak azt kell tudnia, hogy mikor és hol jelentkezzenek munkavégzésre a folyamatos működés ideje alatt, és hogy a normál feladataikat érinti-e ez. Az EIR adminisztrátoroknak további képzésre lehet szükségük arra vonatkozóan, hogyan hozzanak létre rendszereket alternatív feldolgozási és tárolási helyeken, hogyan működtessék megfelelően a kijelölt rendszereket. A vészhelyzeti tervezésben érintett további munkavállalók, vezetők pedig részletesebb képzést kaphatnak arról, hogyan végezzék el a létfontosságú feladatokat kijelölt helyszíneken, és hogyan létesítsenek kommunikációt más szervezetekkel, külső felekkel a folyamatos működéssel kapcsolatos tevékenységek koordinálása érdekében. A képzések tartalmát rendszeresen, ill. a szervezet által meghatározott események mentén felül kell vizsgálni és aktualizálni szükséges.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek folyamatos működésre felkészítő képzést kell biztosítania az EIR felhasználói számára, amely képzés a felhasználók szerepkörének vagy felelősségi körének megfelelő.
2. A képzést a szerepkörbe vagy felelősségbe kerülésüket követő meghatározott időn belül kell elvégezni.
3. Amikor az EIR változásai ezt szükségessé teszik, a képzést frissíteni kell.
4. A képzést az érintett szervezet által meghatározott gyakorisággal kell elvégezni.

5. A szervezetnek meghatározott gyakorisággal vagy meghatározott eseményeket követően felül kell vizsgálnia és frissítenie a folyamatos működésre felkészítő képzés tartalmát.

Kapcsolódó intézkedések

3.2. Biztonságtudatossági képzés

3.9. Szerepkör alapú biztonsági képzés

3.13. A biztonsági képzésre vonatkozó dokumentációk

7.2. Üzletmenet-folytonossági terv

7.13. Üzletmenet-folytonossági terv tesztelése

7.29. Telekommunikációs szolgáltatások

9.2. Képzés a biztonsági események kezelésére

9.9.1. Biztonsági események kezelése

9.35. Információszivárgásra adott válaszlépések

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

3.1.4.3. A folyamatos működésre felkészítő képzés

ISO/IEC 27001:2023 referencia

A.6.3

NIST SP 800-53 rev.5 referencia

CP-3

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

7.11. A FOLYAMATOS MŰKÖDÉSRE FELKÉSZÍTŐ KÉPZÉS – SZIMULÁLT ESEMÉNYEK

7.11. A szervezet a folyamatos működésre felkészítő képzésben szimulált eseményeket alkalmaz, hogy elősegítse a személyzet hatékony reagálását a szervezet működése szempontjából kritikus helyzetekben.

MAGYARÁZAT

Az érintett szervezet által alkalmazott szimulált események olyan környezetet teremtenek, ahol a munkavállalók valós fenyegető eseményeket tapasztalhatnak meg, beleértve például a kibertámadásokat, a szervezeti adatokat titkosító zsarolóvírus támadásokat, vagy a hardver- vagy szoftverhibákat, vagy éppen a fizikai biztonsági fenyegetéseket. Ezek a szimulált események lehetővé teszik a munkavállalók számára, hogy gyakorolják és fejlesszék a válaszreakcióikat, és felkészüljenek a valós helyzetekre. Az alkalmazott szimulált események segítenek a munkavállalóknak megérteni, hogy milyen lépéseket kell tenniük egy adott helyzetben, és hogyan kell reagálniuk a különböző fenyegetésekre. Ez magában foglalja a helyes eljárásokat, a kommunikációt, a döntéshozatalt is. A szimulációs tesztelés segít továbbá a szervezetnek a biztonsági eseménykezelési tervben foglaltak tesztelésében, így a végrehajtott szimulációt követően javasolt annak frissítése is, amennyiben indokolt. A szimulált események segítenek felismerni a fenyegetéseket, megérteni a kockázatokat, és megtanulni, hogyan kell hatékonyan reagálni és kezelni az EIR-t érintő fenyegetéseket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy folyamatos működésre felkészítő képzési programot, amely magában foglalja a szimulált eseményeket. Ez a program lehetővé teszi a munkavállalók számára, hogy valós fenyegetési eseményeket tapasztaljanak meg.
2. A szimulációs tesztek végrehajtásánál törekedni kell arra, hogy a tesztelés kontrolláltan, a vonatkozó szabályzatokkal (pl.: biztonsági eseménykezelési terv) összhangban történjen, és ne veszélyeztesse a szervezet működési folyamatait.
3. A szervezetnek rendszeresen ellenőriznie kell a képzési program hatékonyságát, és dokumentálnia kell a képzési eseményeket és a személyzet reakcióit. Ez lehetővé teszi, hogy a

szervezet azonosítsa a képzési programban, szabályozási környezetben esetlegesen felmerülő hiányosságokat és javító intézkedéseket hajtson végre.

4. A szervezetnek biztosítania kell, hogy a munkavállalók rendszeresen részt vegyenek a képzési programban, és a szervezet naprakész legyen a legújabb fenyegetésekkel és a megfelelő reagálási stratégiákkal kapcsolatban.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.1.4.3. A folyamatos működésre felkészítő képzés

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-3(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

7.12. A FOLYAMATOS MŰKÖDÉSRE FELKÉSZÍTŐ KÉPZÉS – A KÉPZÉSI KÖRNYEZETBEN HASZNÁLT MECHANIZMUSOK

7.12. A szervezet valós működési mechanizmusokat alkalmaz, hogy ezáltal alaposabb és valósághűbb vészhelyzeti képzési környezetet biztosítson.

MAGYARÁZAT

A működési mechanizmusok olyan folyamatokra utalnak, amelyeket egy szervezeti cél elérése érdekében hoztak létre, vagy egy olyan rendszerre, amely egy adott szervezeti alapfeladatot vagy alapfunkciót támogat. A tényleges alapfeladatok és alapfunkciók, valamint EIR-ek és/vagy létesítmények felhasználhatók szimulált események létrehozására és a szimulált események realitásának fokozására a rendkívüli helyzetekre vonatkozó felkészítés során. A szervezetnek valós működési mechanizmusokat kell alkalmaznia, hogy a munkavállalók minél valósághűbb környezetben készülhessenek fel a krízishelyzetekre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a működési mechanizmusokat, amelyeket alkalmazni kíván a képzései során, beleértve az alkalmazott rendszereket és fizikai helyszíneket egyaránt.
2. A szervezetnek ezután meg kell határoznia, hogy melyik valós folyamatokat, EIR-t és/vagy létesítményeket fogja használni a szimulált események generálásához és a szimulált események valóságtartalmának fokozásához a vészhelyzeti képzés során.
3. A szervezetnek meg kell terveznie és végre kell hajtania a szimulált eseményeket.
4. A szervezetnek dokumentálnia kell a szimulált eseményeket és a vészhelyzeti képzések végrehajtását.
5. A szervezetnek értékelnie kell a vészhelyzeti képzést és a szimulált eseményeket. Ez magában foglalja a vészhelyzeti képzés és a szimulált események hatékonyságának értékelését, valamint a működési mechanizmusok és az EIR továbbfejlesztését a vészhelyzeti képzés és a szimulált események hatékonyságának növelése érdekében.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-3(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

7.13. ÜZLETMENET-FOLYTONOSSÁGI TERV TESZTELÉSE

7.13. A szervezet:

7.13.1. meghatározott gyakorisággal és meghatározott teszteken keresztül vizsgálja az EIR-re vonatkozó üzletmenet-folytonossági tervet a terv hatékonyságának és a szervezet felkészültségének felmérése céljából; értékeli az üzletmenet-folytonossági terv tesztelési eredményeit;

7.13.2. felülvizsgálja az üzletmenet-folytonossági terv tesztelési eredményeit;

7.13.3. a felülvizsgálat eredményei alapján, szükség esetén javítja a tervet.

MAGYARÁZAT

Az üzletmenet-folytonossági terv hatékonyságának és az érintett szervezet felkészültségének felmérésére szolgáló tesztelési módszerek közé tartoznak a ellenőrzőlisták, a különböző gyakorlatok, a szimulációk. Az érintett szervezetek a vészhelyzeti tervekben meghatározott követelmények alapján hajtják végre a tesztelést, beleértve a vészhelyzeti műveleteknek a szervezeti működésre, eszközökre és személyekre gyakorolt hatásainak meghatározását.

Az üzletmenet-folytonossági terv tesztelési eredményeinek értékelése során elemezni kell a tesztelés során kapott adatokat, hogy megállapítsák a terv hatékonyságát és az esetleges hiányosságokat. Ez magában foglalja a tesztelési eredmények dokumentálását, amelyet később fel lehet használni a terv továbbfejlesztésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a tesztelési gyakoriságot és a tesztek típusát, amelyeken keresztül vizsgálni fogja az EIR-re vonatkozó üzletmenet-folytonossági tervet.

2. A szervezet - a tesztelés megfelelő végrehajtását követően - értékeli az üzletmenet-folytonossági terv tesztelési eredményeit. Ez magában foglalja a terv hatékonyságának és a szervezet felkészültségének felmérését.

3. Felül kell vizsgálni az üzletmenet-folytonossági terv tesztelési eredményeit. Ez magában foglalja a tervben talált esetleges gyengeségek azonosítását és a szükséges változtatások meghatározását.

4. A felülvizsgálat eredményei alapján, szükség esetén javítani szükséges a tervet. Ez magában foglalhatja a tervben talált gyengeségek kijavítását és a terv hatékonyságának növelését.

5. Végül dokumentálni szükséges a tesztelési eredményeket és a tervben végrehajtott változtatásokat. Ez lehetővé teszi a szervezet számára, hogy nyomon kövesse a terv fejlődését és hatékonyságát.

Kapcsolódó intézkedések

3.9. Szerepkör alapú biztonsági képzés

7.2. Üzletmenet-folytonossági terv

7.10. A folyamatos működésre felkészítő képzés

7.29. Telekommunikációs szolgáltatások

7.35. Az elektronikus információs rendszer mentései

9.5. Biztonsági események kezelésének tesztelése

9.9.1. Biztonsági események kezelése

13.2. Rendszerbiztonsági terv

1.15. Tesztelés, képzés és felügyelet

19.2. Ellátási láncra vonatkozó kockázatkezelési szabályzat

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

3.1.4.4. Az üzletmenet-folytonossági terv tesztelése

ISO/IEC 27001:2023 referencia

A.5.29; A.5.30

NIST SP 800-53 rev.5 referencia

CP-4

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

7.14. Üzletmenet-folytonossági terv tesztelése – Összehangolás a kapcsolódó tervekkel

7.14. A szervezet egyezteti az üzletmenet-folytonossági terv tesztelését a kapcsolódó tervekért felelős szervezeti egységekkel.

Magyarázat

A vészhelyzeti tervezési tervek közé tartoznak például az üzletmenet-folytonossági tervek, a katasztrófa utáni helyreállítási tervek, a működésfolytonossági tervek, a válságkommunikációs tervek, a kritikus infrastruktúra-tervek, és a biztonsági eseménykezelési tervek. Az üzletmenet-folytonossági tervet mind a készítési, mind a tesztelési fázisaiban egyeztetni szükséges a releváns kapcsolódó tervekért felelős szervezeti egységekkel. Az üzletmenet-folytonossági terv tesztelését a tesztelés megindítása előtt szükséges egyeztetni.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia azokat a terveket, amelyek kapcsolódnak az EIR üzletmenet-folytonossági tervéhez. Ezek a tervek lehetnek például a katasztrófa utáni helyreállítási tervek, a biztonsági eseménykezelési tervek, a működésfolytonossági tervek, a válságkommunikációs tervek, a kritikus infrastruktúra tervek, és a kiberbiztonsági esemény-reagálási tervek.
2. A szervezetnek egyeztetnie kell a kapcsolódó tervekért felelős szervezeti egységekkel a kiberbiztonsági követelményeknek való megfelelés érdekében. Ez magában foglalja a tesztelési folyamatok, a naplózás és dokumentáció, valamint a vészhelyzeti eljárások koordinálását.
3. A szervezetnek biztosítania kell, hogy a tesztelési folyamatok összhangban legyenek a kapcsolódó tervekkel, és hogy ezek a tervek megfeleljenek a kiberbiztonsági követelményeknek.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a terveket, hogy biztosítsa azok relevanciáját és hatékonyságát. Ez magában foglalja a kapcsolódó tervekért felelős szervezeti egységekkel való egyeztetést is.
5. A szervezetnek dokumentálnia kell a tesztelési folyamatokat és az eredményeket, hogy bizonyítékot szolgáltasson a követelményeknek való megfelelésről.

Kapcsolódó intézkedések

9.34. Biztonsági eseménykezelési terv

1.9. A szervezet működése szempontjából kritikus infrastruktúra biztonsági terve

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

3.1.4.4. Az üzletmenet-folytonossági terv tesztelése

ISO/IEC 27001:2023 referencia

A.5.30

NIST SP 800-53 rev.5 referencia

CP-4(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

7.15. ÜZLETMENET-FOLYTONOSSÁGI TERV TESZTELÉSE – ALTERNATÍV FELDOLGOZÁSI HELYSZÍN

7.15. A szervezet teszteli az üzletmenet folytonossági tervet az alternatív feldolgozási helyszínen:

7.15.1. a vészhelyzeti személyzetnek a létesítménnyel és az elérhető erőforrásokkal való megismertetése érdekében; és

7.15.2. az alternatív feldolgozási helyszín képességeinek értékelése és a vészhelyzeti műveletek támogatása céljából.

MAGYARÁZAT

Az alternatív feldolgozási helyszín körülményei jelentősen eltérhetnek az elsődleges helyszín körülményeitől. Az alternatív helyszín meglátogatása és a helyszínen rendelkezésre álló tényleges képességek megismerése értékes információkat nyújthat a potenciális sebezhetőségekről, amelyek befolyásolhatják az érintett szervezet üzleti funkcióit. A helyszíni látogatás lehetőséget adhat a vészhelyzeti tervek, így az üzletmenet-folytonossági terv finomítására a tesztelés során felfedezett sebezhetőségek kezelése érdekében.

A szervezetnek tesztelnie kell az üzletmenet-folytonossági tervet az alternatív feldolgozási helyszínen. Ez magában foglalja a vészhelyzeti személyzet megismertetését a létesítménnyel és az elérhető erőforrásokkal. Ez nem csak a személyzet felkészültségét növeli, hanem lehetővé teszi, hogy a személyzet jobban megértse az EIR működését és a helyszínen rendelkezésre álló erőforrásokat.

Ezenkívül az érintett szervezetnek értékelnie kell az alternatív feldolgozási helyszín képességeit és a vészhelyzeti műveletek támogatását. Ez magában foglalja az EIR teljesítményének, kapacitásának és megbízhatóságának értékelését, valamint a helyszínen rendelkezésre álló erőforrások, például az energiaellátás, a hűtés és a fizikai biztonság értékelését.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell terveznie és elő kell készítenie a tesztelési folyamatot. Ez magában foglalja a tesztelési forgatókönyv kidolgozását, a tesztelési időpontok meghatározását, valamint a tesztelésben részt vevő személyek kiválasztását és felkészítését.

2. A szervezetnek biztosítania kell, hogy a vészhelyzeti személyzet megismerkedjen az alternatív feldolgozási helyszínnel és annak erőforrásaival. Ez magában foglalhatja a helyszínen történő bejárásokat, a rendelkezésre álló EIR bemutatását, valamint a helyszínen elérhető egyéb erőforrások ismertetését.
3. A szervezetnek értékelnie kell az alternatív feldolgozási helyszín képességeit. Ez magában foglalja az EIR teljesítményének, megbízhatóságának és biztonságának értékelését, valamint a helyszín fizikai biztonságának felmérését.
4. A szervezetnek tesztelnie kell a vészhelyzeti műveleteket az alternatív feldolgozási helyszínen. Ez magában foglalja a vészhelyzeti eljárások gyakorlását, a vészhelyzeti személyzet feladatainak és felelősségeinek tesztelését, valamint a vészhelyzeti kommunikációs rendszerek működésének ellenőrzését.
5. A szervezetnek dokumentálnia szükséges a tesztelési folyamat eredményeit, beleértve a felmerült problémákat és az azokra adott válaszokat. A dokumentáció segíthet a szervezetnek a tesztelési folyamat eredményeinek értékelésében, az üzletmenet-folytonossági terv finomításában, valamint a jövőbeli tesztelések tervezésében.
6. A szervezetnek felül kell vizsgálnia és frissítenie kell a vészhelyzeti tervet a tesztelési folyamat során szerzett tapasztalatok alapján.

Kapcsolódó intézkedések

7.23. Alternatív feldolgozási helyszín

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

3.1.4.4. Az üzletmenet-folytonossági terv tesztelése

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CP-4(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

7.16. ÜZLETMENET-FOLYTONOSSÁGI TERV TESZTELÉSE – AUTOMATIZÁLT TESZTELÉS

7.16. A szervezet meghatározott automatizált mechanizmusok segítségével teszteli az üzletmenet-folytonossági tervet.

MAGYARÁZAT

Az érintett szervezet olyan automatizált mechanizmusokat kell alkalmazzon, amelyek segítenek az üzletmenet-folytonossági terv tesztelésében. Ezek a mechanizmusok képesek kell legyenek a terv minden aspektusát átfogóan tesztelni, beleértve a különböző vészhelyzeti forgatókönyveket és a különböző üzleti funkciókat. Az automatizált mechanizmusok használata lehetővé teszi, hogy az érintett szervezet realisztikus környezetben tesztelje az üzletmenet-folytonossági tervet. Ez azt jelenti, hogy az EIR valós terhelés alatt kerül tesztelésre, ami segít felmérni, hogy az EIR hogyan reagál a valós vészhelyzetekre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia egy üzletmenet-folytonossági tervet, amely részletesen leírja, hogy milyen lépéseket kell tenniük különböző kiberbiztonsági események esetén.
2. A szervezetnek be kell szereznie a megfelelő automatizált mechanizmusokat, amelyek segítségével tesztelhető az üzletmenet-folytonossági terv. Ezek a mechanizmusok lehetnek például szoftverek, amelyek képesek szimulálni különböző kiberbiztonsági támadásokat és biztonsági eseményeket.
3. A szervezetnek rendszeresen, előre meghatározott időközönként tesztelnie kell az üzletmenet-folytonossági tervet az automatizált mechanizmusok segítségével. A tesztelés során az EIR-t és a támogatott üzleti funkciókat is meg kell terhelniük, hogy valós körülmények között lássák, hogyan reagál az EIR. A tesztelés során a szakfelügyelet biztosítása elengedhetetlen.
4. A szervezetnek naplót kell vezetnie a tesztelések eredményeiről, hogy nyomon követhető legyen, melyik teszt milyen eredményt hozott, és hogy szükség esetén módosíthassák az üzletmenet-folytonossági tervet.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az üzletmenet-folytonossági tervet, hogy az mindig naprakész legyen és megfeleljen a követelményeknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-4(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

7.17. Üzletmenet-folytonossági terv tesztelése – Teljes helyreállítás és rekonstrukció

7.17. Az üzletmenet-folytonossági terv tesztelésének részét képezi a rendszer teljes és az utolsó ismert állapotba történő helyreállítása.

Magyarázat

Az üzletmenet-folytonossági terv tesztelése során az érintett szervezeteknek biztosítaniuk kell, hogy képesek legyenek visszaállítani az EIR-t a teljes, utolsó ismert állapotába. A szervezetnek gondoskodnia kell arról, hogy az üzletmenet-folytonossági tesztelés részét képezze az EIR teljes visszaállítása az utolsó ismert állapotba. A rendszer visszaállítási idejének összhangban kell lennie a tervekben meghatározott helyreállítási időcélokkal (RTO, RPO). A tesztelés során az érintett szervezeteknek értékelniük kell a helyreállítási eljárásaik hatékonyságát, és szükség esetén módosítaniuk kell a tervet a jövőbeni helyreállítási műveletek optimalizálása érdekében.

A követelmény alkalmazásának lépései

1. A szervezetnek létre kell hoznia egy üzletmenet-folytonossági tervet, vagy ahhoz kapcsolódóan egy katasztrófa utáni helyreállítási tervet, amelynek célja az szervezeti alapfunkciók és üzleti funkciók helyreállítása. Ez magában foglalja a különböző tevékenységek végrehajtását, amelyek segítenek a szervezetnek visszatérni a normál működési állapotba.
2. A szervezetnek a teszt során végre kell hajtania a teljes működési állapot visszaállítását az EIR vonatkozásában, beleértve a hardver, a szoftverprogramok és az adatok állapotinformációit is.
3. A szervezetnek meg kell őriznie az EIR állapotinformációit, hogy megkönnyítse az EIR újraindítását és a szervezet normál működési módjába való visszatérését, minimális zavarokkal az alapfeladatok és az alapfunkciók számára.
4. A szervezetnek rendszeresen tesztelnie kell az üzletmenet-folytonossági tervet, hogy biztosítsa, hogy képes lesz helyreállítani az EIR-t a legutóbb ismert állapotba, ha szükséges.
5. A szervezetnek dokumentálnia kell a tesztelést, hogy nyomon követhesse a helyreállítási folyamatot és az esetleges problémákat. A dokumentáció segíthet az érintett szervezetnek azonosítani a potenciális problémákat és megoldásokat találni rájuk.

Kapcsolódó intézkedések

7.43. Az elektronikus információs rendszer helyreállítása és újraindítása

17.77. Ismert állapot való meghibásodás

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

CP-4(4)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

7.18. ÜZLETMENET-FOLYTONOSSÁGI TERV TESZTELÉSE – ÖNTESZTELÉS

7.18. A szervezet meghatározott mechanizmusokat alkalmaz az EIR vagy rendszerelem működésének zavarására és hátrányos befolyásolására.

MAGYARÁZAT

Gyakran a legjobb módszer az EIR ellenálló képességének értékelésére, ha valamilyen módon zavarják az EIR működését. Az érintett szervezet által alkalmazott mechanizmusok számos módon zavarhatják az EIR funkcióit vagy szolgáltatásait, beleértve a kritikus rendszerelemek megszüntetését vagy letiltását, a rendszerelemek konfigurációjának megváltoztatását, a kritikus funkcionalitás akadályoztatását vagy a jogosultságok megváltoztatását. Az automatizált, folyamatos és szimulált kibertámadások és szolgáltatási zavarok felfedhetik a váratlan funkcionális függőségeket, és segíthetnek a növelni a szervezet kiberbiztonsági rezilienciáját egy valódi kibertámadás esetén.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet először határozza meg azokat a mechanizmusokat, amelyeket az EIR vagy rendszerelem működésének zavarására és hátrányos befolyásolására kíván alkalmazni. Ezek a mechanizmusok számos módon zavarhatják az EIR funkcióit vagy szolgáltatásait, beleértve a kritikus rendszerelemek megszüntetését vagy letiltását, a rendszerelemek konfigurációjának megváltoztatását, a kritikus funkcionalitás akadályozását vagy a jogosultságok megváltoztatását.
2. A szervezet alkalmazza ezeket a mechanizmusokat az EIR zavarására. Ez lehet automatizált, folyamatos, vagy szimulált kibertámadás és szolgáltatás zavarás.
3. A szervezet naplózza és elemzi az EIR reakcióit és teljesítményét a zavarások alatt. Ez segíthet feltárni a váratlan funkcionális függőségeket.
4. A szervezet végül értékeli és frissíti a mechanizmusokat és stratégiákat az EIR zavarására és hátrányos befolyásolására, a naplózott eredmények és tapasztalatok alapján.

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

CP-4(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a mechanizmusok illetve a rendszer vagy rendszerelem meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

7.19. BIZTONSÁGI TÁROLÁSI HELYSZÍN

7.19. A szervezet:

7.19.1. létrehoz egy biztonsági tárolási helyszínt, beleértve a szükséges megállapodásokat, a rendszer biztonsági mentési információinak tárolásához és visszakereséséhez;

7.19.2. biztosítja, hogy a biztonsági tárolási helyszín ugyanolyan szintű védelmi intézkedéseket biztosítson, mint az elsődleges helyszín.

MAGYARÁZAT

A biztonsági tárolási helyszínek földrajzilag elkülönülnek az elsődleges tárolóhelyektől, az információk és adatok másolatát biztosítják, ha az elsődleges tárolóhely nem elérhető. Hasonlóképpen, az alternatív feldolgozási helyszínek esetén, amik lehetőséget biztosítanak, arra az esetre, ha az elsődleges feldolgozási helyszín nem állna rendelkezésre. A földrajzilag elosztott architektúrák, amelyek megfelelnek az üzletmenet folytonossági követelményeket, biztonsági tároló helyszínnek is tekinthetők. A biztonsági tároló helyszínekre vonatkozó megállapodásoknak hasonló biztonsági követelményeknek kell megfelelniük, mint az elsődleges tároló helyszíneknek, így ki kell térnie a megállapodásnak többek között a biztonsági helyszín lokációjának környezetére, a rendszerekhez és létesítményekhez való hozzáférés szabályaira, a fizikai és környezeti biztonsági követelményekre, valamint a biztonsági másolatokat tartalmazó adathordozók átadásának és visszavételének koordinálása. A biztonsági tároló helyszínek tükrözik az üzletmeneti folytonossági tervekben foglalt követelményeket, hogy a szervezetek a szervezeti rendszerek kompromittálódása, meghibásodása vagy megszakadása ellenére is fenn tudják tartani az alapvető ügymeneti és üzleti funkciókat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az érintett szervezet hozzon létre egy biztonsági tárolási helyszínt, amely földrajzilag különbözik az elsődleges tárolási helyszíntől, és képes a duplikált információk és adatok tárolására, ha az elsődleges tárolási helyszín nem érhető el.
2. Az érintett szervezet biztosítson alternatív feldolgozási helyszíneket, amelyek feldolgozási képességet biztosítanak, ha az elsődleges feldolgozási helyszín nem érhető el.
3. Az érintett szervezet fontolja meg a földrajzilag elosztott architektúrákat, amelyek támogatják a vészhelyzeti követelményeket, mint alternatív tárolási helyszíneket.

4. Az érintett szervezet kössön megállapodásokat az alternatív tárolási helyszínekkel, amelyek tartalmazzák a helyszínek környezeti feltételeit, az EIR és létesítmények hozzáférési szabályait, a fizikai és környezeti védelmi követelményeket, valamint a biztonsági mentési adathordozók szállításának és visszakeresésének koordinációját.
5. Az érintett szervezet biztosítsa, hogy az alternatív tárolási helyszínek tükrözzék a vészhelyzeti tervek követelményeit, így az érintett szervezet képes fenntartani az alapvető küldetési és üzleti funkciókat, annak ellenére, hogy az EIR-ben kompromittálódás, hiba vagy zavar lép fel.
6. Az érintett szervezet biztosítsa, hogy az alternatív tárolási helyszín ugyanolyan szintű védelmi intézkedéseket biztosítson, mint az elsődleges helyszín.

Kapcsolódó intézkedések

7.2. Üzletmenet-folytonossági terv
7.23. Alternatív feldolgozási helyszín
7.29. Telekommunikációs szolgáltatások
7.35. Az elektronikus információs rendszer mentései
7.43. Az elektronikus információs rendszer helyreállítása és újraindítása
11.4. Adathordozók tárolása
11.6. Adathordozók szállítása
12.6. A fizikai belépés ellenőrzése
17.102. Elosztott feldolgozás és tárolás
18.68. Előrelátható meghibásodás megelőzése

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

3.1.4.5. Biztonsági tárolási helyszín

ISO/IEC 27001:2023 referencia

A.5.29; A.7.5; A.8.14

NIST SP 800-53 rev.5 referencia

CP-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

7.20. Biztonsági tárolási helyszín – Elkülönítés az elsődleges tárolási helyszíntől

7.20. A szervezet megfelelően elkülöníti a biztonsági tárolási helyszínt az elsődleges tárolási helyszíntől, az azonos veszélyeknek való kitettségük csökkentése érdekében.

Magyarázat

Az érintett szervezet a kockázatértékelésekben meghatározza azokat a fenyegetéseket, amelyek a biztonságos tárolási helyszínt érintik, ideértve a természeti katasztrófákat, szerkezeti hibákat, ellenséges támadásokat és a mulasztásokból vagy elkövetésekkel kapcsolatos hibákat. A szervezet meghatározza, hogy mi számít elegendő elkülönítésnek az elsődleges és az alternatív tárolóhelyek között, a fenyegetések típusától függően. Olyan fenyegetések esetén, mint az ellenséges támadások, a helyszínek közötti elkülönítés mértéke kevésbé releváns.

Az EIR tárolóhelyek elkülönítése kritikus fontosságú a kiberbiztonság szempontjából. A szervezetnek biztosítania kell, hogy az EIR elsődleges tárolóhelye megfelelően elkülönüljön a biztonsági tárolóhelytől. Ez azt jelenti, hogy a két helyszínnek nem szabad azonos fenyegetéseknek kitettnek lennie, hogy minimalizálják a potenciális kockázatokat. Például, ha mind az elsődleges, mind a biztonsági tárolóhely ugyanazon a földrajzi területen található, akkor mindkettő ugyanannak a természeti katasztrófának lehet kitéve, vagy ha mindkét telephely ugyanazon az áram betápláson keresztül jut energiához, adott kiesés esetén mindkét telephely érintett, így ez komoly kockázatot jelenthet az EIR számára.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia a kockázatértékelésben azokat a fenyegetéseket, amelyek a biztonságos tárolási helyszínt érintik. Ezek a fenyegetések magukban foglalhatják a természeti katasztrófákat, a szerkezeti hibákat, az ellenséges támadásokat és a mulasztásokból vagy egyéb cselekményekből eredő hibákat.
2. A szervezetnek meg kell határoznia, hogy mi számít elegendő elkülönítésnek az elsődleges és az alternatív tárolási helyszínek között, figyelembe véve a releváns fenyegetéseket. Például ellenséges támadások esetén a helyszínek közötti elkülönítés mértéke kevésbé releváns.

3. A szervezetnek úgy kell megterveznie és implementálnia az EIR-t, hogy az megfelelően elkülönítse a biztonsági tárolási helyszínt az elsődleges tárolási helyszíntől. Ez magában foglalhatja a fizikai elkülönítést, a hálózati elkülönítést, vagy akár a különböző szolgáltatók használatát is.

KAPCSOLÓDÓ INTÉZKEDÉSEK

15.4. Kockázatértékelés

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

3.1.4.5. Biztonsági tárolási helyszín

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-6(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

7.21. BIZTONSÁGI TÁROLÁSI HELYSZÍN – HELYREÁLLÍTÁSI IDŐ ÉS HELYREÁLLÍTÁSI PONT CÉLJAI

7.21. A szervezet a biztonsági tárolási helyszínt úgy konfigurálja, hogy az elősegítse a helyreállítási tevékenységeket, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

MAGYARÁZAT

Az érintett szervezetek a vészhelyzeti tervezés részeként meghatározzák a helyreállítási időt és a helyreállítási pontokat. A biztonsági tárolási helyszín konfigurációja magában foglalja a fizikai létesítményeket és az EIR-t, amelyek támogatják a helyreállítási műveleteket, és biztosítják azok hozzáférhetőségét és helyes végrehajtását.

Az EIR konfigurációjának megfelelő beállítása elengedhetetlen a helyreállítási célok eléréséhez. Ez magában foglalja a megfelelő adatbiztonsági protokollok, hálózati beállítások és rendszerfelügyeleti eszközök használatát, amelyek mind hozzájárulnak a helyreállítási folyamatok hatékonyságához és megbízhatóságához.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet először határozza meg a helyreállítási időt és a helyreállítási pontokat, mint a vészhelyzeti tervezés részét.
2. A szervezetnek konfigurálnia kell a biztonsági tárolási helyszínt. Ez magában foglalja a fizikai létesítményeket és az EIR-t, amelyek támogatják a helyreállítási műveleteket.
3. A szervezetnek biztosítania kell, hogy az EIR hozzáférhető legyen és helyesen működjön a helyreállítási tevékenységek során.
4. A szervezetnek ellenőriznie kell, hogy az EIR konfigurációja összhangban van-e a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.
5. A szervezetnek naplót kell vezetnie a helyreállítási tevékenységekről, beleértve az EIR konfigurációjának változásait is.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a helyreállítási terveket és az EIR konfigurációját, hogy biztosítsa a követelményeknek való megfelelést.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.1.4.5. Biztonsági tárolási helyszín

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CP-6(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

7.22. Biztonsági tárolási helyszín – Hozzáférhetőség

7.22. A szervezet azonosítja a potenciális hozzáférési problémákat a biztonsági tárolási helyszínhez egy meghatározott területre kiterjedő zavar vagy katasztrófa esetére és ezek alapján konkrét kockázatcsökkentő intézkedéseket határoz meg.

Magyarázat

Területi zavarok alatt olyan zavarok értendők, amelyek széles földrajzi körben jelentkezhetnek. A konkrét kockázatcsökkentő intézkedések közé tartozik a biztonsági mentési információk másolása más alternatív, biztonsági tárolási helyszínekre, ha hozzáférési problémák merülnek fel az eredetileg kijelölt biztonsági tárolási helyszíneken, vagy fizikai hozzáférési terv készítése a biztonsági mentési információkhoz, ha a biztonsági tárolási helyszín elektronikus hozzáférhetősége megszakad.

A katasztrófák esetében a szervezetnek előre meg kell határoznia a potenciális hozzáférési problémákat a biztonsági tárolási helyszín vonatkozásában. Ez magában foglalhatja a hozzáférési útvonalak, a hozzáférési jogosultságok, a hozzáférési idők és a hozzáférési módszerek értékelését. A szervezetnek dokumentálnia kell a hozzáférési problémák megoldására tett lépéseket, és rendszeresen felül kell vizsgálnia és frissítenie kell ezeket, hogy biztosítsa az EIR folyamatos biztonságát és hozzáférhetőségét krízishelyzetek esetén is.

A követelmény alkalmazásának lépései

1. A szervezet először azonosítsa a potenciális hozzáférési problémákat a biztonsági tárolási helyszínhez egy meghatározott területre kiterjedő zavar vagy katasztrófa esetére. Ez magában foglalhatja a hozzáférési útvonalak, a kommunikációs csatornák és az EIR hozzáférési pontjainak vizsgálatát.
2. A szervezet végezzen kockázatelemzést, hogy meghatározza a potenciális hozzáférési problémák valószínűségét és hatását. Ez magában foglalhatja a különböző zavarok és katasztrófák, például természeti katasztrófák, ember okozta katasztrófák és technológiai hibák elemzését.

3. A szervezet határozzon meg konkrét kockázatcsökkentő intézkedéseket a potenciális hozzáférési problémák kezelésére.
4. A szervezet hajtson végre felülvizsgálatot a kockázatcsökkentő intézkedések hatékonyságának értékelésére. Ez magában foglalhatja a hozzáférési problémák előfordulásának nyomon követését, a kockázatcsökkentő intézkedések hatékonyságának értékelését és a szükséges módosítások végrehajtását.
5. A szervezet biztosítsa a folyamatos képzést és tudatosságot a hozzáférési problémák kezelésére és a kockázatcsökkentő intézkedések alkalmazására. Ez magában foglalhatja a munkavállalók képzését a hozzáférési problémák felismerésére és kezelésére, valamint a kockázatcsökkentő intézkedések alkalmazására.

Kapcsolódó intézkedések

15.4. Kockázatértékelés

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

3.1.4.5. Biztonsági tárolási helyszín

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CP-6(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

7.23. ALTERNATÍV FELDOLGOZÁSI HELYSZÍN

7.23. A szervezet:

7.23.1. Kijelöl egy alternatív feldolgozási helyszínt azért, hogy ha az elsődleges feldolgozási képesség nem áll rendelkezésre, az EIR előre meghatározott műveleteit, előre meghatározott időn belül - összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal - az alternatív helyszínen újrakezdhesse, vagy folytathassa.

7.23.2. Gondoskodik arról, hogy a működés újrakezdéséhez, vagy folytatásához szükséges eszközök és feltételek az alternatív feldolgozási helyszínen, vagy meghatározott időn belül rendelkezésre álljanak, akár külső szervezettel kötött szerződések által biztosítva.

7.23.3. Biztosítja, hogy az alternatív feldolgozási helyszín védelmi intézkedései egyenértékűek legyenek az elsődleges helyszínen alkalmazottakkal.

MAGYARÁZAT

A tartalék feldolgozási helyszínek földrajzilag elkülönülnek az elsődleges feldolgozási helyektől, és biztosítják a feldolgozási képességet abban az esetben, ha az elsődleges feldolgozási helyszín nem elérhető. A tartalék feldolgozási képesség megoldható fizikai feldolgozási helyszín vagy egyéb alternatívák segítségével, például egy felhőalapú szolgáltatóhoz vagy más, belső vagy külső feldolgozási szolgáltatáshoz való átállással. A földrajzilag elosztott kialakítás, amely megfelel a vészhelyzeti követelményeknek, szintén tartalék feldolgozási helynek tekinthető. A tartalék feldolgozási helyszínekre vonatkozó szerződésekben meghatározott intézkedések tartalmazzák a tartalék helyszín környezeti feltételeit, a hozzáférési szabályokat, a fizikai és környezeti követelményeket, valamint a személyzet áthelyezésének és beosztásának koordinálását. A tartalék feldolgozás helyszínekre vonatkozó követelmények tükrözik az vészhelyzeti tervekben szereplő követelményeket, a szervezet célok és alapfunkciók fenntartása érdekében, a rendszerek zavarának, kompromittálódásának vagy meghibásodásának ellenére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az érintett szervezetnek ki kell jelölnie egy alternatív feldolgozási helyszínt, amely földrajzilag különbözik az elsődleges feldolgozási helyszíntől. Ez a helyszín biztosítja a feldolgozási képességet, ha az elsődleges helyszín nem áll rendelkezésre.

2. Az alternatív feldolgozási képesség biztosítása lehet fizikai helyszín vagy más alternatívák, mint például a feladatok átvétele egy felhő alapú szolgáltatóhoz, vagy más belső vagy külső feldolgozási szolgáltatáshoz.

3. Az érintett szervezetnek gondoskodnia kell arról, hogy az alternatív feldolgozási helyszínen, vagy meghatározott időn belül rendelkezésre álljanak a működés újrakezdéséhez, vagy folytatásához szükséges eszközök és feltételek, akár külső szervezettel kötött szerződések által biztosítva.

4. Az alternatív feldolgozási helyszínen alkalmazott védelmi intézkedéseknek egyenértékűeknek kell lenniük az elsődleges helyszínen alkalmazottakkal. Ez magában foglalja az alternatív helyszínek környezeti feltételeit, hozzáférési szabályokat, fizikai és környezetvédelmi követelményeket, valamint a személyzet átadásának és kijelölésének koordinációját.

5. Az érintett szervezetnek követelményeket kell meghatároznia az alternatív feldolgozási helyszínek számára, amelyek tükrözik a vészhelyzeti tervekben foglalt követelményeket, hogy fenntartsák az alapvető alapfeladatokat és üzleti funkciókat, annak ellenére, hogy zavar, kompromittálás vagy hiba lép fel az EIR-ben.

Kapcsolódó intézkedések

7.2. Üzletmenet-folytonossági terv

7.19. Biztonsági tárolási helyszín

7.29. Telekommunikációs szolgáltatások

7.35. Az elektronikus információs rendszer mentései

7.43. Az elektronikus információs rendszer helyreállítása és újraindítása

10.21. Kellő időben történő karbantartás

12.6. A fizikai belépés ellenőrzése

12.28. Vészhelyzeti tápellátás

12.31. Vészvilágítás

12.43. Munkavégzésre kijelölt alternatív helyszín

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

3.1.4.6. Tartalék feldolgozási helyszín

ISO/IEC 27001:2023 REFERENCIA

A.5.29; A.7.5; A.8.14

NIST SP 800-53 REV.5 REFERENCIA

CP-7

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

7.24. Alternatív feldolgozási helyszín – Elkülönítés az elsődleges helyszíntől

7.24. A szervezet olyan alternatív feldolgozási helyszínt jelöl ki, amely megfelelően elkülönül az elsődleges feldolgozási helyszíntől, az azonos fenyegetésekkel szembeni kitettség csökkentése érdekében.

Magyarázat

A fenyegetések, amelyek az alternatív feldolgozási helyszíneket érintik, az érintett szervezet kockázatértékeléseiben kerülnek meghatározásra, és magukban foglalják a természeti katasztrófákat, szerkezeti hibákat, ellenséges támadásokat és a mulasztásokból adódó hibákat. A szervezetek meghatározzák, hogy mi számít elegendő elkülönülésnek az elsődleges és az alternatív feldolgozási helyszínek között a számukra aggodalomra okot adó fenyegetések alapján. Olyan fenyegetések esetén, mint az ellenséges támadások, a helyszínek közötti elkülönülés kevésbé releváns.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a kockázatértékelés során azokat a fenyegetéseket, amelyek az alternatív feldolgozási helyszínt érinthetik. Ezek a fenyegetések magukban foglalhatják a természeti katasztrófákat, a szerkezeti hibákat, a támadásokat és a mulasztásokból vagy elkövetésekkel kapcsolatos hibákat.
2. A szervezetnek meg kell határoznia, hogy mi számít elegendő elkülönülésnek az elsődleges és az alternatív feldolgozási helyszínek között, figyelembe véve a releváns fenyegetéseket. Például, ha a fenyegetések között szerepelnek támadások, akkor az elkülönülés mértéke kevésbé releváns.
3. A szervezetnek ki kell jelölnie az alternatív feldolgozási helyszínt, amely megfelelően elkülönül az elsődleges helyszíntől.
4. A szervezetnek biztosítania kell, hogy az EIR megfelelően működjön az alternatív feldolgozási helyszínen, és képes legyen kezelni az azonos fenyegetéseket.

5. A szervezetnek dokumentációt kell vezetnie az alternatív feldolgozási helyszínen történő tevékenységekről, hogy nyomon követhető legyen az EIR működése és a fenyegetések kezelése.

Kapcsolódó intézkedések

15.4. Kockázatértékelés

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

3.1.4.6. Tartalék feldolgozási helyszín

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CP-7(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

7.25. ALTERNATÍV FELDOLGOZÁSI HELYSZÍN – HOZZÁFÉRHETŐSÉG

7.25. A szervezet azonosítja a potenciális hozzáférési problémákat az alternatív feldolgozási helyszínhez egy meghatározott területre kiterjedő zavar vagy katasztrófa esetére és ezek alapján konkrét kockázatcsökkentő intézkedéseket határoz meg.

MAGYARÁZAT

A területi zavarok vagy katasztrófák olyan események, amelyek befolyásolhatják az EIR hozzáférését és működését az alternatív feldolgozási helyszínen. Például természeti katasztrófák, mint az árvizek, földrengések, tűzvészek, vagy ember által okozott események, mint a terrorcselekmények, háborúk vagy nagyobb technológiai hibák. A szervezetnek azonosítania kell a potenciális hozzáférési problémákat, amelyek ilyen zavarok vagy katasztrófák esetén felmerülhetnek. Ez magában foglalja a hozzáférési útvonalak, az infrastruktúra, az energiaellátás, a kommunikációs hálózatok és az EIR működésének potenciális akadályait vagy korlátait. A szervezetnek konkrét kockázatcsökkentő intézkedéseket kell meghatároznia ezekre a problémákra. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kockázatcsökkentő intézkedéseket, hogy biztosítsa az EIR folyamatos működését és hozzáférhetőségét minden körülmények között.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell a potenciális hozzáférési problémákat az alternatív feldolgozási helyszín vonatkozásában egy meghatározott területre kiterjedő zavar vagy katasztrófa esetére. Ez magában foglalhatja a hálózati hozzáférési problémákat, a fizikai hozzáférési korlátozásokat, vagy a szükséges infrastruktúra hiányát.
2. A szervezetnek értékelnie kell a kockázatokat, amelyeket ezek a hozzáférési problémák jelentenek az EIR számára. Ez magában foglalhatja a kritikus adatok elvesztését, a szolgáltatások leállását, vagy a biztonsági eseményeket.
3. A szervezetnek meg kell határoznia a kockázatcsökkentő intézkedéseket, amelyeket ezekre a hozzáférési problémákra alkalmaznak. Ez magában foglalhatja a redundáns hálózati

kapcsolatok létrehozását, a fizikai hozzáférési pontok biztonságának növelését vagy az alternatív feldolgozási helyszínek létrehozását.

4. A szervezetnek implementálnia kell ezeket a kockázatcsökkentő intézkedéseket, és naplózni kell azokat, hogy bizonyíték legyen a megfelelősségről.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kockázatcsökkentő intézkedéseket, hogy biztosítsa az EIR folyamatos védelmét a területre kiterjedő zavarokkal szemben.

Kapcsolódó intézkedések

15.4. Kockázatértékelés

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

3.1.4.6. Tartalék feldolgozási helyszín

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CP-7(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

7.26. ALTERNATÍV FELDOLGOZÁSI HELYSZÍN – SZOLGÁLATÁS PRIORITÁSA

7.26. A szervezet az alternatív feldolgozási helyszínre vonatkozóan olyan megállapodásokat köt, és olyan intézkedéseket vezet be, amelyek a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási időcélokkal) összhangban álló szolgáltatásprioritási rendelkezéseket tartalmaznak.

MAGYARÁZAT

A szolgáltatásprioritási megállapodások olyan megállapodásokra utalnak, amelyek biztosítják, hogy az érintett szervezet olyan prioritást élvez, amely összhangban van a rendelkezésre állási követelményeivel és az információforrások rendelkezésre állásával a logikai alternatív feldolgozási és/vagy a fizikai alternatív feldolgozási helyszínen. A szervezetek helyreállítási időcélokat állapítanak meg a vészhelyzeti tervezés részeként.

A szervezet az EIR-re vonatkozó prioritási megállapodásokat köt a szolgáltatókkal, hogy biztosítsa annak prioritásait a szervezet rendelkezésre állási követelményeivel összhangban. Ezek az EIR megállapodások tartalmazzák a logikai alternatív feldolgozási helyszínek és a fizikai alternatív feldolgozási helyszínek információforrásainak rendelkezésre állását is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a rendelkezésre állási követelményeit és a helyreállítási időcélokat. Ezek a követelmények és célok alapján határozzák meg, hogy milyen prioritású szolgáltatásokra van szükségük az alternatív feldolgozási helyszínen.
2. A szervezetnek meg kell kötnie megállapodásokat a szolgáltatókkal, amelyek biztosítják, hogy az EIR rendelkezésre állási követelményeinek megfelelő prioritású szolgáltatásokat kapnak. Ezek a megállapodások tartalmazzák a szolgáltatásprioritási rendelkezéseket.
3. A szervezetnek be kell vezetnie azokat az intézkedéseket, amelyek biztosítják, hogy az alternatív feldolgozási helyszínen a szolgáltatásprioritási rendelkezések betartásra kerülnek. Ezek az intézkedések magukban foglalhatják a szolgáltatók teljesítményének naplózását és értékelését, valamint a szolgáltatásprioritási rendelkezések betartásának ellenőrzését.

4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a szolgáltatásprioritási megállapodásokat és intézkedéseket, hogy biztosítsa, hogy azok továbbra is összhangban vannak az EIR rendelkezésre állási követelményeivel és a helyreállítási időcélokkal.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.1.4.6. Tartalék feldolgozási helyszín

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CP-7(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

7.27. Alternatív feldolgozási helyszín – használatra való felkészítés

7.27. A szervezet úgy készíti fel az alternatív feldolgozási helyszínt, hogy az meghatározott időn belül készen álljon az alapfunkciók működésének támogatására.

Magyarázat

A helyszín előkészítése magában foglalja a konfigurációs beállítások létrehozását az alternatív feldolgozási helyszínen - az EIR vonatkozásában. Az alternatív feldolgozási helyszín és az ott lévő EIR-ek konfigurációja összhangban kell legyen az elsődleges helyszínnel, és a vonatkozó követelményekkel. A szervezetnek gondoskodnia kell arról, hogy az alternatív helyszín megfelelően fel legyen készítve a kritikus funkciók támogatására a meghatározott időn belül. Ez magában foglalja az EIR konfigurációjának beállítását, a szükséges hardverek és szoftverek telepítését, valamint a hálózati kapcsolatok és a biztonsági intézkedések meglétét. A szervezetnek biztosítania kell, hogy az alternatív feldolgozási helyszín rendelkezzen a szükséges erőforrásokkal és képességekkel az alapvető funkciók zavartalan működéséhez. A szervezetnek dokumentációt kell vezetnie az alternatív helyszín előkészítéséről, beleértve a végrehajtott tevékenységeket, az esetleges problémákat és a megoldásokat. Ez lehetővé teszi a szervezet számára, hogy nyomon kövesse a folyamatot, értékelje a teljesítményt és szükség esetén módosítsa a terveket. Az alternatív helyszín előkészítése során a szervezetnek figyelembe kell vennie a különböző kockázati tényezőket, beleértve a természeti katasztrófákat, a szabotázst és a kiberbiztonsági fenyegetéseket. A szervezetnek megfelelő biztonsági intézkedéseket kell hoznia ezeknek a kockázatoknak a kezelésére, és rendszeresen felül kell vizsgálnia és frissítenie a biztonsági protokollokat.

A követelmény alkalmazásának lépései

1. A szervezet kijelöli az alternatív feldolgozási helyszínt, amelyet fel kell készíteni az alapfunkciók támogatására.
2. A szervezetnek meg kell határoznia az EIR konfigurációs beállításait az alternatív feldolgozási helyszínen, összhangban a fő helyszínen szükséges beállításokkal.

3. A szervezetnek biztosítania kell, hogy az alapvető eszközök és a meghatározott erőforrások rendelkezésre álljanak az alternatív feldolgozási helyszínen.
4. A szervezetnek tesztelnie kell az alternatív feldolgozási helyszínt, hogy biztosítsa, hogy az képes lesz támogatni az EIR alapfunkcióit a meghatározott időn belül.
5. A szervezetnek dokumentálnia kell a felkészülési folyamatot, beleértve a tesztelési eredményeket és az esetleges problémákat, hogy szükség esetén vissza lehessen követni és javítani lehessen a folyamatot.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az alternatív feldolgozási helyszín felkészülési tervét, hogy biztosítsa, hogy az mindig naprakész legyen és készen álljon a használatra.

Kapcsolódó intézkedések

6.2. Alapkonfiguráció
6.23. Konfigurációs beállítások
7.13. Üzletmenet-folytonossági terv tesztelése

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

3.1.4.6. Tartalék feldolgozási helyszín

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CP-7(4)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

7.28. Alternatív feldolgozási helyszín – Az elsődleges helyszínre való visszatérés akadályoztatása

7.28. A szervezet tervet készít és felkészül azokra a körülményekre, amikor nem lehetséges a visszatérés az elsődleges feldolgozási helyszínre.

Magyarázat

Előfordulhatnak olyan helyzetek, amelyek megakadályozzák a szervezetet abban, hogy visszatérjen az elsődleges feldolgozási helyszínre, például, ha egy természeti katasztrófa megrongálta vagy elpusztította a létesítményt. A szervezetnek tervet kell készítenie és fel kell készülnie ezekre a körülményekre. Ez a terv magában foglalhatja a másodlagos feldolgozási helyszínek használatát, az adatok biztonságos tárolását és visszaállítását, valamint a működés folytonosságának biztosítását. Az EIR-nek képesnek kell lennie az adatok biztonságos tárolására és visszaállítására, valamint a működés folytonosságának biztosítására a másodlagos feldolgozási helyszínen, amennyiben nem lehetséges a visszatérés az elsődleges feldolgozási helyszínre, vagy a szervezet úgy dönt, hogy nem tér vissza arra.

A követelmény alkalmazásának lépései

1. A szervezetnek fel kell ismernie és értékelnie kell a különböző kockázatokat és fenyegetéseket, amelyek megakadályozhatják a visszatérést az elsődleges feldolgozási helyszínre. Ez magában foglalhatja a természeti katasztrófákat, mint például árvíz vagy hurrikán, de technológiai hibákat és emberi hibákat is.
2. A szervezetnek ki kell dolgoznia egy tervet, amely leírja, hogyan kezelik ezeket a helyzeteket. Ez a terv magában foglalhatja a másodlagos feldolgozási helyszínek használatát, az adatok biztonságos tárolását és visszaállítását, valamint a működés folytatását a rendkívüli helyzetek idején.
3. A szervezetnek tesztelnie kell a tervet, hogy biztosítsa annak hatékonyságát, továbbá azt, hogy a másodlagos feldolgozási helyszín alkalmas a hosszú távú működés biztosítására, amennyiben a szervezet nem tér vissza az elsődleges feldolgozási helyszínre.

4. A szervezetnek dokumentálnia szükséges a tesztelési eredményeket és a terv végrehajtását, hogy bizonyítékot szolgáltasson a követelményeknek való megfelelésről.
5. A szervezetnek folyamatosan felül kell vizsgálnia és frissítenie kell a kapcsolódó tervet, hogy az naprakész legyen és megfeleljen a változó körülményeknek és fenyegetéseknek.

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

CP-7(6)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

7.29. TELEKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK

7.29. A szervezet tartalék infokommunikációs szolgáltatásokat létesít. Erre vonatkozóan olyan megállapodásokat köt, amelyek lehetővé teszik az EIR alapfunkcióinak, vagy meghatározott műveleteinek számára azok meghatározott időtartamon belüli újrakezdését, ha az elsődleges infokommunikációs kapacitás nem áll rendelkezésre sem az elsődleges, sem a tartalék feldolgozási vagy tárolási helyszínen.

MAGYARÁZAT

Az alkalmazott alternatív infokommunikációs szolgáltatásoknak összhangban kell lenniük a vészhelyzeti tervekben foglalt üzletmenet-folytonossági követelményekkel, melyek célja az alapfeladatok és alapfunkciók fenntartása az elsődleges infokommunikációs szolgáltatások elvesztése esetén. Az alternatív infokommunikációs szolgáltatások használata további szervezeti vagy kereskedelmi megoldások vagy műholdas kommunikáció használatát foglalja magában. A szervezetnek érvényesítenie kell az alternatív szolgáltatásokra vonatkozó megállapodásaiban az üzletmenet-folytonossági követelményeit.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek tartalék infokommunikációs szolgáltatásokat kell létrehoznia, amelyek magukban foglalják az adat- és hangszolgáltatásokat az elsődleges és alternatív feldolgozási és tárolási helyszínek számára.
2. A szervezetnek meg kell határoznia az üzletmenet-folytonossági tervekben szereplő, vonatkozó követelményeket, hogy fenntartsák az alapvető működési és üzleti funkciókat az elsődleges infokommunikációs szolgáltatások elvesztése esetén.
3. A szervezetnek érvényesítenie kell az alternatív szolgáltatásokra vonatkozó megállapodásaiban az üzletmenet-folytonossági követelményeit, figyelembe kell vennie olyan tényezőket, mint a rendelkezésre állás, a szolgáltatás minősége és a hozzáférés, amikor alternatív infokommunikációs megállapodásokat köt.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.2. Üzletmenet-folytonossági terv

7.19. Biztonsági tárolási helyszín

7.23. Alternatív feldolgozási helyszín

7.47. Alternatív kommunikációs protokollok

17.17. A határok védelme

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

3.1.4.7. Infokommunikációs szolgáltatások

ISO/IEC 27001:2023 REFERENCIA

A.5.29; A.7.11

NIST SP 800-53 REV.5 REFERENCIA

CP-8

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

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

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

7.30. TELEKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK – SZOLGÁLTATÁSPRIORITÁSI RENDELKEZÉSEK

7.30. Amennyiben A szervezet által igénybe vett elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására szerződés keretében kerül sor, akkor annak tartalmaznia kell a szolgáltatásprioritási rendelkezéseket, összhangban a szervezet rendelkezésre állási követelményeivel (köztük a helyreállítási időcélokkal).

MAGYARÁZAT

Az érintett szervezetnek gondoskodnia kell arról, hogy az elsődleges és a tartalék infokommunikációs szolgáltatások nyújtására vonatkozó szerződéseik tartalmazzák a szolgáltatásprioritási rendelkezéseket. Ezeknek a rendelkezéseknek összhangban kell lenniük az érintett szervezet rendelkezésre állási követelményeivel, beleértve a helyreállítási időcélokat is. Mivel az EIR rendelkezésre állása kritikus fontosságú az érintett szervezet számára ezért a szolgáltatásprioritási rendelkezéseknek ezt tükrözniük kell.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia az elsődleges és a tartalék infokommunikációs szolgáltatásokat, amelyeket igénybe vesz.
2. A szervezetnek szerződést kell kötnie az infokommunikációs szolgáltatóval, amely tartalmazza a szolgáltatásprioritási rendelkezéseket.
3. A szerződésnek összhangban kell lennie az érintett szervezet rendelkezésre állási követelményeivel, beleértve a helyreállítási időcélokat is.
4. A szervezetnek biztosítania kell, hogy a szolgáltató képes legyen teljesíteni ezeket a követelményeket, és rendelkezzen a szükséges erőforrásokkal és kapacitással.
5. A szervezetnek rendszeresen ellenőriznie kell a szolgáltató teljesítményét, és dokumentálnia kell a szolgáltatás minőségét és a rendelkezésre állást.
6. Ha a szolgáltató nem tudja teljesíteni a szerződésben foglaltakat, a szervezetnek intézkedéseket kell tennie, például másik szolgáltatót kell keresnie.
7. A szervezetnek biztosítania kell, hogy a szolgáltató is betartja a kiberbiztonsági követelményeket, és megfelelő védelmet nyújt az EIR számára.

8. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a szerződést a változó követelmények és körülmények alapján.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.1.4.7. Infokommunikációs szolgáltatások

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-8(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

7.31. TELEKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK – KRITIKUS MEGHIBÁSODÁSI PONT

7.31. A szervezet olyan tartalék infokommunikációs szolgáltatásokat vesz igénybe, amelyek csökkentik az elsődleges infokommunikációs szolgáltatásokkal közös hibalehetőségek valószínűségét.

MAGYARÁZAT

Az érintett szervezet számára fontos, hogy a tartalék infokommunikációs szolgáltatásokat olyan szolgáltatóktól szerezze be, akik nem ugyanazt a fizikai vonalat használják. Ez azért fontos, mert ha az elsődleges és a tartalék szolgáltatások ugyanazt a fizikai vonalat használják, akkor azzal megnő a közös hibalehetőségek (un. single-point-of-failure) kockázata.

Például, ha egy fizikai vonal meghibásodik, akkor mind az elsődleges, mind a tartalék szolgáltatások megszakadhatnak, ami komoly kockázatot jelent az EIR számára. Ezért az érintett szervezetnek biztosítania kell, hogy a tartalék infokommunikációs szolgáltatások fizikailag különböző vonalakon működjenek.

Ezenkívül fontos a szolgáltatói átláthatóság a tényleges fizikai átviteli képesség tekintetében. Az érintett szervezetnek tisztában kell lennie azzal, hogy milyen fizikai infrastruktúrát használnak a szolgáltatók, és hogy ez milyen hatással van az EIR-re. Az érintett szervezetnek a dokumentációiban rögzítenie kell az összes releváns információt, beleértve a szolgáltatók által használt fizikai vonalakat és azok állapotát, hogy képes legyen megfelelően kezelni a kockázatokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia az elsődleges infokommunikációs szolgáltatásokat, amelyekre támaszkodik a működése során.
2. A szervezetnek fel kell mérnie az elsődleges infokommunikációs szolgáltatások hibalehetőségeit, és meg kell határoznia, melyek azok a területek, ahol a hibák közös előfordulása a legvalószínűbb.
3. A szervezetnek meg kell keresnie azokat a tartalék infokommunikációs szolgáltatásokat, amelyek képesek csökkenteni az elsődleges szolgáltatásokkal közös hibalehetőségek

valószínűségét. Ez magában foglalhatja más szolgáltatók használatát, más technológiák alkalmazását vagy redundáns rendszerek létrehozását.

4. A szervezetnek be kell integrálnia ezeket a tartalék infokommunikációs szolgáltatásokat az EIR-be, és biztosítania kell, hogy ezek a szolgáltatások rendelkezésre állnak, ha az elsődleges szolgáltatások hibásodnak meg.

5. A szervezetnek rendszeresen dokumentálnia kell és felül kell vizsgálnia a tartalék infokommunikációs szolgáltatások állapotát és teljesítményét, hogy biztosítsa, hogy ezek a szolgáltatások megfelelően működnek és csökkentik a közös hibalehetőségek valószínűségét.

6. A szervezetnek folyamatosan felül kell vizsgálnia és frissítenie kell a tartalék infokommunikációs szolgáltatások stratégiáját, hogy biztosítsa, hogy az mindig megfelel az aktuális kockázatoknak és az EIR igényeinek.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.1.4.7. Infokommunikációs szolgáltatások

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CP-8(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

7.32. TELEKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK – ELSŐDLEGES ÉS MÁSODLAGOS SZOLGÁLTATÓK KÜLÖNVÁLASZTÁSA

7.32. A szervezet tartalék infokommunikációs szolgáltatásokat szerez be, nem csak az elsődleges szolgáltatóktól, hanem a tőlük elkülönült független szolgáltatóktól is, hogy csökkentse a szervezet azonos fenyegetéseknek való kitettségét.

MAGYARÁZAT

Az infokommunikációs szolgáltatásokat érintő fenyegetéseket az érintett szervezet kockázatértékeléseiben határozza meg, és ezek közé tartoznak a természeti katasztrófák, szerkezeti hibák, kiber vagy fizikai támadások, valamint a mulasztások vagy szándékos (szervezeten belüli) károkozás. Az érintett szervezetek csökkenthetik a közös sérülékenységeket azzal, hogy minimalizálják az infokommunikációs szolgáltatók közötti megosztott infrastruktúrát, és elegendő földrajzi elkülönítést érnek el a szolgáltatások között. Az érintett szervezetek megfontolhatják egyetlen szolgáltató használatát olyan helyzetekben, ahol a szolgáltató képes alternatív infokommunikációs szolgáltatásokat nyújtani, amelyek megfelelnek a kockázatértékelésben megfogalmazott elkülönítési igényeknek. Ez a megközelítés csökkenti az azonos fenyegetéseknek való kitettséget, mivel a különböző szolgáltatók általában különböző infrastruktúrákat és védelmi mechanizmusokat használnak, így egy adott fenyegetés, amely az egyik szolgáltatót érinti, nem feltétlenül érinti a többit. Ezenkívül a tartalék szolgáltatók használata lehetővé teszi az EIR gyors helyreállítását egy esetleges biztonsági esemény esetén.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek kockázatelemzést kell végeznie, amelyben meghatározza azokat a fenyegetéseket, amelyek az infokommunikációs szolgáltatásokat érintik. Ezek a fenyegetések magukban foglalhatják a természeti katasztrófákat, a strukturális hibákat, a kiber vagy fizikai támadásokat, valamint a mulasztásokból vagy szándékos (szervezeten belüli) károkozásból eredő hibákat.

2. A szervezet csökkenti a közös sérülékenységeket azzal, hogy olyan infokommunikációs szolgáltatók szolgáltatásait veszi igénybe, amelyek fizikailag elkülönült vonalakat és infrastruktúrát használnak, valamint földrajzilag megfelelően elkülönülnek egymástól.
3. A szervezet megfontolhatja egyetlen szolgáltató használatát olyan helyzetekben, ahol a szolgáltató képes alternatív infokommunikációs szolgáltatásokat nyújtani, amelyek megfelelnek a kockázatelemzésben megfogalmazott elválasztási igényeknek.
4. A szervezetnek tartalék infokommunikációs szolgáltatásokat kell beszereznie, nem csak az elsődleges szolgáltatóktól, hanem a tőlük elkülönült független szolgáltatóktól is.
5. A szervezetnek dokumentálnia kell a folyamatot, hogy nyomon követhesse a változásokat és a fejlesztéseket, valamint, hogy biztosítsa a kiberbiztonsági követelményeknek való megfelelést.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CP-8(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

7.33. TELEKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK – SZOLGÁLTATÓI ÜZLETMENET-FOLYTONOSSÁGI TERV

7.33. A szervezet:

7.33.1. Előírja, hogy az elsődleges és a tartalék infokommunikációs szolgáltatóknak rendelkezniük kell üzletmenet-folytonossági tervvel.

7.33.2. Felülvizsgálja a szolgáltatók üzletmenet-folytonossági terveit annak érdekében, hogy megfelelnek-e az általa meghatározott üzletmenet-folytonossági követelményeknek.

7.33.3. Meghatározott gyakorisággal bekéri a szolgáltatóktól a folyamatos működéssel kapcsolatos képzések és tesztelések dokumentációját.

MAGYARÁZAT

Bizonyos esetekben a szolgáltatói üzletmenet folytonossági tervek kivonata elegendő evidenciaként szolgálhat a szervezet számára a felülvizsgálati követelmények teljesítéséhez. Az infokommunikációs szolgálatók a Belügyminisztériummal, valamint a BM Országos Katasztrófavédelemmel egyeztetve részt vehetnek a katasztrófa utáni helyreállítási gyakorlatokban is. A szervezetek az ilyen típusú tevékenységeket felhasználhatják a szolgáltatói üzletmenet-folytonossági tervek felülvizsgálatával, tesztelésével és képzésével kapcsolatos követelmények teljesítése érdekében.

Az érintett szervezet előírja, hogy az elsődleges és a tartalék infokommunikációs szolgáltatóknak rendelkezniük kell üzletmenet-folytonossági tervvel. Ez a terv részletezi, hogy a szolgáltató hogyan kívánja biztosítani a szolgáltatások folyamatos működését váratlan események, például természeti katasztrófák vagy technikai hibák esetén.

Az érintett szervezet meghatározott gyakorisággal bekéri a szolgáltatóktól a folyamatos működéssel kapcsolatos képzések és tesztelések dokumentációját. Ez lehetővé teszi az érintett szervezet számára, hogy ellenőrizze, hogy a szolgáltatók megfelelően felkészültek-e a váratlan események kezelésére, és hogy a szolgáltatások folyamatosan működnek-e ilyen események esetén is. A dokumentáció felülvizsgálata során az érintett szervezet naplózhatja a szolgáltatók által végzett tevékenységeket, és szükség esetén visszajelzést adhat a szolgáltatóknak a további fejlesztések érdekében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek elő kell írnia, hogy az elsődleges és a tartalék infokommunikációs szolgáltatóknak rendelkezniük kell üzletmenet-folytonossági tervvel.
2. A szervezet felülvizsgálja a szolgáltatók üzletmenet-folytonossági terveit. Ez azt jelenti, hogy a szervezetnek meg kell vizsgálnia, hogy a szolgáltatók tervei megfelelnek-e az általa meghatározott üzletmenet-folytonossági követelményeknek. Ez magában foglalhatja a tervben szereplő lépések, stratégiák és eljárások értékelését.
3. A szervezet meghatározott gyakorisággal bekéri a szolgáltatóktól a folyamatos működéssel kapcsolatos képzések és tesztelések dokumentációját. Ez azt jelenti, hogy az érintett szervezetnek rendszeresen ellenőriznie kell, hogy a szolgáltatók megfelelően képzik-e a személyzetüket a folyamatos működés biztosítása érdekében, és rendszeresen tesztelik-e a rendszereiket.
4. Az érintett szervezetnek figyelembe kell vennie a szolgáltatók üzletmenet-folytonossági terveinek sajátosságait. Egyes esetekben a szolgáltatók tervének összefoglalása elegendő bizonyíték lehet az érintett szervezet számára a felülvizsgálati követelmény teljesítéséhez.
5. Az infokommunikációs szolgáltatók részt vehetnek folyamatos katasztrófa-helyreállítási gyakorlatokban is a Belügyminisztérium és az állami és helyi kormányzatok koordinációjában. A szervezet ezeket a tevékenységeket használhatja a szolgáltatók üzletmenet-folytonossági tervének felülvizsgálatával, tesztelésével és képzésével kapcsolatos bizonyítékok igénylésére.
6. A szervezetnek dokumentálnia kell a fent említett tevékenységeket, hogy bizonyítani tudja, hogy megfelel a kiberbiztonsági követelményeknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.10. A folyamatos működésre felkészítő képzés

7.13. Üzletmenet-folytonossági terv tesztelése

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

CP-8(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

7.34. TELEKOMMUNIKÁCIÓS SZOLGÁLTATÁSOK – MÁSODLAGOS TÁVKÖZLÉSI SZOLGÁLTATÁS TESZTELÉSE

7.34. A szervezet meghatározott gyakorisággal teszteli a tartalék infokommunikációs szolgáltatásokat.

MAGYARÁZAT

Az érintett szervezetnek rendszeresen ellenőriznie kell a tartalék infokommunikációs szolgáltatásokat, hogy biztosítsa azok megfelelő működését. Ez magában foglalja a szolgáltatások tesztelését, hogy megbizonyosodjon arról, hogy képesek helyettesíteni az elsődleges szolgáltatásokat, ha szükséges.

A tesztelés gyakorisága az érintett szervezet belső szabályaitól és a szolgáltatások kritikusságától függ. Például, ha egy szolgáltatás létfontosságú az érintett szervezet működése szempontjából, akkor annak tesztelése gyakrabban történhet meg.

A tesztelés során dokumentációval által nyomon követhető, hogy a tartalék infokommunikációs szolgáltatások megfelelően működnek-e. Ha a tesztelés során problémákat észlelnek, akkor azokat azonnal orvosolni kell, hogy az EIR zavartalanul működhessen.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a tartalék infokommunikációs szolgáltatásokat, amelyeket tesztelni szeretne. Ez magában foglalhatja a szervereket, hálózati eszközöket, szoftvereket és egyéb rendszerelemeket.
2. A szervezetnek meg kell határoznia a tesztelés gyakoriságát. Ez lehet heti, havi, negyedéves, félévente vagy évente, attól függően, hogy milyen gyakran szeretnék ellenőrizni a tartalék infokommunikációs szolgáltatások működését.
3. A szervezetnek létre kell hoznia egy tesztelési tervet, amely részletezi a tesztelési folyamatot, beleértve a tesztelendő rendszerelemeket, a tesztelés időpontjait, a tesztelési eljárásokat és a tesztelési eredmények értékelését.
4. A szervezetnek végrehajtania kell a tesztelési tervet a meghatározott időpontokban. Ez magában foglalhatja a tartalék infokommunikációs szolgáltatások működésének ellenőrzését, a hibák azonosítását és a hibák javítását.

5. A szervezetnek dokumentálnia kell a tesztelési eredményeket, beleértve a tesztelés időpontját, a tesztelési eredményeket, a hibákat és a hibák javítását. A dokumentáció segíthet az érintett szervezetnek nyomon követni a tartalék infokommunikációs szolgáltatások működését és javítani a kiberbiztonsági teljesítményt.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a tesztelési tervet, hogy biztosítsa a tartalék infokommunikációs szolgáltatások hatékony működését és a kiberbiztonsági követelményeknek való megfelelést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.10. A folyamatos működésre felkészítő 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

CP-8(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

7.35. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER MENTÉSEI

7.35. A szervezet:

7.35.1. Meghatározott gyakorisággal mentést készít az EIR-ben tárolt felhasználói szintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

7.35.2. Meghatározott gyakorisággal mentést készít az EIR-ben tárolt rendszerszintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

7.35.3. Meghatározott gyakorisággal mentést készít az EIR dokumentációjáról, beleértve a biztonságra vonatkozó információkat is, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

7.35.4. Megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a biztonsági tárolási helyszínen.

MAGYARÁZAT

Az EIR információk magukban foglalják az EIR állapotinformációkat, az operációs rendszert, a köztes szoftvert, az alkalmazásszoftvert és a licenceket. A felhasználói szintű információk olyan információkat is tartalmaznak, amelyek nem EIR információk. Az EIR biztonsági mentések sértetlenségének védelmére alkalmazott mechanizmusok közé tartoznak a digitális aláírások és a kriptográfiai hash-ek. Az EIR biztonsági mentések tükrözik a vészhelyzeti tervekben foglalt követelményeket, valamint az érintett szervezet egyéb követelményeit az információk biztonsági mentésével kapcsolatban.

Az EIR dokumentációja magában foglalja a biztonsági információkat is. Az érintett szervezet gondoskodik a mentett információk bizalmasságának, sértetlenségének és rendelkezésre állásának védelméről mind az elsődleges, mind a biztonsági tárolási helyszínen. A naplókban rögzítik az EIR-ben tárolt információk biztonsági mentésének gyakoriságát, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meghatározott gyakorisággal mentést kell készítenie az EIR-ben tárolt felhasználói szintű információkról. Ezek nem az EIR információk, szervezetenként eltérhet a felhasználóiként meghatározott információ.
2. Az szervezetnek meghatározott gyakorisággal mentést kell készítenie az EIR-ben tárolt rendszerszintű információkról. Ez magában foglalja a rendszer állapotára vonatkozó információkat, az operációs rendszer szoftvert, a köztes szoftvert, az alkalmazás szoftvert és a licenceket.
3. A szervezetnek meghatározott gyakorisággal mentést kell készítenie az EIR dokumentációjáról, beleértve a biztonságra vonatkozó információkat is.
4. A szervezetnek meg kell védenie a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását mind az elsődleges, mind a biztonsági tárolási helyszínen. A mentések sértetlenségének védelmére használt mechanizmusok közé tartoznak a digitális aláírások és a kriptográfiai hash-ek.
5. A szervezetnek biztosítania kell, hogy az EIR mentések tükrözzék a vészhelyzeti tervekben foglalt követelményeket, valamint az információk mentésére vonatkozó egyéb szervezeti követelményeket.
6. A szervezetnek tisztában kell lennie azzal, hogy vonatkozó törvények, végrehajtási rendeletek, irányelvek, szabályok, szabályzatok, szabványok és iránymutatások vonatkozhatnak rá, amelyek követelményeket támasztanak bizonyos információkkal (pl. személyes adatok, különleges személyes adatok) kapcsolatban. A szervezetnek be kell vonnia a szervezet vezető adatvédelmi tisztviselőjét és jogi tanácsadóját ezen követelmények helyes teljesítése érdekében.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.2. Üzletmenet-folytonossági terv

7.19. Biztonsági tárolási helyszín

7.43. Az elektronikus információs rendszer helyreállítása és újraindítása

11.4. Adathordozók tárolása

11.6. Adathordozók szállítása

17.40. Az adatátvitel bizalmassága és sértetlensége

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

18.13. Az EIR monitorozása

18.68. Előrelátható meghibásodás megelőzése

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

3.1.4.8. Az elektronikus információs rendszer mentései

ISO/IEC 27001:2023 REFERENCIA

A.5.29; A.5.33; A.8.13

NIST SP 800-53 REV.5 REFERENCIA

CP-9

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

7.36. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER MENTÉSEI – MEGBÍZHATÓSÁG ÉS SÉRTETLENSÉG TESZTELÉSE

7.36. A szervezet meghatározott gyakorisággal teszteli a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének garantálása érdekében.

MAGYARÁZAT

Az EIR információk magukban foglalják az EIR állapotinformációkat, az operációs rendszert, a köztes szoftvert, az alkalmazásszoftvert és a licenceket. A felhasználói szintű információk olyan információkat is tartalmaznak, amelyek nem EIR információk. A mentések sértetlenségének védelmére alkalmazott eljárások közé tartoznak a digitális aláírások és a kriptográfiai hash-ek. A mentések tükrözik a vészhelyzeti tervek követelményeit, valamint az mentésére vonatkozó egyéb szervezeti követelményeket. A szervezetekre vonatkozhatnak olyan törvények, végrehajtási rendeletek, rendeletek vagy irányelvek, amelyek meghatározott információk (pl. személyes adatok, különleges személyes adatok) további követelményeket írnak elő. A szervezetnek egyeztetnie kell az adatvédelmi és jogi felelőssel ezen követelményekkel kapcsolatban.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a tesztelés gyakoriságát. Ez a gyakoriság függ a szervezet adatbiztonsági kockázatának mértékétől és az adatok fontosságától.
2. A szervezetnek rendszeresen ellenőriznie kell a rendszerelemeit, ahol a mentett információk tárolásra kerülnek. Ez magában foglalja az EIR hardver- és szoftverelemeinek ellenőrzését, hogy biztosítsák azok megbízhatóságát.
3. A szervezetnek tesztelnie kell az információ visszaállítására használt műveleteket. Ez magában foglalja a visszaállítási folyamatok ellenőrzését, hogy biztosítsák, hogy azok megbízhatóan működnek.
4. A szervezetnek ellenőriznie kell az információ sértetlenségét. Ez magában foglalja a mentett információk ellenőrzését, hogy biztosítsák, hogy azok nem sérültek meg vagy változtak meg a mentés óta.

5. A szervezetnek dokumentálnia kell a tesztelési folyamatot. Ez magában foglalja a tesztelési eredmények rögzítését, hogy bizonyíték legyen a tesztelési folyamat megbízhatóságáról.
6. Az érintett szervezetnek független és szakosodott teszteket kell használnia az EIR megbízhatóságának minden aspektusára. Például a mentési fájlok véletlenszerű mintájának visszafejtése és szállítása az alternatív tárolóhelyről vagy mentési helyről, és az információ összehasonlítása az elsődleges feldolgozási helyen lévő ugyanazzal az információval, biztosíthatja a megbízhatóságot.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.13. Üzletmenet-folytonossági terv tesztelése

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

3.1.4.8. Az elektronikus információs rendszer mentései

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-9(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

7.37. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER MENTÉSEI – VISSZAÁLLÍTÁS TESZTELÉSE MINTAVÉTELLEL

7.37. A szervezet a helyreállítási terv tesztelésének részeként egy kiválasztott mintát használ a mentett információkból az EIR kiválasztott funkcióinak helyreállítása során.

MAGYARÁZAT

Az EIR információk magukban foglalják az EIR állapotinformációkat, az operációs rendszert, a köztes szoftvert, az alkalmazásszoftvert és a licenceket. A felhasználói szintű információk olyan információkat is tartalmaznak, amelyek nem EIR információk. A mentések sértetlenségének védelmére alkalmazott eljárások közé tartoznak a digitális aláírások és a kriptográfiai hash-ek. A mentések tükrözik a vészhelyzeti tervek követelményeit, valamint az mentésére vonatkozó egyéb szervezeti követelményeket. A szervezetekre vonatkozhatnak olyan törvények, végrehajtási rendeletek, rendeletek vagy irányelvek, amelyek meghatározott információk (pl. személyes adatok, különleges személyes adatok) további követelményeket írnak elő. A szervezetnek egyeztetnie kell az adatvédelmi és jogi felelőssel ezen követelményekkel kapcsolatban.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR funkciói helyreállíthatók és támogatni tudják a szervezeti alapfeladataikat.
2. A helyreállítási terv tesztelése során alaposan tesztelni kell a kiválasztott EIR funkciókat.
3. A teszteléshez a mentett információkból egy mintát vesznek, hogy meghatározzák, a funkciók az elvárt módon működnek-e.
4. A szervezet meghatározhatja a funkciók és a mentett információk mintaméretét.
5. A tesztelés eredményeit dokumentálni kell, hogy későbbi elemzésre és felülvizsgálatra kerülhessen sor.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.13. Üzletmenet-folytonossági terv tesztelése

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

3.1.4.8. Az elektronikus információs rendszer mentései

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-9(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

7.38. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER MENTÉSEI – KRITIKUS INFORMÁCIÓK ELKÜLÖNÍTETT TÁRHELYE

7.38. A szervezet az EIR szervezet működése szempontjából kritikus szoftvereinek és egyéb biztonsággal kapcsolatos információinak mentéseit az elsődleges feldolgozási helyszíntől elkülönített létesítményben vagy egy tűzbiztos tárolóban tárolja.

MAGYARÁZAT

Az elkülönített tárolás a kritikus információkra vonatkozik, függetlenül a biztonsági mentési adathordozó típusától. Az EIR kritikus szoftverei közé tartoznak az operációs rendszerek, a köztes szoftverek, a kriptográfiai kulcskezelő rendszerek és az behatolásérzékelő rendszerek. A biztonsággal kapcsolatos információk közé tartoznak az EIR hardver, szoftver és firmware komponenseinek leltárai. Az alternatív tárolóhelyek, beleértve a földrajzilag elosztott architektúrákat, az érintett szervezet számára külön tároló létesítményeket szolgáltatnak. Az érintett szervezetek alternatív tárolóhelyeken automatizált biztonsági mentési folyamatokat hajthatnak végre az elkülönített tárolás biztosítása érdekében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, melyek azok a szoftverek és információk, amelyek kritikusak az EIR működése szempontjából. Ide tartoznak az operációs rendszerek, köztes szoftverek, kriptográfiai kulcskezelő rendszerek és behatolásérzékelő rendszerek, valamint a hardver, szoftver és firmware elemek leltárai.
2. A szervezetnek biztosítania kell, hogy ezeknek a kritikus információknak a mentéseit elkülönített létesítményben vagy tűzbiztos tárolóban tárolja. Az elkülönített tárolás lehet automatizált biztonsági mentési folyamatok alkalmazása alternatív tárolóhelyeken, például adatközpontokban.
3. A szervezetnek figyelembe kell vennie a földrajzi elosztottságot is, amikor elkülönített tárolóhelyeket választ. Ez azt jelenti, hogy a különböző adatokat különböző helyeken kell tárolni, hogy minimalizálják a kockázatot, ha egy helyszín kompromittálódik.

4. A szervezetnek dokumentálnia kell a mentési folyamatot, hogy nyomon követhető legyen, mely adatokat mentették el, mikor és hol. Ez segít az adatvesztés esetén a helyreállításban, valamint a biztonsági események nyomon követésében és elemzésében.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.2. Alapkonfiguráció

6.23. Konfigurációs beállítások

6.36. Rendszerelem leltár

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

3.1.4.8. Az elektronikus információs rendszer mentései

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-9(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a működés szempontjából kritikus szoftverek és egyéb biztonsággal kapcsolatos információk meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

7.39. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER MENTÉSEI – ÁTVITEL MÁSODLAGOS TÁROLÁSI HELYSZÍNRE

7.39. A szervezet meghatározott adatátviteli sebességgel vagy meghatározott idő alatt, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal, átmásolja az EIR mentésének információit az alternatív tárolási helyszínre.

MAGYARÁZAT

Az EIR mentési információit elektronikusan vagy a tárolására szolgáló adathordozó fizikai szállításával lehet átvinni az alternatív tárolási helyszínre. Az átvitel módja függ az adatok mennyiségétől, a rendelkezésre álló sávszélességtől, az adatátviteli sebességtől és a helyreállítási időtől és a helyreállítási pontoktól.

Az érintett szervezetnek előre meg kell határoznia az adatátviteli sebességet, hogy összhangban legyen a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal. Például, ha a helyreállítási idő célja 24 óra, akkor az EIR-nek képesnek kell lennie arra, hogy az összes mentési információt 24 órán belül átmásolja az alternatív tárolási helyszínre.

.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a helyreállítási időt és a helyreállítási pontokat, amelyek meghatározzák, hogy mennyi idő alatt és milyen gyakran kell a mentéseket átmásolni az alternatív tárolási helyszínre.
2. A szervezetnek meg kell határoznia az adatátviteli sebességet, amelyet az EIR mentésének információinak átmásolására használnak. Ez a sebesség összhangban kell legyen a helyreállítási idővel és a helyreállítási pontokkal.
3. A szervezetnek ki kell választania egy alternatív tárolási helyszínt, ahova az EIR mentésének információit átmásolják. Ez a helyszín lehet egy másik fizikai helyszín, vagy egy felhő alapú tároló.
4. A szervezetnek be kell állítania az EIR mentésének információinak automatikus átmásolását az alternatív tárolási helyszínre a meghatározott adatátviteli sebességgel és a meghatározott időközönként.

5. A szervezetnek dokumentálnia kell kell az EIR mentésének információinak átmásolását, hogy nyomon követhető legyen a folyamat és biztosítható legyen a kiberbiztonsági követelményeknek való megfelelés.
6. Az érintett szervezetnek rendszeresen ellenőriznie kell az EIR mentésének információinak átmásolását, hogy biztosítsa a folyamat zavartalan működését és a helyreállítási idő és a helyreállítási pontok betartását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.23. Alternatív feldolgozási helyszín
11.3. Adathordozók címkézése
11.4. Adathordozók tárolása
11.6. Adathordozók szállítása

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

3.1.4.8. Az elektronikus információs rendszer mentései

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-9(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az a helyreállítási időre és a helyreállítási pontra vonatkozó célkitűzésekkel összhangban lévő időtartam és átviteli sebesség meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

7.40. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER MENTÉSEI – REDUNDÁNS MÁSODLAGOS RENDSZER

7.40. A szervezet az EIR biztonsági mentését egy másodlagos, redundáns rendszeren tárolja, amely az elsődleges EIR-től különálló helyen található, és információvesztés vagy működési zavarok nélkül állítható üzembe.

MAGYARÁZAT

A rendszerbiztonság és a működésfolytonosság fenntartására a legjobb megoldás, ha kettő vagy több redundáns rendszer létezik. Ezek az alternatív rendszerek tükrözik az elsődleges rendszer minden információját, beleértve az adatok másolását.

Ha ilyen típusú redundanciát alkalmaznak, és a két rendszer között kellő földrajzi távolság van, az is elképzelhető, hogy a másodlagos rendszer egy másik feldolgozási helyként is szolgálhat.

Ez a megközelítés számos előnnyel járhat. Megbízhatóbb lesz a működés, mivel ha az egyik rendszer leáll, a többi még mindig működőképes marad. A megfelelő folyamatokkal támogatott redundáns rendszerek csökkentik a szolgáltatáskiesést, mivel bármely probléma esetén azonnal átállhatnak a másodlagos rendszerre, ami jelentősen csökkenti a leállási időt. Mivel az információkat különböző helyeken tárolják, ez csökkenti az adatvesztés kockázatát. Mindegyik rendszer rendelkezik a teljes adatmásolattal, így az adatok helyreállítása egyszerű, ha bármelyik rendszer meghibásodik.

Egy ilyen rendszer megtervezése és fenntartása azonban költséges lehet, és szükséges hozzá a kapacitással, az adatátviteli sebességgel és az adatok szinkronizálásával kapcsolatos kérdések megoldása.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először létre kell hoznia egy másodlagos, redundáns EIR-t, amely tükrözi az elsődleges EIR-t, beleértve az információk replikációját is.
2. A szervezetnek biztosítania kell, hogy elegendő földrajzi távolság legyen az elsődleges és a másodlagos EIR között. Ez a távolság segít megelőzni, hogy egyetlen helyi biztonsági esemény mindkét rendszert érintse.

3. A szervezetnek rendszeresen tesztelnie kell a másodlagos EIR-t, hogy biztosítsa annak képességét az információvesztés nélküli működésre és az elsődleges EIR helyreállítására.
4. A szervezetnek dokumentálnia kell a tesztelési folyamatot és az eredményekről, hogy bizonyítékot szolgáltasson a redundáns rendszer működőképességéről.
5. Az érintett szervezetnek biztosítania kell, hogy a másodlagos EIR rendelkezzen a szükséges biztonsági intézkedésekkel, beleértve a fizikai és hálózati védelmet, valamint a megfelelő hozzáférés-kezelést.
6. Az érintett szervezetnek rendszeresen frissítenie kell a másodlagos EIR-t, hogy az mindig naprakész legyen és tükrözze az elsődleges EIR aktuális állapotát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.23. Alternatív feldolgozási helyszín

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

CP-9(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

7.41. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER MENTÉSEI – KETTŐS JÓVÁHAGYÁS A TÖRLÉSRE VAGY MEGSEMMISÍTÉSRE

7.41. A szervezet kettős jóváhagyáshoz köti a szervezet által meghatározott biztonsági mentési információk törlését vagy megsemmisítését.

MAGYARÁZAT

A kettős jóváhagyás biztosítja, hogy a biztonsági mentési információk törlése vagy megsemmisítése csak akkor történhet meg, ha azt két felhatalmazott személy végzi el. Azok a személyek, akik törlik vagy megsemmisítik a biztonsági mentési információkat, rendelkeznek azzal a szakértelemmel vagy készséggel, hogy megállapítsák, a tervezett információ törlése vagy megsemmisítése megfelel-e az érintett szervezet szabályainak és eljárásainak. Az összejátszás kockázatának csökkentése érdekében az érintett szervezet fontolóra veheti a kettős jóváhagyási feladatok személyek közötti rotációját.

Az EIR kritikus szerepet játszik az érintett szervezet működésében, és a biztonsági mentési információk törlése vagy megsemmisítése jelentős hatással lehet az EIR működésére és sértetlenségére. Ezért fontos, hogy az ilyen típusú műveletek csak kettős jóváhagyás után történjenek meg, hogy minimalizálják a hibák és a nem megfelelő törlések kockázatát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia és dokumentálnia a biztonsági mentési információk törlésének vagy megsemmisítésének szabályait és eljárásait.
2. A szervezetnek ki kell jelölnie legalább két személyt, akik rendelkeznek a szükséges képességekkel és szakértelemmel a biztonsági mentési információk törlésének vagy megsemmisítésének végrehajtására. Ezeknek a személyeknek meg kell érteniük és követniük kell az érintett szervezet szabályait és eljárásait.
3. A szervezetnek implementálnia kell a kettős jóváhagyási eljárást az EIR-ben. Ez azt jelenti, hogy a biztonsági mentési információk törlése vagy megsemmisítése csak akkor hajtható végre, ha mindkét kijelölt személy jóváhagyja azt.

4. A szervezetnek dokumentálnia kell minden törlési vagy megsemmisítési műveletet az EIR-ben, beleértve a kettős jóváhagyást is. A dokumentációban rögzíteni kell a törlés vagy megsemmisítés időpontját, a végrehajtó személyeket, és a törlés vagy megsemmisítés részleteit.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a biztonsági mentési információk törlésének vagy megsemmisítésének szabályait és eljárásait, valamint a kettős jóváhagyási eljárást, hogy biztosítsa azok hatékonyságát és relevanciáját.
6. A szervezet megfontolhatja a kettős jóváhagyási feladatok rotációját más személyek között, hogy csökkentse az összejátszás kockázatát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

2.59. Felelősségek szétválasztása

11.2. Hozzáférés az adathordozókhoz

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

CP-9(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági mentésekről szóló információ meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

7.42. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER MENTÉSEI – KRIPTOGRÁFIAI VÉDELEM

7.42. A szervezet kriptográfiai mechanizmusokat alkalmaz, hogy megakadályozza a meghatározott biztonsági mentési információk jogosulatlan felfedését és módosítását.

MAGYARÁZAT

A kriptográfiai mechanizmusok kiválasztásának alapja a biztonsági mentés adatainak bizalmas és sértetlenséget garantáló védelme. A kiválasztott mechanizmusok erőssége az információ biztonsági besorolásával arányos. A kriptográfiai védelem az elsődleges és a másodlagos helyszíneken tárolt információkra egyaránt vonatkozik. Azok a szervezetek, amelyek a tárolt információk védelmére kriptográfiai mechanizmusokat alkalmaznak, a kriptográfiai kulcskezelési megoldásokat is figyelembe veszik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a kriptográfiai mechanizmusokat, amelyeket a biztonsági mentési információk védelmére kíván alkalmazni. Ez a döntés a biztonsági mentési információk bizalmasságának és sértetlenségének megőrzésén alapul.
2. A szervezetnek biztosítania kell, hogy a kiválasztott mechanizmusok erőssége arányban áll az információ biztonsági kategóriájával vagy besorolásával.
3. A szervezetnek alkalmaznia kell a kriptográfiai védelmet az EIR biztonsági mentési információira mind az elsődleges, mind az másodlagos vagy további helyszínein.
4. A szervezetnek, amennyiben kriptográfiai mechanizmusokat alkalmaz az információ védelmére, figyelembe kell vennie a kriptográfiai kulcskezelési megoldásokat is.
5. A szervezetnek dokumentálnia kell a kriptográfiai mechanizmusok használatát, azok nyomon követésére és ellenőrzésére. A dokumentáció segíthet az érintett szervezetnek azonosítani és kezelni a potenciális biztonsági problémákat.
6. Az érintett szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kriptográfiai mechanizmusokat, hogy biztosítsa azok hatékonyságát és relevanciáját a változó biztonsági környezetben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

17.81. Tárolt (at rest) adatok védelme

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-9(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági mentésekről szóló információ meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

7.43. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER HELYREÁLLÍTÁSA ÉS ÚJRAINDÍTÁSA

7.43. A szervezet a meghatározott helyreállítási idővel és helyreállítási ponttal kapcsolatos célkitűzésekkel összhangban lévő időtartam alatt gondoskodik az EIR utolsó ismert, üzembiztos állapotba történő helyreállításáról és újraindításáról egy összeomlást, kompromittálódást vagy hibát követően.

MAGYARÁZAT

A helyreállítás a vészhelyzeti terv tevékenységeinek végrehajtását jelenti, amelyek célja az érintett szervezet alapfeladatainak és alapfunkcióinak helyreállítása. Az újraindítás a helyreállítást követően történik, és magában foglalja az EIR-ek teljes, üzembiztos állapotba való visszaállításának tevékenységeit. A helyreállítási és újraindítási műveletek tükrözik a szervezeti alapfeladatokat és az üzleti (ügymeneti) célkitűzéseket; a helyreállítási pontokat, a helyreállítási időt és a újraindítási célkitűzéseketet; valamint az érintett szervezet mérőszámait, amelyek összhangban vannak a vészhelyzeti terv követelményeivel. Az újraindítás magában foglalja azoknak az ideiglenes EIR képességeknek a kikapcsolását, amelyekre a helyreállítási műveletek során szükség lehetett. Az újraindítás továbbá magában foglalja a teljesen helyreállított EIR képességek értékelését, a folyamatos monitorozási tevékenységek újraindítását, az EIR újraengedélyezését, és a tevékenységeket, amelyek az EIR-t és az érintett szervezetet felkészítik a jövőbeli összeomlásokra, szabályok megsértésére, kompromittálódásokra vagy hibákra. A helyreállítási és újraindítási képességek magukban foglalhatják az automatizált mechanizmusokat és a manuális eljárásokat. Az érintett szervezetek a vészhelyzeti tervezés részeként határozzák meg a helyreállítási időt és a helyreállítási pont célkitűzéseket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet a vészhelyzeti tervezés részeként meghatározza a helyreállítási időt és a helyreállítási pont célokat.
2. A szervezetnek a helyreállítás során végre kell hajtania a vészhelyzeti tervnek foglaltakat az érintett szervezet alapfeladatának és alapfunkcióinak helyreállítása érdekében.

3. A helyreállítást követően az újraindítás során meghatározott tevékenységeket hajtanak végre az EIR teljes üzembiztos állapotba való visszaállításához.
4. A helyreállítási és újraindítási műveletek tükrözik az alapfeladatokat és üzleti (ügymeneti) célkitűzéseket, úgy, mint helyreállítási pont és idő, valamint az újraindítási célok, és a szervezet által meghatározott mérőszámok, amelyek összhangban vannak a vészhelyzeti terv követelményeivel.
5. A helyreállítási folyamat során dokumentálni kell az összes tevékenységet, hogy nyomon követhető legyen a folyamat és a jövőbeni biztonsági események megelőzése érdekében tanulni lehessen belőle.

Kapcsolódó intézkedések

7.2. Üzletmenet-folytonossági terv
7.13. Üzletmenet-folytonossági terv tesztelése
7.19. Biztonsági tárolási helyszín
7.23. Alternatív feldolgozási helyszín
7.35. Az elektronikus információs rendszer mentései
9.9.1. Biztonsági események kezelése
16.16. Biztonságtervezési elvek
17.77. Ismert állapot való meghibásodás
18.68. Előrelátható meghibásodás megelőzése

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

3.1.4.9. Az elektronikus információs rendszer helyreállítása és újraindítása

ISO/IEC 27001:2023 referencia

A.5.29

NIST SP 800-53 rev.5 referencia

CP-10

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az a helyreállítási idővel és a helyreállítási ponttal összhangban álló időtartam meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

7.44. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER HELYREÁLLÍTÁSA ÉS ÚJRAINDÍTÁSA – TRANZAKCIÓK HELYREÁLLÍTÁSA

7.44. A szervezet tranzakció alapú EIR-ek esetén tranzakció-helyreállítást hajt végre.

MAGYARÁZAT

Tranzakció-alapú EIR-ek közé tartoznak az adatbázis-kezelő EIR-ek és a tranzakciófeldolgozó EIR-ek. A tranzakció-helyreállítást támogató mechanizmusok közé tartozik a tranzakció visszagörgetése és a tranzakció naplózása.

A tranzakció visszagörgetése egy olyan folyamat, amelyben az érintett szervezet visszaállítja az EIR állapotát a tranzakció kezdőpontjára, ha a tranzakciót nem sikerült teljesen végrehajtani. Ez biztosítja, hogy az EIR konzisztens maradjon, és megakadályozza az adatok elvesztését vagy sérülését.

A tranzakció naplózása során a szervezet naplózza a tranzakció összes lépését. Ha a tranzakció nem sikerül, a napló segítségével a szervezet képes visszaállítani az EIR állapotát a tranzakció kezdete előtti állapotra. A naplózás lehetővé teszi az érintett szervezet számára, hogy nyomon kövesse a tranzakciók történetét, és segít a hibakeresésben és a problémák megoldásában.

Ezek a mechanizmusok nélkülözhetetlenek a tranzakció-alapú EIR-ekben, mivel biztosítják az adatok sértetlenségét és rendelkezésre állását, valamint megvédik az érintett szervezetet az adatvesztéstől vagy adatsérüléstől.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, hogy mely EIR-ek tartoznak a tranzakció-alapú kategóriába. Ezek általában adatbázis-kezelő és tranzakciófeldolgozó rendszerek.
2. A szervezetnek implementálnia kell a tranzakció-helyreállítást támogató mechanizmusokat. Ezek közé tartozik a tranzakció visszagörgetése és a tranzakció naplózása.
3. A tranzakció visszagörgetése esetén az érintett szervezetnek biztosítania kell, hogy az EIR képes legyen visszavonni a tranzakciókat, ha hiba történik. Ez azt jelenti, hogy az EIR-nek képesnek kell lennie visszaállítani az adatokat a tranzakció előtti állapotba.

4. A tranzakció naplózása esetén az érintett szervezetnek naplót kell vezetnie minden tranzakcióról, amit az EIR végrehajt. Ez lehetővé teszi az érintett szervezet számára, hogy nyomon követhesse a tranzakciók történetét, és helyreállíthassa azokat, ha szükséges.
5. A szervezetnek rendszeresen ellenőriznie kell az EIR-eket, hogy biztosítsa a tranzakció-helyreállítási mechanizmusok megfelelő működését.
6. A szervezetnek biztosítania kell, hogy a tranzakció-helyreállítási mechanizmusok megfelelnek a kiberbiztonsági követelményeknek. Ez magában foglalja a tranzakciók sértetlenségének és bizalmasságának és rendelkezésre állásának ellenőrzését.
7. A szervezetnek képzést kell biztosítania a munkatársak számára a tranzakció-helyreállítási mechanizmusok használatáról és a kiberbiztonsági legjobb gyakorlatokról.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.1.4.9. Az elektronikus információs rendszer helyreállítása és újraindítása

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CP-10(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

7.45. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER HELYREÁLLÍTÁSA ÉS ÚJRAINDÍTÁSA – MEGHATÁROZOTT IDŐN BELÜLI VISSZAÁLLÍTÁS

7.45. A szervezet biztosítja, hogy a rendszerelemeket előre definiált helyreállítási idő alatt helyre lehessen állítani, olyan ellenőrzött konfigurációból és sértetlenségvédett információkból, amelyek a rendszerelem ismert működési állapotát reprezentálják.

MAGYARÁZAT

A helyreállítás során a rendszerelemeket ellenőrzött konfigurációból állítják helyre. Ez azt jelenti, hogy a szervezetnek rendelkeznie kell egy olyan konfiguráció menedzsment rendszerrel, amely képes nyomon követni és ellenőrizni a rendszerelemek konfigurációját. Ez lehetővé teszi a szervezet számára, hogy gyorsan és hatékonyan helyreállítsa a rendszerelemeket a kívánt állapotba. A rendszerelemek helyreállítása során a szervezetnek biztosítania kell, hogy a helyreállított információk sértetlenségvédettek legyenek. Ez azt jelenti, hogy a szervezetnek rendelkeznie kell olyan biztonsági intézkedésekkel, amelyek megakadályozzák az információk módosítását, törlését vagy megsemmisítését a helyreállítás során.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek definiálnia kell egy helyreállítási időt, amely alatt a rendszerelemeket helyre kell állítani.
2. A szervezetnek biztosítania kell, hogy rendelkezésre álljon egy ellenőrzött konfiguráció, amely a rendszerelemek ismert működési állapotát képviseli. Ez a konfiguráció lehet egy biztonsági mentés vagy egy szabványosított rendszerkép.
3. A szervezetnek biztosítania kell, hogy a helyreállítási folyamat során csak sértetlenségvédett információkat használjanak. Ez azt jelenti, hogy az információkat meg kell védeni a módosításoktól, törléstől vagy hozzáférési kísérletektől a helyreállításig.
4. A szervezetnek rendszeresen ellenőriznie kell a helyreállítási folyamatot, hogy biztosítsa a helyreállítási idő betartását és a rendszerelemek helyes működését. Ez magában foglalhatja a helyreállítási naplók ellenőrzését és a helyreállítási folyamat tesztelését.

5. A szervezetnek biztosítania kell, hogy a helyreállítási folyamatot a szervezet összes érintett részlege ismeri és megérti. Ez magában foglalhatja a helyreállítási folyamat dokumentálását és a személyek képzését.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a helyreállítási folyamatot, hogy biztosítsa annak hatékonyságát és relevanciáját a rendszerelemek a változó állapothoz képest.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.2. Alapkonfiguráció
6.23. Konfigurációs beállítások

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

3.1.4.9. Az elektronikus információs rendszer helyreállítása és újraindítása

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CP-10(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az helyreállítási időszakok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

7.46. AZ ELEKTRONIKUS INFORMÁCIÓS RENDSZER HELYREÁLLÍTÁSA ÉS ÚJRAINDÍTÁSA – RENDSZERELEM VÉDELEM

7.46. A szervezet védi azokat a rendszerelemeket, amelyeket a helyreállítás során használnak.

MAGYARÁZAT

Az érintett szervezet védi azokat a rendszerelemeket, amelyeket a helyreállítás során használnak. Ez magában foglalja a fizikai és technikai ellenőrzéseket is. A helyreállítás és újraindítás során használt biztonsági mentési és helyreállítási elemek közé tartozhatnak például a router táblák (routing table), fordítóprogramok (compiler) és egyéb EIR szoftverek. A szervezet gondoskodik arról, hogy ezek a rendszerelemek megfelelően védettek legyenek mind fizikai, mind technikai szempontból. A szervezetnek biztosítania kell, hogy ezek az elemek ne legyenek hozzáférhetőek illetéktelen személyek számára, azokat megfelelően karbantartsák és frissítsék, hogy megvédjék őket a potenciális kiberbiztonsági fenyegetésektől. Ezenkívül az érintett szervezetnek naplóznia is szükséges, hogy nyomon követhesse és ellenőrizhesse a rendszerelemek használatát és védelmét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a rendszerelemeket, amelyeket a helyreállítás során használnak. Ezek lehetnek hardverek, firmware-ek és szoftverek.
2. A szervezetnek fizikai és technikai védelmi intézkedéseket kell bevezetnie a rendszerelemek védelme érdekében. Ez magában foglalhatja a hozzáférési jogosultságok szabályozását, a fizikai biztonsági intézkedéseket, valamint a szoftverek és firmware-ek biztonsági frissítéseit.
3. A szervezetnek biztonsági mentéseket kell készítenie a rendszerelemekről, és helyreállítási terveket kell kidolgoznia. A biztonsági mentéseknek magukban kell foglalniuk az összes helyreállításhoz szükséges szoftvert, melyeket a szervezetnek kell meghatároznia.
4. A szervezetnek naplóznia és monitoroznia kell, hogy nyomon követhesse a rendszerelemek állapotát és a hozzájuk történő hozzáféréseket. A naplózás segíthet a rendellenességek és a biztonsági események korai felismerésében.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a helyreállítási terveket és a biztonsági intézkedéseket, hogy biztosítsa a rendszerelemek védelmét a változó kiberbiztonsági fenyegetésekkel szemben.
6. A szervezetnek képzést kell biztosítania a munkatársak számára a helyreállítási folyamatokról és a rendszerelemek védelmének fontosságáról.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése
2.60. Legkisebb jogosultság elve
11.2. Hozzáférés az adathordozókhoz
11.4. Adathordozók tárolása
12.6. A fizikai belépés ellenőrzése
12.17. A fizikai hozzáférések felügyelete

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

CP-10(6)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

7.47. ALTERNATÍV KOMMUNIKÁCIÓS PROTOKOLLOK

7.47. A szervezet biztosítja a meghatározott alternatív kommunikációs protokollok alkalmazását a műveletek folyamatosságának fenntartása érdekében.

MAGYARÁZAT

A vészhelyzeti tervek és az ezekhez kapcsolódó vészhelyzeti képzés vagy tesztelés részeként az érintett szervezet beépít egy alternatív kommunikációs protokoll képességet az EIR-ek ellenálló képességének kialakítása érdekében. A kommunikációs protokollok váltása befolyásolhatja a szoftvereket és az EIR működési aspektusait. A szervezetek értékelik az alternatív kommunikációs protokollok bevezetésének potenciális mellékhatásait a megvalósítás előtt.

Az alternatív kommunikációs protokollok alkalmazása segít a szervezetnek fenntartani a műveletek folyamatosságát, még olyan esetekben is, amikor a fő kommunikációs csatornák nem működnek. Ez lehetővé teszi a szervezet számára, hogy gyorsan reagáljon a váratlan eseményekre, minimalizálja a műveletek zavarait és fenntartsa az EIR működését.

Az alternatív kommunikációs protokollok alkalmazásának dokumentálása és rendszeres felülvizsgálata segít a szervezetnek biztosítani, hogy ezek a protokollok megfelelően működnek és készen állnak a használatra, amikor szükség van rájuk. A dokumentáció és felülvizsgálat segít az érintett szervezetnek azonosítani és kezelni az esetleges problémákat, mielőtt azok hatással lennének az EIR működésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia a vészhelyzeti terveket, amelyek magukban foglalják az alternatív kommunikációs protokollok alkalmazásának képességét, mint a szervezeti EIR rendszerek ellenálló képességének létrehozásának részét.
2. A szervezetnek be kell építenie a vészhelyzeti képzéseket vagy teszteket, amelyek az alternatív kommunikációs protokollok alkalmazását is magukban foglalják.
3. A szervezetnek figyelembe kell vennie, hogy a kommunikációs protokollok váltása befolyásolhatja az alkalmazásokat és a rendszerek működési aspektusait.
4. A szervezetnek értékelnie kell az alternatív kommunikációs protokollok bevezetésének potenciális mellékhatásait a megvalósítás előtt.

5. A szervezetnek dokumentálnia kell, hogy nyomon követhesse és ellenőrizhesse az alternatív kommunikációs protokollok alkalmazását és hatékonyságát.
6. A szervezetnek folyamatosan felül kell vizsgálnia és frissítenie kell a vészhelyzeti terveket és a kommunikációs protokollokat, hogy biztosítsa az EIR-ek ellenálló képességét és a műveletek folyamatosságát.

Kapcsolódó intézkedések

7.2. Üzletmenet-folytonossági terv
7.29. Telekommunikációs szolgáltatások
7.49. Alternatív biztonsági mechanizmusok alkalmazása

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.29

NIST SP 800-53 rev.5 referencia

CP-11

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az alternatív kommunikációs protokollok meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

7.48. ÁTÁLLÁS BIZTONSÁGOSÜZEMMÓDRA

7.48. Az érintett EIR a szervezet által meghatározott korlátozásokkal rendelkező biztonságos üzemmódba vált, amennyiben a szervezet által meghatározott feltételek észlelésre kerülnek.

MAGYARÁZAT

Azon EIR-ek esetében, amelyek kritikus alapfeladatokat és alapfunkciókat támogatnak - például katonai műveleteket, erőművek műveleteit és légi forgalomirányítási műveleteket - a szervezetek meghatározhatnak bizonyos feltételeket, amelyek alatt ezek az EIR-ek átváltanak egy előre meghatározott biztonságos üzemmódra. A biztonságos üzemmód, amelyet automatikusan vagy manuálisan lehet aktiválni, korlátozza azokat a műveleteket, amelyeket az EIR végrehajthat, amikor ezek a feltételek előállnak. A korlátozás magában foglalja csak a kiválasztott funkciók végrehajtásának engedélyezését, amelyeket korlátozott teljesítmény mellett vagy csökkentett kommunikációs sávszélességgel lehet végrehajtani.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az szervezetnek azonosítania kell azokat a feltételeket, amelyek esetén az EIR biztonságos üzemmódra kell váltania.
2. A szervezetnek meg kell határoznia, hogy milyen funkciókat engedélyez a biztonságos üzemmódban. A korlátozások közé tartozhat, hogy csak kiválasztott funkciók futtathatók, amelyek korlátozott energiaellátás mellett vagy csökkentett kommunikációs sávszélességgel is elvégezhetők.
3. A szervezetnek dokumentálnia kell, hogy nyomon követhesse, mikor és milyen körülmények között vált az EIR biztonságos üzemmódra. Ez segít az érintett szervezetnek a kiberbiztonsági események elemzésében és a jövőbeni biztonsági események megelőzésében.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.2. Alapkonfiguráció
16.16. Biztonságtervezési elvek
17.77. Ismert állapot való meghibásodás
18.68. Előrelátható meghibásodás megelőzése
18.79. Hiba esetén alkalmazandó biztonsági eljárások

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

CP-12

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a feltételek illetve a korlátozásokkal rendelkező biztonságos üzemmód meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

7.49. ALTERNATÍV BIZTONSÁGI MECHANIZMUSOK ALKALMAZÁSA

7.49. A szervezet a meghatározott tartalék vagy kiegészítő biztonsági mechanizmusokat alkalmazza a meghatározott biztonsági funkciók megvalósítására, amikor az elsődleges biztonsági funkció megvalósítása nem elérhető vagy veszélyeztetett.

MAGYARÁZAT

A tartalék vagy kiegészítő biztonsági mechanizmusok alkalmazása megnöveli az EIR rugalmasságát, elősegíti a vészhelyzeti tervezést és a műveletek folyamatosságát. Az üzletmenet-folytonosság biztosítása érdekében az érintett szervezetek implementálhatnak tartalék vagy kiegészítő biztonsági mechanizmusokat. Ezek a mechanizmusok lehetséges, hogy kevésbé hatékonyak, mint az elsődleges mechanizmusok, azonban a tartalék vagy kiegészítő mechanizmusok alkalmazása támogatja az üzletmenet-folytonosságot, amely máskülönben hátrányosan érintett lehet, ha a műveleteket fel kellene függeszteni, amíg az elsődleges funkciók megvalósításának eszközeit helyreállítják. Amennyiben egy szervezet figyelembe veszi a költségeket és a szükséges erőfeszítést, előfordulhat, hogy a tartalék vagy kiegészítő mechanizmusokat csak az EIR, a rendszerelemek vagy az EIR szolgáltatások által nyújtott kritikus biztonsági képességekre alkalmazza. Például, ha a többtényezős tokeneket alkalmaz - amelyek a biztonságos hitelesítés standard eszközei - kompromittálódnak, a szervezet egyszer használatos eszközöket használhat helyettük.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a biztonsági funkciókat, amelyek kritikusak az üzletmenet-folytonosság szempontjából.
2. A szervezetnek ki kell dolgoznia egy tartalék vagy kiegészítő biztonsági mechanizmusokat tartalmazó tervet, amelyeket akkor lehet alkalmazni, ha az elsődleges biztonsági funkciók megvalósítása nem lehetséges vagy veszélyeztetett.
3. A szervezetnek figyelembe kell vennie a költségeket és a szükséges erőfeszítéseket, amelyeket az alternatív képességek biztosítása igényel.

4. A szervezetnek készen kell állnia arra, hogy a tartalék vagy kiegészítő mechanizmusokat alkalmazza, ha szükséges.

5. A szervezetnek dokumentálnia kell a tartalék vagy kiegészítő mechanizmusok alkalmazását, hogy nyomon követhető legyen a biztonsági funkciók megvalósítása és a potenciális biztonsági események.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.2. Üzletmenet-folytonossági terv

7.47. Alternatív kommunikációs protokollok

18.68. Előrelátható meghibásodás megelőzése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.5.29

NIST SP 800-53 REV.5 REFERENCIA

CP-13

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az alternatív vagy kiegészítő biztonsági mechanizmusok illetve a biztonsági funkciók meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024