Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Biztonsági események kezelése

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

9.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

9.1. A szervezet:

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

9.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó biztonsági eseménykezelési szabályzatot, amely

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

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

9.1.1.2. A biztonsági eseménykezelési eljárásrendet, amely a biztonsági eseménykezelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

9.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a biztonsági eseménykezelési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

9.1.3. Felülvizsgálja és frissíti az aktuális biztonsági eseménykezelési szabályzatot és a biztonsági eseménykezelési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

MAGYARÁZAT

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

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

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

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

által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően.

Kapcsolódó intézkedések

1.10. Kockázatkezelési stratégia
14.12. Fegyelmi intézkedések
18.67. Információ kezelése és megőrzése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

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

NIST SP 800-53 rev.5 referencia

IR-1

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

9.2. KÉPZÉS A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉRE

9.2. A szervezet:

9.2.1. Biztonsági eseménykezelési képzést biztosít a felhasználóknak a rájuk bízott szerepek és felelősségek szerint:

9.2.1.1. A biztonsági eseménykezelési szerepkör vagy felelősség kijelölését követően, illetve a rendszerhez való hozzáférés megszerzéstől számított meghatározott időn belül.

9.2.1.2. Amikor a rendszer változásai szükségessé teszik.

9.2.1.3. Ezt követően meghatározott gyakorisággal.

9.2.2. A szervezet meghatározott gyakorisággal, valamint meghatározott eseményeket követően felülvizsgálja és frissíti a biztonsági események kezelésére vonatkozó képzés tartalmát.

MAGYARÁZAT

A biztonsági eseményekre felkészítő képzés alapvetően szerepkör alapú. A szerepkörök figyelembevételével kell meghatározni a képzés tartalmát és mélységét. Például előfordulhat, hogy a felhasználóknak csak azt kell tudniuk, kit értesítsenek és milyen csatornán, vagy hogyan ismerjenek fel egy eseményt, azonban a rendszergazdák további képzést igényelhetnek a biztonsági események kezelésével kapcsolatban. A biztonsági eseményekre reagáló személyzet specifikusabb képzésben részesülhet az adatgyűjtési technikák, a jelentéstétel, a rendszer-helyreállítás és a rendszer-visszaállítás témakörében. A biztonsági eseményekre felkészítő képzés magában foglalja a felhasználók képzését a külső és belső forrásokból származó gyanús tevékenységek azonosítására és azok jelentésére. Az események, amelyek előidézhetik a reagálásra vonatkozó képzési tartalom frissítését (többek között) az eseménykezelési eljárás tesztelése; egy tényleges biztonsági eseményre adott válaszból levont tanulságok; az értékelés vagy az ellenőrzés megállapításai; a vonatkozó törvények, végrehajtási rendeletek, irányelvek, előírások, szabványok, ajánlások változásai.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztonsági eseménykezelési képzést kell biztosítania a szervezethez köthető személyek számára a rájuk bízott szerepek és felelősségek szerint.
2. A szervezetnek gondoskodnia kell a biztonsági eseménykezeléssel kapcsolatos felelősségek ellátásáról.
3. A szervezetnek rendszeresen frissítenie kell a képzési anyagot és szükség esetén továbbképzést kell biztosítania (például amikor az EIR változásai ezt szükségessé teszik).
4. A szervezetnek meghatározott gyakorisággal meg kell ismételnie a képzést annak érdekében, hogy a felhasználók biztonsági ismeretei naprakészek legyenek.
5. A szervezet meghatározott gyakorisággal, valamint meghatározott eseményeket követően felülvizsgálja és frissíti a biztonsági események kezelésére vonatkozó képzés tartalmát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

3.2. Biztonságtudatossági képzés
3.9. Szerepkör alapú biztonsági képzés
3.13. A biztonsági képzésre vonatkozó dokumentációk
7.10. A folyamatos működésre felkészítő képzés
9.5. Biztonsági események kezelésének tesztelése
9.9.1. Biztonsági események kezelése
9.34. Biztonsági eseménykezelési terv
9.35. Információszivárgásra adott válaszlépések

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

3.1.5.9. Képzés a biztonsági események kezelésére

ISO/IEC 27001:2023 REFERENCIA

A.6.3

NIST SP 800-53 REV.5 REFERENCIA

IR-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

9.3. KÉPZÉS A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉRE – SZIMULÁLT ESEMÉNYEK

9.3. A szervezet szimulált eseményeket épít be a biztonsági események kezelésére vonatkozó képzésbe, hogy elősegítse a személyzet számára a válsághelyzetekben szükséges reagálást.

MAGYARÁZAT

Az érintett szervezet a biztonsági események kezelésére szolgáló tervben követelményeket határoz a biztonsági eseményekre történő reagálással összefüggésben. A szimulált események tanulságainak beépítése a biztonsági események kezelésével kapcsolatos képzésbe segíti a szervezetet abban, hogy a személyzet megértse az egyéni felelősségeket és azt, hogy milyen konkrét intézkedéseket kell tennie válsághelyzetekben.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a követelményeket a biztonsági eseményekre való reagálásra vonatkozóan.
2. A szervezetnek létre kell hoznia egy biztonsági eseménykezelési tervet, amely részletesen leírja, hogyan kell reagálni a különböző típusú eseményekre.
3. A szervezetnek be kell építenie szimulált eseményeket az eseménykezelési képzésbe.
4. A szervezetnek biztosítania kell, hogy a személyzet megértse a hozzájuk köthető egyéni felelősségeket és a válsághelyzetekben megteendő konkrét lépéseket.
5. A szervezetnek dokumentálnia kell a képzéseket és a szimulált eseményeket annak érdekében, hogy nyomon követhesse a személyzet fejlődését és a képzés hatékonyságát.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az eseménykezelési tervet és az ezzel kapcsolatos képzési programot annak érdekében, hogy biztosítsa azok naprakészségét és hatékonyságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.1.5.9. Képzés a biztonsági események kezelésére

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-2(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

9.4. KÉPZÉS A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉRE – AUTOMATIZÁLT KÉPZÉSI KÖRNYEZET

9.4. A szervezet automatizált mechanizmusokat alkalmaz, hogy a biztonsági eseménykezelési képzéséhez valósághű környezetet biztosítson.

MAGYARÁZAT

Az automatizált mechanizmusok alaposabb és valósághűbb biztonsági eseménykezelési képzési környezetet biztosíthatnak. Ez megvalósítható például a kezelést igénylő esetek teljesebb lefedésével, valósághűbb képzési forgatókönyvek és környezetek kiválasztásával, valamint a reagálás hangsúlyozásával.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a biztonsági eseményeket, amelyekre a képzés során összpontosítani szeretne. Ezek az események lehetnek például adatvesztés, adatszivárgás, EIR-t érintő támadások stb.
2. A szervezetnek ki kell választania és be kell szereznie azokat az automatizált mechanizmusokat, amelyek képesek szimulálni a kiválasztott eseményeket.
3. A szervezetnek be kell állítania az automatizált mechanizmusokat, hogy a lehető legvalósághűbb környezetet biztosítsák a képzés során. Ez magában foglalhatja például a támadások időzítésének, intenzitásának és típusának beállítását.
4. A szervezetnek rendszeresen felül kell vizsgálnia a biztonsági események képzéséhez köthető automatizált mechanizmusokat és képzési környezeteket annak érdekében, hogy azok mindig naprakész legyenek a legújabb kiberbiztonsági fenyegetéseket és trendeket illetően.
6. A szervezetnek értékelnie kell a képzés hatékonyságát. Ez magában foglalhatja a képzésen részt vevők visszajelzéseinek begyűjtését és értékelését, illetve korábbi képzések eredményeivel történő összehasonlítást.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.1.5.9. Képzés a biztonsági események kezelésére

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-2(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

9.5. BIZTONSÁGI ESEMÉNYEK KEZELÉSÉNEK TESZTELÉSE

9.5. A szervezet meghatározott módon és gyakorisággal teszteli a rendszerre vonatkozó biztonsági eseménykezelési képességek hatékonyságát.

MAGYARÁZAT

Az érintett szervezet teszteli a biztonsági eseménykezelési képességeit annak érdekében, hogy felmérje azok hatékonyságát és a potenciális gyengeségeket, valamint a hiányosságokat azonosítsa. Az eseménykezelési tesztelés magában foglalja a ellenőrzési listák használatát, a teljes tesztelést vagy a meglévő tervek strukturált átnézését (tabletop gyakorlat), valamint a szimulációkat is. A biztonsági események kezelésének tesztelése magában foglalhatja a szervezeti működést, az eszközöket, valamint az eseménykezelés miatt érintett személyekre gyakorolt hatások meghatározását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a teszteléshez használt módszereket és a tesztelés gyakoriságát.
2. Az szervezetnek rendszeresen tesztelnie kell az EIR-re vonatkozó biztonsági eseménykezelési képességeit annak érdekében, hogy meghatározza azok hatékonyságát és azonosítsa a potenciális gyengeségeket vagy hiányosságokat.
3. A szervezetnek értékelnie kell a tesztelés eredményeit annak érdekében, hogy meghatározza az eseménykezelési folyamatok hatékonyságát.
4. A szervezetnek dokumentálnia kell a tesztelési folyamatot és annak eredményeit. Ezáltal nyomon követheti a fejlődést és az esetleges változásokat.
5. A szervezetnek folyamatosan felül kell vizsgálnia és frissítenie kell az EIR-re vonatkozó biztonsági eseménykezelési képességeit a tesztelési eredmények alapján.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.10. A folyamatos működésre felkészítő képzés
7.13. Üzletmenet-folytonossági terv tesztelése
9.2. Képzés a biztonsági események kezelésére

9.9.1. Biztonsági események kezelése

9.34. Biztonsági eseménykezelési terv

1.15. Tesztelés, képzés és felügyelet

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

3.1.5.9. Képzés a biztonsági események kezelésére

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-3

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

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

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

9.6. BIZTONSÁGI ESEMÉNYEK KEZELÉSÉNEK TESZTELÉSE – AUTOMATIZÁLT TESZTELÉS

9.6. A szervezet meghatározott automatizált eszközök használatával teszteli a biztonsági eseménykezelési képességét.

MAGYARÁZAT

Az érintett szervezet automatizált mechanizmusokat alkalmaz a biztonsági eseménykezelési képességének alaposabb és hatékonyabb teszteléséhez. Ez kivitelezhető azáltal, hogy teljeskörű lefedettséget biztosítanak a biztonsági eseménykezeléssel kapcsolatban felmerült problémákkal kapcsolatban, valósághű tesztkörnyezeteket és forgatókönyveket választanak, valamint tesztelik a biztonsági eseménykezelési képességet is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell választania a megfelelő automatizált eszközöket, amelyekkel tesztelni tervezi a biztonsági eseménykezelési képességét.
2. A szervezetnek meg kell határoznia a tesztelési forgatókönyveket és környezeteket, amelyek a legreálisabbak és leginkább relevánsak a szervezet számára.
3. A szervezetnek el kell végeznie a teszteket az EIR-en a kiválasztott automatizált eszközök segítségével, hogy megbizonyosodjon arról, hogy a biztonsági eseménykezelési képesség megfelelően működik-e.
4. A szervezetnek értékelnie kell a tesztelési eredményeket, és meg kell határoznia, hogy milyen lépéseket kell tennie a biztonsági eseménykezelési képesség javítása érdekében.
5. A szervezetnek dokumentálnia kell a tesztelési folyamatot és az eredményeket, annak érdekében, hogy nyomon követhesse a fejlődést és bizonyítékot szolgáltathasson a megfelelőségről.
6. A szervezetnek rendszeresen meg kell ismételnie ezt a folyamatot, hogy biztosítsa a biztonsági eseménykezelési képesség folyamatos hatékonyságát és fejlődését.

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

IR-3(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.7. BIZTONSÁGI ESEMÉNYEK KEZELÉSÉNEK TESZTELÉSE – ÖSSZEHANGOLÁS A KAPCSOLÓDÓ TERVEKKEL

9.7. A szervezet egyezteti a biztonsági eseménykezelés tesztelését a kapcsolódó tervekért felelős szervezeti egységekkel.

MAGYARÁZAT

Az érintett szervezetnek számos olyan tervvel kell rendelkeznie, amelyek kapcsolódnak a biztonsági eseménykezelés teszteléséhez. Ilyenek például az üzletmenet-folytonossági tervek, a katasztrófa-helyreállítási tervek, a működés folytonosságának tervei, a vészhelyzeti tervek, a válságkommunikációs tervek és a kritikus infrastruktúra tervei.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie, mely szervezeti egységek felelősek a biztonsági eseményekhez kapcsolódó tervekért.
2. A szervezetnek ezután egyeztetnie kell ezekkel a szervezeti egységekkel a biztonsági eseménykezelés teszteléséről. Ez magában foglalhatja a tesztelési időpontok, módszerek és eszközök meghatározását.
3. A szervezetnek végül értékelnie kell a biztonsági eseménykezelés tesztelésének eredményeit, és szükség esetén módosítania kell a kapcsolódó terveket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.1.5.9. Képzés a biztonsági események kezelésére

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-3(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

9.8. Biztonsági események kezelésének tesztelése – Folyamatos fejlesztés

9.8. A szervezet a tesztelés során keletkezett kvalitatív és kvantitatív adatokat felhasználva

9.8.1. megállapítja a biztonsági eseménykezelési folyamatok hatékonyságát;

9.8.2. folyamatosan fejleszti a biztonsági eseménykezelési folyamatokat; és

9.8.3. olyan biztonsági eseménykezelési intézkedéseket és mérőszámokat alkalmaz, amelyek pontosak, következetesek és reprodukálhatók.

Magyarázat

A biztonsági eseménykezelési tevékenységek megfelelő működése érdekében az érintett szervezetek használhatnak mérőszámokat és értékelési kritériumokat a biztonsági eseménykezelési programok értékelésére, annak érdekében, hogy folyamatosan javítsák az eseménykezelés teljesítményét. Ezek a törekvések elősegítik a biztonsági eseménykezelés hatékonyságának javulását és csökkentik az események hatásait.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a tesztelés során keletkezett kvalitatív és kvantitatív adatokat. Ez magában foglalja az adatok gyűjtését, elemzését és értékelését, illetve a biztonsági eseménykezelési folyamatok hatékonyságának megállapítását.
2. A szervezetnek folyamatosan fejlesztenie kell a biztonsági eseménykezelési folyamatokat.
3. A szervezetnek olyan biztonsági eseménykezelési intézkedéseket és mérőszámokat kell alkalmaznia, amelyek pontosak, következetesek és reprodukálhatók. Ez magában foglalja a mérőszámok kiválasztását és alkalmazását, valamint a mérőszámok rendszeres felülvizsgálatát és frissítését.
4. A szervezetnek dokumentálnia kell a biztonsági eseménykezelési folyamatokat, beleértve a tesztelés során keletkezett adatokat, a folyamatok fejlesztését és a mérőszámok alkalmazását. A dokumentálás segít az érintett szervezetnek nyomon követni a folyamatok hatékonyságát és a fejlesztések eredményességét.
5. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a biztonsági eseménykezelési folyamatait, hogy biztosítsa azok hatékonyságát és folyamatos fejlesztését.

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

IR-3(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

9.9. BIZTONSÁGI ESEMÉNYEK KEZELÉSE

9.9.1. A szervezet:

9.9.2. Biztonsági eseménykezelési képességet alakít ki, amely összhangban van a biztonsági eseménykezelési tervvel, és magában foglalja a felkészülést, az észlelést és elemzést, az elszigetelést, a felszámolást és a helyreállítást.

9.9.3. A szervezet összehangolja a biztonsági eseménykezelési tevékenységeket az üzletmenet-folytonossági tervezési tevékenységekkel.

9.9.4. A szervezet beépíti a folyamatos biztonsági eseménykezelési tevékenységekből származó tanulságokat a biztonsági eseménykezelési eljárásokba, képzésbe és tesztelésbe.

9.9.5. A szervezet biztosítja, hogy a biztonsági eseménykezelési tevékenységek összehasonlíthatók és kiszámíthatók legyenek a szervezeten belül.

MAGYARÁZAT

A biztonsági eseménykezelési tevékenységek megfelelő működése érdekében az érintett szervezetek használhatnak mérőszámokat és értékelési kritériumokat a biztonsági eseménykezelési programok értékelésére, annak érdekében, hogy folyamatosan javítsák az eseménykezelés teljesítményét. Ezek a törekvések elősegítik a biztonsági eseménykezelés hatékonyságának javulását és csökkentik az események hatásait.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a tesztelés során keletkezett kvalitatív és kvantitatív adatokat. Ez magában foglalja az adatok gyűjtését, elemzését és értékelését, illetve a biztonsági eseménykezelési folyamatok hatékonyságának megállapítását.
2. A szervezetnek folyamatosan fejlesztenie kell a biztonsági eseménykezelési folyamatokat.
3. A szervezetnek olyan biztonsági eseménykezelési intézkedéseket és mérőszámokat kell alkalmaznia, amelyek pontosak, következetesek és reprodukálhatók. Ez magában foglalja a mérőszámok kiválasztását és alkalmazását, valamint a mérőszámok rendszeres felülvizsgálatát és frissítését.
4. A szervezetnek dokumentálnia kell a biztonsági eseménykezelési folyamatokat, beleértve a tesztelés során keletkezett adatokat, a folyamatok fejlesztését és a mérőszámok alkalmazását.

A dokumentálás segít az érintett szervezetnek nyomon követni a folyamatok hatékonyságát és a fejlesztések eredményességét.

5. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a biztonsági eseménykezelési folyamatait, hogy biztosítsa azok hatékonyságát és folyamatos fejlesztését.

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

IR-3(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

9.10. Biztonsági események kezelése – Automatizált eseménykezelő folyamatok

9.10. A szervezet meghatározott automatizált mechanizmusok segítségével támogatja a biztonsági eseménykezelési folyamatot.

Magyarázat

Az érintett szervezet automatizált mechanizmusokat alkalmaz a biztonsági eseménykezelési folyamat támogatására. Ezek az eszközök magukban foglalják az online eseménykezelő rendszereket és azokat az eszközöket, amelyek támogatják a biztonsági események kezeléséhez szükséges adatok gyűjtését, a teljes hálózati csomagok rögzítését és a forensics elemzést.

A követelmény alkalmazásának lépései

1. A szervezetnek be kell vezetnie olyan automatizált mechanizmusokat, amelyek támogatják a biztonsági eseménykezelési folyamatot. Ezek lehetnek online eseménykezelő rendszerek és eszközök, amelyek támogatják biztonsági események kezeléséhez szükséges adatok gyűjtését, a teljes hálózati csomagok rögzítését és a forenzikus elemzést.
2. A szervezetnek biztosítania kell, hogy az EIR többi rendszereleme megfelelően integrálva van ezekkel az automatizált mechanizmusokkal, és képesek kommunikálni egymással a biztonsági események kezelése érdekében.
3. A szervezetnek rendszeresen ellenőriznie kell az EIR-t és az automatizált mechanizmusokat, hogy biztosítsa azok megfelelő működését és hatékonyságát. Ez magában foglalhatja a rendszeres tesztelést és a naplók áttekintését.
4. A szervezetnek biztosítania kell, hogy a szervezethez köthető személyek megfelelően képzett és felkészült a biztonsági események kezelésére, és képesek használni az EIR-t és az automatizált mechanizmusokat.
5. A szervezetnek folyamatosan frissítenie kell az EIR-t és az automatizált mechanizmusokat, hogy lépést tudjanak tartani a legújabb biztonsági fenyegetésekkel és sérülékenységekkel.
6. A szervezetnek biztosítania kell, hogy a biztonsági események kezelése során betartják a releváns jogszabályokat és szabályozásokat, beleértve a naplózási követelményeket is.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.1.5.2. Automatikus eseménykezelés: Az érintett szervezet automatizált mechanizmusokat alkalmaz az eseménykezelési eljárások támogatására.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-4(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

9.11. Biztonsági események kezelése – Dinamikus újrakonfigurálás

9.11. A szervezet a meghatározott rendszerelemekhez kapcsolódó dinamikus újrakonfigurálási funkciót épít be a biztonsági eseményekre történő reagálási képességébe.

Magyarázat

A dinamikus újrakonfigurálási funkció magában foglalhatja a router szabályok, hozzáférési-ellenőrzési listák, a behatolás észlelő vagy megelőző rendszer paramétereit és az egyéb védelmi funkciót ellátó eszközök vagy tűzfalak szűrési szabályainak változtatását. Az érintett szervezet dinamikus újrakonfigurálást végezhet az EIR-ekben annak érdekében, hogy megállítsa a támadásokat, félrevezesse a támadókat, és elkülönítse az EIR komponenseit, ezzel csökkentve a támadásból eredő károk mértékét. Az érintett szervezet az újrakonfigurálási képességek definiálása során az EIR-ek újrakonfigurálásához konkrét időkereteket határoz meg, és figyelembe veszi, hogy a fenyegetések hatékony kezeléséhez gyors intézkedésre lehet szükség.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia azokat a rendszerelemeket, amelyekhez a dinamikus újrakonfigurálási funkciót hozzá kívánja rendelni.
2. A szervezetnek meg kell valósítania a dinamikus újrakonfigurálási funkciót a meghatározott rendszerelemekben.
3. A szervezetnek be kell építenie a dinamikus újrakonfigurálási képességet a biztonsági eseményekre történő reagálási képességébe.

Kapcsolódó intézkedések

2.2. Fiókkezelés
2.28. Információáramlási szabályok érvényesítése
6.2. Alapkonfiguráció

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-4(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek illetve a dinamikus újrakonfigurációra vonatkozó típusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.12. BIZTONSÁGI ESEMÉNYEK KEZELÉSE – MŰKÖDÉS FOLYTONOSSÁGA

9.12. A szervezet a szervezeti célok teljesülésének és az üzleti funkciók folyamatosságának biztosítása érdekében osztályozza a biztonsági eseményeket, és az egyes osztályokhoz rendelt meghatározott válaszlépéseket hajtja végre a biztonsági eseményekre reagálva.

MAGYARÁZAT

A biztonsági események osztályai közé tartoznak a tervezést vagy megvalósítást érintő hibák és mulasztások, valamint a kártékony céllal végrehajtott támadások. A biztonsági események kezelése során megtett intézkedések magukban foglalhatják az EIR elavulását, az EIR leállítását, a manuális üzemmódba való visszaállást, vagy egy alternatív technológia élesítését amely esetén az EIR más módon működik, megtévesztést szolgáló intézkedéseket, alternatív információáramlást, vagy olyan üzemmódba történő átkapcsolást, melyet a támadás alatt álló EIR esetén alkalmaznak. Az érintett szervezet megfontolja, hogy biztonsági esemény esetén a működés folytonosságára vonatkozó követelmények ütköznek-e az EIR automatikus leállításának képességével.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet osztályozza a biztonsági eseményeket az általa meghatározott osztályok alapján.
2. A szervezet a biztonsági események osztályaihoz végrehajtandó intézkedéseket határoz meg.
3. A szervezet mérlegeli, hogy biztonsági esemény esetén a működés folytonosságára vonatkozó követelmények ütköznek-e az EIR automatikus leállításának képességével.
4. A szervezet dokumentálja az összes biztonsági eseményt és az azzal összefüggésben megtett intézkedéseket annak érdekében, hogy értékelje és továbbfejlessze a biztonsági intézkedéseket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-4(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági eseményekre vonatkozó osztályok illetve az egyes osztályokhoz rendelt meghatározott válaszlépések meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.13. BIZTONSÁGI ESEMÉNYEK KEZELÉSE – INFORMÁCIÓK KORRELÁCIÓJA

9.13. A szervezet korrelálja a biztonsági eseményekre vonatkozó információkat a szervezet egyéb releváns információival az átfogóbb helyzetfelismerés és -értékelés érdekében.

MAGYARÁZAT

Az érintett szervezetnek a biztonsági eseményekre vonatkozó információkat össze kell hangolnia az érintett szervezet egyéb releváns információival, hogy átfogóbb képet kapjon a helyzetről és értékelni tudja azt. Ez a folyamat magában foglalja a különböző forrásokból származó információk összegyűjtését és elemzését, beleértve a különböző jelentéseket és az érintett szervezet által létrehozott jelentési eljárásrendeket. Például egy fenyegető esemény, mint például egy kibertámadás, csak akkor figyelhető meg, ha a szervezet különböző forrásokat felhasználva összegyűjti az elérhető információkat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy rendelkezik a szükséges technológiával és eszközökkel a biztonsági események korrelálásához.
2. A szervezetnek létre kell hoznia egy folyamatot, amely lehetővé teszi a biztonsági események és az EIR egyéb releváns információinak összegyűjtését és korrelálását. Ez magában foglalhatja például a biztonsági események naplózását, a hálózati forgalom elemzését, valamint az alkalmazások és felhasználók viselkedésének monitorozását.
3. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a korreláció eredményeit. Ez magában foglalhatja a biztonsági események trendjeinek, mintázatainak és anomáliáinak elemzését, valamint a potenciális biztonsági fenyegetések azonosítását.
4. A szervezetnek be kell építenie a korrelációs folyamatot a biztonsági stratégiájába és szabályzataiba. Ez magában foglalhatja a korrelációs folyamat felelőseinek és feladatainak meghatározását, valamint a folyamat eredményeinek felhasználását a kiberbiztonságot érintő döntéshozatalban.
5. A szervezetnek folyamatosan frissítenie és finomítania kell a korrelációs folyamatot, hogy reagálni tudjon az új biztonsági fenyegetésekre és kihívásokra. Ez magában foglalhatja a

korrelációs szabályok és algoritmusok frissítését, valamint az új adatforrások integrálását a folyamatba.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.1.5.3. Információ korreláció: Az érintett szervezet összekapcsolja a biztonsági eseményekre vonatkozó információkat és az egyedi eseményekre való reagálásokat, hogy szervezetszintű rálátást nyerjen a biztonsági eseményekkel kapcsolatos tudatosságra és reagálásokra.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-4(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

9.14. Biztonsági események kezelése – Rendszer automatikus leállítása

9.14. A szervezet olyan konfigurálható képességet alkalmaz, amely automatikusan leállítja a rendszert a meghatározott biztonsági szabályok megsértésének észlelése esetén.

Magyarázat

Az érintett szervezet mérlegeli, hogy a képesség, amely automatikusan leállítja az EIR-t, összeegyeztethető-e a meghatározott működés folytonossági követelményekkel. A biztonsági előírások megsértése olyan támadásokat foglal magában, melyek során sérült az EIR sértetlensége, lemásolták az érintett szervezet információit, valamint megismerték az érintett szervezet által alkalmazott szoftverek súlyos hibáit. Mindez negatívan befolyásolhatja az érintett szervezet célkitűzéseit, funkcióit, illetve veszélyeztetheti személyek biztonságát.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell vizsgálnia, hogy az automatikus leállítási képesség összeegyeztethető-e a meghatározott működés-folytonossági követelményekkel.
2. A szervezetnek meg kell határoznia a biztonsági szabályokat, amelyek megsértése esetén az EIR automatikusan leáll.
3. A szervezetnek implementálnia kell egy konfigurálható képességet, amely automatikusan leállítja az EIR-t a biztonsági szabályok megsértésének észlelése esetén.
4. A szervezetnek naplózási tevékenységet kell folytatnia annak érdekében, hogy nyomon követhesse a biztonsági szabályok megsértését és az EIR automatikus leállítását.
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a biztonsági szabályokat és az automatikus leállítási képességhez köthető előírásokat vagy eljárásrendeket annak érdekében, hogy biztosítsa az EIR védelmét a legújabb biztonsági fenyegetésekkel szemben.

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

IR-4(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonság sértések meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.15. BIZTONSÁGI ESEMÉNYEK KEZELÉSE – BELSŐ FENYEGETÉSEK

9.15. A szervezet biztonsági eseménykezelési képességet alakít ki a belső fenyegetésekkel kapcsolatos eseményekre vonatkozóan.

MAGYARÁZAT

A belső fenyegetésekkel kapcsolatos biztonsági események kezelésére való kifejezett összpontosítás további hangsúlyt fektet az ilyen típusú fenyegetésekre, valamint a megfelelő és időben történő reagáláshoz különleges eseménykezelési képességek szükségére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell ismernie a belső fenyegetések jelentőségét és potenciális hatását az EIR-re és a szervezetre nézve. Ez magában foglalja a belső fenyegetésekkel kapcsolatos tudatosság növelését és a belső fenyegetésekkel szembeni védekezés fontosságának kommunikálását az érintett szervezet minden tagja számára.
2. A szervezetnek ki kell dolgoznia és implementálnia kell egy biztonsági eseménykezelési tervet, amely részletesen leírja, hogyan reagál a belső fenyegetésekkel kapcsolatos eseményekre. Ez a terv magában foglalja a belső fenyegetések azonosításának, értékelésének és kezelésének folyamatát, valamint a válaszadási lépéseket.
3. A szervezetnek naplóznia kell és rendszeresen felül kell vizsgálnia a naplókat annak érdekében, hogy azonosítsa az esetleges belső fenyegetéseket és megtegye a szükséges intézkedéseket.
4. A szervezetnek folyamatosan képeznie kell munkavállalóit a belső fenyegetésekkel kapcsolatban, annak érdekében, hogy ismertek legyenek számukra a fenyegetéssel kapcsolatos legújabb információk és képesek legyenek hatékonyan kezelni ezeket az eseményeket.
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a biztonsági eseménykezelési tervet annak érdekében, hogy biztosítsa annak naprakészségét és hatékonyságát a belső fenyegetésekkel szemben.

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

IR-4(6)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

9.16. Biztonsági események kezelése – Belső fenyegetések – Szervezeten belüli együttműködés

9.16. A szervezet a meghatározott szervezeti egységek bevonásával koordinálja a belső fenyegetések kezelésére szolgáló biztonsági eseménykezelési képességet.

Magyarázat

Az érintett szervezetnek a belső fenyegetések kezelésére szolgáló biztonsági eseménykezelési képességét számos szervezeti egység bevonásával kell koordinálnia pl.: az üzleti tulajdonosokat, az EIR felelőseit, az emberi erőforrások (HR) menedzseléséért felelős részlegeket, a beszerzési területet, a fizikai biztonságért felelős területet, tapasztalt információbiztonságért felelős munkatársat, az üzemeltetésért felelős területet, a kockázatok kezeléséért felelős területet és a jogi területet. Emellett az érintett szervezet szükség esetén segítséget kérhet a helyi rendvédelmi szervektől.

A követelmény alkalmazásának lépései

1. A szervezetnek fel kell készülnie a belső fenyegetések kezelésére. Ez magában foglalja a szükséges eszközök, erőforrások és személyzet rendelkezésre állásának biztosítását.
2. A szervezetnek be kell vonnia a meghatározott szervezeti egységeket.
3. A szervezetnek folyamatosan monitoroznia és elemeznie kell az EIR-ben történő tevékenységeket, hogy időben észlelje a belső fenyegetéseket. Ez magában foglalja a naplók rendszeres áttekintését és elemzését.
4. A szervezetnek felül kell vizsgálnia és szükség esetén frissítenie kell a belső fenyegetések kezelésének folyamatát annak érdekében, hogy biztosítsa annak naprakészségét és hatékonyságát.
5. A szervezetnek szükség esetén segítséget vagy támogatást kell kérnie a helyi rendvédelmi szervektől.

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

IR-4(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az entitások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.17. BIZTONSÁGI ESEMÉNYEK KEZELÉSE – EGYÜTTMŰKÖDÉS KÜLSŐ SZERVEZETEKKEL

9.17. A szervezet a kijelölt külső szervezetekkel együttműködve korrelálja és megosztja a biztonsági eseményekkel kapcsolatos információit, hogy átfogó képet kapjon a biztonsági eseményekről, és hatékonyabban tudjon reagálni rájuk.

MAGYARÁZAT

Az érintett szervezet számára a biztonsági eseményekkel kapcsolatos információk összehangolása külső szervezetekkel együttműködve - beleértve például az üzleti partnereket, ügyfeleket és fejlesztőket - jelentős előnyökkel járhat. A szervezeteken átívelő koordináció fontos kockázatkezelési képesség lehet. Ez a képesség lehetővé teszi az érintett szervezet számára, hogy felhasználja a különböző forrásokból származó információkat, ezáltal hatékonyan reagáljon a biztonsági eseményekre és azokra a támadásokra, amelyek potenciálisan befolyásolhatják az érintett szervezet működését, eszközeit és munkavállalóit.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a külső szervezeteket, amelyekkel együttműködik a biztonsági eseményekkel kapcsolatos információk korrelálásában és megosztásában.
2. A szervezetnek létre kell hoznia egy koordinációs mechanizmust, amely lehetővé teszi az információk cseréjét a külső szervezetekkel. Ez a mechanizmus lehet formális vagy informális, de biztosítania kell az információk biztonságos és hatékony áramlását.
3. A szervezetnek rendszeresen meg kell osztania a biztonsági eseményekkel kapcsolatos információkat a kijelölt külső szervezetekkel. Ez magában foglalhatja a biztonsági események jelentéseit, a naplókat és más releváns adatokat.
4. A szervezetnek korrelálnia kell a külső szervezetektől kapott információkat a saját biztonsági eseményeivel. Ez lehetővé teszi az érintett szervezet számára, hogy átfogó képet kapjon a biztonsági eseményekről, és hatékonyabban tudjon reagálni rájuk.
5. A szervezetnek folyamatosan értékelnie kell a koordinációs mechanizmust, és szükség esetén módosítania kell azt, hogy biztosítsa a biztonsági eseményekkel kapcsolatos információk hatékony korrelálását és megosztását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.51. Szervezeten átívelő naplózás

1.17. Fenyegetettség tudatosító program

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

IR-4(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a külső szervezetek illetve a biztonsági eseményekre vonatkozó információk meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.18. BIZTONSÁGI ESEMÉNYEK KEZELÉSE – DINAMIKUS VÁLASZADÁSI KÉPESSÉG

9.18. A szervezet dinamikus reagálási képességeket alkalmaz a biztonsági események kezelésére.

MAGYARÁZAT

A dinamikus reagálási képesség az időben megtett, biztonsági eseményekre adott új vagy helyettesítésre szolgáló szervezeti képességeket jelenti. Ez magában foglalja az alapfunkciók, valamint az EIR szintjén megvalósított képességeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek implementálnia kell a dinamikus válaszadási képességeket. Ez magában foglalhatja a biztonsági eszközök és technológiák telepítését, biztonsági protokollok és eljárások bevezetését, valamint a személyzet képzését és felkészítését.
2. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén módosítania kell a dinamikus reagálási képességeit annak érdekében, hogy biztosítsa azok hatékonyságát és naprakészségét. Ez magában foglalja a fenyegetések, támadások és sérülékenységek újraértékelését, a stratégiák és eljárásrendek felülvizsgálatát, valamint a biztonsági eszközök és technológiák frissítését.

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

IR-4(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a dinamikus reagálási képességek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.19. BIZTONSÁGI ESEMÉNYEK KEZELÉSE – ELLÁTÁSI LÁNC KOORDINÁCIÓJA

9.19. A szervezet összehangolja az ellátási láncban bekövetkező biztonsági események kezelését az ellátási láncban részt vevő szervezetekkel.

MAGYARÁZAT

Az ellátási láncban részt vevő szervezetek magukba foglalják a termékfejlesztőket, rendszerintegrátorokat, gyártókat, csomagolókat, összeszerelőket, disztribútorokat, eladókat és a viszonteladókat is. Az ellátási láncot érintő biztonsági események bármikor bekövetkezhetnek, és magukban foglalhatják a fő- vagy alvállalkozókat, az információtechnológiai termékeket, az EIR-elemeket, a fejlesztési folyamatokat vagy az abban érintett személyzetet, valamint a terjesztési folyamatokat vagy a raktárhelyiségeket érintő érintő támadásokat. Az érintett szervezet megfontolja, hogy a biztonsági eseményekkel kapcsolatos információk védelmét és megosztását szolgáló folyamatokat beépíti az információcserére vonatkozó megállapodásaiba, valamint az állami felügyeleti szervek felé történő bejelentési kötelezettsége során is figyelembe veszi azokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie az ellátási láncban részt vevő szervezeteket.
2. A szervezetnek fel kell készülnie arra, hogy a biztonsági események bárhol bekövetkezhetnek az ellátási láncban, beleértve a fő- vagy alvállalkozókat, az információtechnológiai termékeket, az EIR-elemeket, a fejlesztési folyamatokat vagy a személyzetet, valamint a disztribúciós folyamatokat vagy a raktározási létesítményeket.
3. A szervezetnek meg kell fontolnia, hogy beépíti az információvédelmi és megosztási folyamatokat az információcserére vonatkozó megállapodásokba, valamint a kormányzati felügyeleti szerveknek felé történő események jelentési kötelezettségét.
4. A szervezetnek naplóznia kell a biztonsági eseményeket, hogy nyomon követhesse és elemezhesse azokat. Ez lehetővé teszi az érintett szervezet számára, hogy azonosítsa a gyengeségeket és javítsa az EIR biztonságát.

5. A szervezetnek együtt kell működnie az ellátási láncban részt vevő összes szervezettel, hogy összehangolja a biztonsági események kezelését és megossza a releváns információkat. Ez magában foglalhatja a közös válaszlépések kidolgozását és a legjobb gyakorlatok megosztását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.6. Információcsere
10.2. Szabályozott karbantartás
16.49. Külső elektronikus információs rendszerek szolgáltatásai
19.19. Értesítési megállapodások

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-4(10)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.20. Biztonsági események kezelése – Integrált eseménykezelő csoport

9.20. A szervezet létrehoz és fenntart egy integrált biztonsági eseménykezelő csoportot, amely a szervezet által meghatározott időn belül bármely kijelölt helyszínen bevethető.

Magyarázat

Az integrált biztonsági eseménykezelő csoport egy olyan szakértőkből álló csapat, amely értékeli, dokumentálja és kezeli a biztonsági eseményeket annak érdekében, hogy a szervezethez köthető EIR-ek és hálózatok gyorsan helyreálljanak, emellett olyan biztonsági intézkedéseket alkalmaz, melyekkel elkerülhetők a jövőbeli biztonsági események. A biztonsági eseménykezelő csoport tagjai lehetnek a forenzikus- és kártékony kód elemzők, az eszközfejlesztők, a rendszerbiztonsági mérnökök, valamint az üzemeltetésért felelős munkatársak. A biztonsági eseménykezelési képesség magában foglalja a bizonyítékok gyors, forenzikus módszerekkel történő megőrzését, emellett a behatolások elemzését és az arra adott válaszlépéseket. Néhány szervezetnél a biztonsági eseménykezelő csoport egy szervezetet egészét lefedő entitás is lehet. Az integrált biztonsági eseménykezelő csoport elősegíti az információk megosztását, és lehetővé teszi az érintett szervezet személyzete számára, hogy a csoportban meglévő, fenyegetéssel kapcsolatos tudás alapján megfelelő védelmi intézkedéseket valósítsanak meg. Mindez lehetővé teszi az érintett szervezet számára, hogy hatékonyabban védekezzenek a behatolások ellen. Ráadásul az integrált csoportok elősegítik a behatolások gyors észlelését, a megfelelő intézkedések kidolgozását és a hatékony védelmi intézkedések bevezetését. Például, amikor egy behatolást észlelnek, akkor az integrált csoport gyorsan kidolgozhat egy megfelelő intézkedést az üzemeltetésért felelős személyzet számára, összekapcsolhatja az új eseménnyel kapcsolatos információkat a korábban bekövetkezett események információival, és kiegészítheti a folyamatban lévő információszerzés fejlesztését. Az integrált biztonsági eseménykezelő csoportok hatékonyabban képesek azonosítani a támadók taktikáit, technikáit és módszereit, amelyek kapcsolódnak az érintett szervezet működéséhez, célkitűzéseihez és üzleti folyamataihoz. Emellett olyan válaszlépéseket dolgozhatnak ki, amelyek nem okoznak fennakadást az érintett szervezet célkitűzéseiben és üzleti folyamataiban. A biztonsági eseménykezelő csoportokat több helyen is elhelyezhetik az

érintett szervezeten belül, annak érdekében, hogy az általuk biztosított képesség még rugalmasabb legyen.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy integrált biztonsági eseménykezelő csoportot, amely különböző szakterületek szakértőkből áll, akik értékelik, dokumentálják és kezelik az eseményeket, hogy a szervezethez köthető EIR-ek és hálózatok gyorsan helyreálljanak emellett olyan biztonsági intézkedéseket alkalmaz, melyekkel elkerülhetők a jövőbeli biztonsági események.
2. A szervezetnek gondoskodnia kell arról, hogy a csapatban olyan szakértőkből álljon, mint például a forenzikus- és kártékony kód elemzők, fejlesztők, a rendszerbiztonsági mérnökök, valamint az üzemeltetésért felelős munkatársak.
3. A szervezetnek biztosítania kell, hogy a csapat képes legyen gyorsan megőrizni a bizonyítékokat, illetve képesek legyenek elemzéseket végezni, valamint reagálni a biztonsági eseményekre.
4. A szervezetnek elő kell segítenie az információk megosztását, és lehetővé kell tennie az érintett szervezet személyzete számára, hogy a csoportban meglévő, fenyegetéssel kapcsolatos tudás alapján megfelelő védelmi intézkedéseket valósíthassanak meg.
5. A szervezetnek biztosítania kell, hogy az integrált biztonsági eseménykezelő csoport képes legyen gyorsan észlelni a behatolásokat, kidolgozni a megfelelő ellenintézkedéseket, és emellett a védelmet erősítő intézkedéseket legyenek képesek alkalmazni.
6. A szervezetnek meg kell fontolnia, hogy biztonsági eseménykezelő csoportokat több helyen is elhelyezzen a szervezeten belül, annak érdekében, hogy az általuk biztosított képesség még rugalmasabb legyen.
7. A szervezetnek biztosítania kell az integrált biztonsági eseménykezelő csoport hosszútávú működését, és rendszeresen nyomon kell követni a tevékenységeiket, annak érdekében, hogy folyamatosan értékeljék és javítsák a teljesítményüket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

3.9. Szerepkör alapú biztonsági képzés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-4(11)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az idő intervallum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

9.21. Biztonsági események kezelése – Kártékony kód és forenzikus vizsgálat

9.21. A szervezet elemzi a kártékony kódokat és minden más olyan nyomot, amelyek a biztonsági esemény után maradtak a rendszerben.

Magyarázat

Egy elszigetelt környezetben gondosan elvégzett, kártékony kód és egyéb, biztonsági esemény után maradt nyom elemzése betekintést nyújthat az érintett szervezet számára a támadók által alkalmazott taktikákba, technikákba és módszerekbe. Emellett utalhat a támadó kilétére vagy azonosíthatók a támadóval kapcsolatos egyedi tulajdonságok. Továbbá a kártékony kód elemzése segítheti az érintett szervezetet a jövőbeli biztonsági eseményekre adott válaszlépések kidolgozásában.

A követelmény alkalmazásának lépései

1. A szervezetnek ki kell alakítania egy elszigetelt környezetet, ahol a kártékony kódokat és a biztonsági esemény után maradt egyéb nyomokat biztonságosan elemezheti.
2. A szervezetnek szakértői csapatot kell kijelölnie, akik képesek a kártékony kódok elemzésére és az esetleges biztonsági rések kezelésére.
3. A szervezetnek naplózásra és monitorozásra van szüksége az EIR-ben, hogy azonosítsa és nyomon kövesse a biztonsági eseményeket.
4. A szervezetnek részletesen elemeznie kell a kártékony kódokat és a biztonsági esemény után maradt nyomokat.
5. Az érintett szervezetnek az elemzés eredményei alapján meg kell határoznia a további lépéseket, beleértve a biztonsági intézkedések megerősítését és a jövőbeni biztonsági eseményekre adott válaszlépéseket.
6. Az érintett szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a biztonsági követelményeket és az EIR-ben alkalmazott védelmi mechanizmusokat, hogy képes legyen elhárítani a folyamatosan változó kiberbiztonsági fenyegetéseket.
7. A szervezetnek dokumentálnia kell az elemzési folyamatot és az eredményeket, hogy referenciaanyagként szolgáljanak a jövőbeni eseményekhez.

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

IR-4(12)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

9.22. BIZTONSÁGI ESEMÉNYEK KEZELÉSE – VISELKEDÉSELEMZÉS

9.22. A szervezet elemzi a rendellenes vagy feltételezhetően rosszindulatú viselkedést, amely meghatározott környezettel vagy erőforrásokkal kapcsolatos.

MAGYARÁZAT

Ha az érintett szervezet fenntart egy megtévesztésre használt környezetet, az ebben a környezetben megfigyelt viselkedések elemzése - beleértve a támadó által megcélzott erőforrásokat és a biztonsági esemény időbeliségét - betekintést nyújthat a támadó által alkalmazott taktikákba, technikákba és módszerekbe. A megtévesztésre használt környezeten kívül, a rendellenes vagy feltételezhetően rosszindulatú viselkedés (pl.: a specifikus erőforrások helyének keresésében bekövetkező változások) elemzése is szolgálhat információval a támadóval kapcsolatban az érintett szervezet számára.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fenn kell tartania egy megtévesztésre használt környezetet.
2. A megtévesztő környezeten kívül az érintett szervezetnek elemeznie kell a rendellenes vagy feltételezhetően rosszindulatú viselkedést (pl.: a specifikus erőforrások helyének keresésében bekövetkező változások).
3. A szervezetnek naplóznia kell, hogy nyomon követhesse és elemezhesse az EIR-ben történő változásokat és eseményeket. A naplózás segíthet azonosítani a rendellenes vagy rosszindulatú viselkedést, és lehetővé teszi a szervezet számára, hogy gyorsan reagáljon a potenciális biztonsági eseményekre.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a biztonsági szabályzatait és eljárásrendjeit annak érdekében, hogy biztosítsa a tulajdonában álló EIR-ek védelmét a legújabb fenyegetésekkel szemben.
5. A szervezetnek képzést kell biztosítania a munkatársak számára ahol megtanulhatják, hogy a rendellenes vagy rosszindulatú viselkedést hogyan ismerhetik fel.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.16

NIST SP 800-53 REV.5 REFERENCIA

IR-4(13)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a környezetek vagy erőforrások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.23. BIZTONSÁGI ESEMÉNYEK KEZELÉSE – BIZTONSÁGI MŰVELETI KÖZPONT

9.23. A szervezet létrehoz és fenntart egy biztonsági műveleti központot.

MAGYARÁZAT

A biztonsági műveleti központ (Security Operations Center - SOC) az érintett szervezet kiberbiztonsági műveleteinek és számítógépes hálózatvédelmének központja. A biztonsági műveleti központ célja, hogy folyamatosan védje és figyelemmel kísérje az érintett szervezet EIR-jeit és hálózatait. A biztonsági műveleti központ felelőssége a kiberbiztonsági események észlelése, elemzése és időben történő kezelése. Az érintett szervezet a biztonsági műveleti központban képzett technikai és üzemeltetői személyzetet alkalmaz (például biztonsági elemzők, biztonsági eseménykezelést végző személyzet, rendszerbiztonsági mérnökök), valamint technikai, menedzsment és operatív követelmények kombinációját alkalmazza (beleértve a monitorozást, szkennelést és a forenzikus eszközöket) a fenyegetések és biztonsági relevanciájú eseményadatok több forrásból történő monitorozására, összefűzésére, korrelációjára, elemzésére és kezelésére. Ezek a források a határvédelmet, a hálózati eszközöket (például routereket, switcheket) és a végponti agent-ek adatfolyamait tartalmazzák. A biztonsági műveleti központ átfogó helyzetfelismerő képességet biztosít, hogy segítsen meghatározni az EIR és az érintett szervezet biztonsági állapotát. A biztonsági műveleti központot többféleképpen lehet kialakítani. A nagyobb szervezetek dedikált biztonsági műveleti központot hozhatnak létre, míg a kisebb szervezetek harmadik féltől igényelhetnek ilyen képességet.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a biztonsági műveleti központ célját és feladatait. Ezek közé tartozik az EIR védelme és monitorozása, valamint a kiberbiztonsági események időben történő észlelése, elemzése és kezelése.
2. A szervezetnek képzett biztonsági és üzemeltetői személyzetet kell alkalmaznia a biztonsági műveleti központban. Ez magában foglalja a biztonsági elemzőket, a biztonsági

eseménykezelést végző személyzetet és a rendszerbiztonsági mérnököket és üzemeltetést végző munkatársakat.

3. Az szervezetnek különböző módszerek és megközelítések kombinációját kell alkalmaznia (beleértve a monitorozást, szkennelést és a forenzikus eszközöket). Ezeket az eszközöket arra használja, hogy monitorozza, összefűzze, korrelálja, elemezze a több forrásból érkező fenyegetéseket és a biztonsági relevanciájú eseményadatokat.

4. A biztonsági műveleti központnak képesnek kell lennie a teljes körű helyzetfelismerésre annak érdekében, hogy segítsen az érintett szervezetnek meghatározni az EIR biztonsági állapotát.

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

IR-4(14)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

9.24. BIZTONSÁGI ESEMÉNYEK KEZELÉSE – SZERVEZETI KAPCSOLATOK ÉS JÓHÍRNÉV HELYREÁLLÍTÁSA

9.24. A szervezet:

9.24.1. kezeli külső kapcsolatait egy bekövetkezett biztonsági eseményhez kötődően; és

MAGYARÁZAT

Fontos, hogy az érintett szervezet rendelkezzen egy kidolgozott stratégiával arra az esetre, amennyiben a szervezetet érintő biztonsági esemény nyilvánosságra kerül, negatív fényt vet az érintett szervezetre, vagy érintette a szervezet partnereit, ügyfeleit. Egy biztonsági esemény nyilvánosságra kerülése rendkívül káros lehet a szervezet számára, és hatással lehet a szervezet üzleti céljaira és tevékenységeire. Az érintett szervezet hírnevének helyreállítása érdekében megtett intézkedések rendkívül fontosak ahhoz, hogy a partnerek és ügyfelek bizalmát vissza lehessen szerezni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy kommunikációs stratégiát, amely részletesen leírja, hogyan kommunikálja a bekövetkezett biztonsági eseményeket a nyilvánosság felé, hogyan tájékoztatja a szervezet által megtett lépésekről.
2. A szervezetnek dokumentálnia kell a biztonsági eseményeket annak érdekében, hogy nyomon követhesse azokat és megelőzhesse a jövőbeni eseményeket.
3. A szervezetnek intézkednie kell hírnevének helyreállítására, mely lehet nyilvános bocsánatkérés, a szervezet által tett intézkedések bemutatása és a jövőbeni biztonsági események megelőzésére irányuló tervek ismertetése.
4. A szervezetnek folyamatosan felül kell vizsgálnia és szükség esetén frissítenie kell a válságkezelési tervét és kommunikációs stratégiáját annak érdekében, hogy biztosítsa azok hatékonyságát és naprakészségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-4(15)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.25. A BIZTONSÁGI ESEMÉNYEK NYOMONKÖVETÉSE

9.25. A szervezet nyomon követi és dokumentálja az EIR biztonsági eseményeit.

MAGYARÁZAT

A biztonsági eseményeket kezelő automatizált rendszerek, melyek az események begyűjtését és elemzését végzik, a CSIRT-ek és egyéb rendelkezésre álló elektronikus adatbázisok és hálózati monitorozó eszközök adatait használják fel.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy eljárásrendet, amely meghatározza, hogyan kell nyomon követni és dokumentálni a biztonsági eseményeket. Ez az eljárásrend tartalmazza az eseményekről szóló jegyzőkönyvek karbantartását, az események állapotát és más, a digitális forenzikus vizsgálatokhoz és az események részleteinek, trendjeinek és kezelésének értékeléséhez szükséges információkat.
2. A biztonsági eseményekkel kapcsolatos információk számos forrásból szerezheti be az érintett szervezet, beleértve a hálózat monitorozását, a biztonsági eseményekről készült jelentéseket, a biztonsági eseményeket kezelő csapatokat, a felhasználói panaszokat, a beszállítói partnereket, a naplók monitorozását, a fizikai hozzáférés monitorozását, valamint a felhasználói és adminisztrátori jelentéseket.
3. Az érintett szervezetnek meg kell határoznia, mely biztonsági eseményeket kell nyomon követnie.
4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az biztonsági események nyomon követését érintő eljárásrendet annak érdekében, hogy biztosítsa annak naprakészségét és hatékonyságát.
5. A szervezetnek biztosítania kell, hogy a személyzet megfelelően képzett és felkészült, annak érdekében, hogy a biztonsági eseményeket nyomon követése és dokumentálása megfelelő legyen.

Kapcsolódó intézkedések

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.22. Naplóbejegyzések csökkentése és jelentéskészítés

9.9.1. Biztonsági események kezelése

9.27. A biztonsági események jelentése

9.34. Biztonsági eseménykezelési terv

12.17. A fizikai hozzáférések felügyelete

1.5. Elektronikus információs rendszerek nyilvántartása

17.12. Szolgáltatásmegtagadással járó támadások elleni védelem

17.17. A határok védelme

18.8. Kártékony kódok elleni védelem

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

3.1.5.4. A biztonsági események figyelése

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

IR-5

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

9.26. A BIZTONSÁGI ESEMÉNYEK NYOMONKÖVETÉSE – AUTOMATIZÁLT NYOMON KÖVETÉS, ADATGYŰJTÉS ÉS ELEMZÉS

9.26. A szervezet automatizált mechanizmusokat alkalmaz a biztonsági események nyomonkövetésére, a biztonsági eseményekre vonatkozó információk gyűjtésére és vizsgálatára.

MAGYARÁZAT

A biztonsági eseményeket kezelő automatizált rendszerek, melyek az események begyűjtését és elemzését végzik, a CSIRT-ek és egyéb rendelkezésre álló elektronikus adatbázisok és hálózati monitorozó eszközök adatait használják fel.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek automatizált eszközöket kell beszereznie, amelyek képesek a biztonsági események nyomon követésére és a kapcsolódó információk gyűjtésére.
2. A szervezetnek úgy kell konfigurálnia a beszerzett eszközöket, hogy vagy a szervezet által meghatározott rendszereket vagy rendszerelemeket vagy a teljes EIR tevékenységét folyamatosan monitorozza és rögzítse a biztonsági eseményeket.
3. A szervezetnek biztosítania kell, hogy a rögzített információkat rendszeresen elemzik, illetve azonosítják a potenciális biztonsági fenyegetéseket vagy sérülékenységeket.
4. A szervezetnek be kell építenie a rögzített információk alapján történő cselekvést a biztonsági események kezelésére vonatkozó eljárásrendjébe.
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az automatizált mechanizmusokat annak érdekében, hogy biztosítsa azok hatékonyságát és naprakészségét.
6. A szervezetnek biztosítania kell, hogy a személyzet megfelelően képzett és felkészült a biztonsági események kezelésére és az automatizált eszközök használatára.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.1.5.5. Automatikus nyomonkövetés, adatgyűjtés és vizsgálat: Az érintett szervezet automatizált mechanizmusokat alkalmaz, hogy segítse a biztonsági események nyomon követését és a biztonsági eseményekre vonatkozó információk gyűjtését és vizsgálatát.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-5(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

9.27. A BIZTONSÁGI ESEMÉNYEK JELENTÉSE

9.27. A szervezet:

9.27.1. Kötelezi a személyzetet arra, hogy jelentse a biztonsági esemény gyanúját vagy bekövetkeztét.

9.27.2. Jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat a jogszabályban meghatározott szervek felé.

MAGYARÁZAT

A bejelentett biztonsági események típusainak, tartalmának és időszerűségének igazodnia kell a jogszabályban elvártakhoz, illetve azokat a jogszabályban meghatározott szervek felé kell az érintett szervezetnek bejelentenie. A biztonsági eseményekből nyert információk fontos bemeneti információként szolgálnak a kockázatelemzéshez, a beszerzések biztonsági szempontjainak meghatározásához, a technológiai termékek kiválasztásához, valamint a szervezeti védelmi intézkedések értékeléséhez.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek olyan szabályzatot kell alkotnia vagy meglévő szabályzatai valamelyikébe (pl. IBSZ) illesztenie, amely kötelezi a szervezethez köthető személyeket arra, hogy jelentsék a biztonsági esemény gyanúját vagy bekövetkeztét.
2. A szervezetnek biztosítania kell, hogy a személyek megfelelő képzést kapjanak a biztonsági események felismerésére és jelentésére.
3. A szervezetnek létre kell hoznia egy jelentéstételre vonatkozó eljárásrendet, amely érthetővé teszi a szervezethez köthető személyek számára, hogy jelentse a biztonsági eseményeket. Az eljárásrend lehetővé teszi a gyors és hatékony jelentéstételt, és biztosítja, hogy a jelentések megfelelően dokumentálva legyenek.
4. A szervezetnek biztosítania kell, hogy a biztonsági eseményekről szóló információkat a jogszabályban meghatározottak szerint jelentik a jogszabályban meghatározott szervek felé. Ez magában foglalja a jelentéshez köthető eljárásrendet, a jelentendő információkat és a jelentés időben történő megtételével kapcsolatos előírásokat.

5. A szervezetnek dokumentálnia kell a biztonsági eseményeket, beleértve a jelentett eseményeket, a megtett intézkedéseket és a következményeket. A dokumentálás segíthet az érintett szervezetnek a kockázatelemzésben, a biztonsági előírások hatékonyságának értékelésében, a biztonsági követelmények meghatározásában a beszerzésekhez és a technológiai termékek kiválasztási kritériumainak meghatározásában.

Kapcsolódó intézkedések

6.23. Konfigurációs beállítások
7.2. Üzletmenet-folytonossági terv
9.9.1. Biztonsági események kezelése
9.25. A biztonsági események nyomonkövetése
9.34. Biztonsági eseménykezelési terv
9.35. Információszivárgásra adott válaszlépések

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

3.1.5.6. A biztonsági események jelentése

ISO/IEC 27001:2023 referencia

A.5.5; A.6.8

NIST SP 800-53 rev.5 referencia

IR-6

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

9.28. A BIZTONSÁGI ESEMÉNYEK JELENTÉSE – AUTOMATIZÁLT JELENTÉS

9.28. A szervezet automatizált mechanizmusokat alkalmaz a biztonsági események bejelentésének támogatására.

MAGYARÁZAT

A biztonsági eseményekről szóló jelentések címzettjeit meg kell határozni. Az automatizált jelentésküldő megoldások közé sorolhatók az e-mail és olyan tájékoztató weboldalak is melyek tartalmát folyamatosan frissítik, valamint az automatikus biztonsági eseménykezelő eszközök és programok.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy kik lesznek a biztonsági eseményekről szóló jelentések címzettjei.
2. A szervezetnek automatizált mechanizmusokat kell alkalmaznia a biztonsági események bejelentésének támogatására.
3. A szervezetnek képesnek kell lennie a biztonsági eseményeket automatikusan észlelni. Ez magában foglalhatja a biztonsági eseményeket észlelő és rögzítő eszközök és szoftverek telepítését és konfigurálását.
4. A szervezetnek folyamatosan karban kell tartania az automatizált bejelentési mechanizmusokat, hogy biztosítsa azok hatékonyságát és megbízhatóságát. Ez magában foglalhatja a szoftverfrissítések telepítését, a rendszer konfigurációjának felülvizsgálatát és módosítását, valamint a rendszer teljesítményének és stabilitásának monitorozását.
5. A szervezetnek biztosítania kell, hogy a szervezethez köthető személyek megfelelően képzettek és felkészültek az automatizált bejelentési mechanizmusok használatára és kezelésére. Ezt elérheti különféle oktatásokkal.

KAPCSOLÓDÓ INTÉZKEDÉSEK

9.31. Segítségnyújtás a biztonsági események kezeléséhez

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

3.1.5.6. A biztonsági események jelentése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-6(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

9.29. A BIZTONSÁGI ESEMÉNYEK JELENTÉSE – ESEMÉNYEKKEL KAPCSOLATOS SÉRÜLÉKENYSÉGEK

9.29. A szervezet megköveteli a biztonsági eseményekkel kapcsolatosan az EIR-ek sérülékenységeinek jelentését a szervezet által meghatározott személyeknek vagy szerepköröknek.

MAGYARÁZAT

Az EIR sérülékenységeit feltáró, lejelentett biztonsági eseményeket az érintett szervezet személyzete elemzi. Az elemzés segíthet priorizálni és a gyakorlatba átültetni az EIR-ben azonosított sérülékenységek kezelésére megteendő intézkedéseket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek szabályoznia kell és létre kell hoznia egy eljárásrendet, amely meghatározza, hogy milyen biztonsági események esetén kell jelentést tenni, és kik azok a személyek vagy szerepkörök, akiknek ezeket a jelentéseket meg kell kapniuk.
2. A szervezetnek biztosítania kell, hogy az EIR sérülékenységeit felfedő biztonsági eseményeket az érintett szervezet személyzete elemezze pl.: az EIR felelősei, üzleti tulajdonosok, tapasztalt információbiztonsági munkatárs, engedélyezést végző terület, a kockázatok kezeléséért felelős terület.
3. Az elemzés segíthet priorizálni és elősegíteni az EIR-ben felfedezett sérülékenységek kezelését.
4. A szervezetnek dokumentálnia kell a biztonsági eseménnyel összefüggésben feltárt, EIR-hez köthető sérülékenységeket.
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a vonatkozó szabályzatot és eljárásrendet annak érdekében, hogy biztosítsa annak naprakészségét és hatékonyságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-6(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.30. A BIZTONSÁGI ESEMÉNYEK JELENTÉSE – ELLÁTÁSI LÁNC KOORDINÁCIÓJA

9.30. A szervezet megosztja a biztonsági eseményekkel kapcsolatos információkat az érintett termék vagy szolgáltatás szállítójával, valamint más szervezetekkel, amelyek részt vesznek az érintett rendszerek vagy rendszerelemek ellátási láncában, vagy annak irányításában.

MAGYARÁZAT

Az ellátási lánc tevékenységekben érintett szervezetek közé tartoznak a termékfejlesztők, az rendszerintegrátorok, a gyártók, a csomagolók, az összeszerelők, az elosztók, az értékesítők és a viszonteladók. Az ellátási lánccal kapcsolatos biztonsági események közé sorolhatók azon támadások, amelyek az információ technológiai termékekkel, EIR-elemekkel, a fejlesztési folyamatokkal vagy személyzettel, az elosztási folyamatokkal vagy a raktárhelyiségekkel kapcsolatosak. Az érintett szervezetek meghatározzák a megosztani kívánt információkat és figyelembe veszik a külső szervezetek tájékoztatásából származó előnyöket. Az előnyök közé sorolható a folyamatok javítása vagy egy biztonsági eseményt kiváltó ok azonosítása.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie, hogy mely szervezetek vesznek részt az EIR ellátási láncában vagy annak irányításában.
2. A szervezetnek meg kell határoznia, hogy milyen információkat oszt meg a biztonsági eseményekről. Ezt a döntést a megosztott információ értékének figyelembevételével kell meghozni, beleértve a folyamatok javításának képességét vagy az eseményt kiváltó ok azonosítását.
3. A szervezetnek létre kell hoznia egy eljrásárendet az információ megosztására. Ez magában foglalhatja a megfelelő csatornák kiválasztását, a megosztás időzítését és annak módját.
4. A szervezetnek biztosítania kell, hogy a megosztott információk megfelelően védettek legyenek. Ez magában foglalhatja az adatok titkosítását, az anonimizálást és más biztonsági intézkedéseket.
5. A szervezetnek dokumentálnia kell a megosztott információkat. Ez lehetővé teszi az érintett szervezet számára, hogy nyomon követhesse kivel, mikor és milyen információkat osztott meg.

6. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az információ megosztásának eljárásrendjét annak érdekében, hogy biztosítsa annak hatékonyságát és naprakészségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

19.19. Értesítési megállapodások

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-6(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

9.31. SEGÍTSÉGNYÚJTÁS A BIZTONSÁGI ESEMÉNYEK KEZELÉSÉHEZ

9.31. A szervezet támogatást biztosít a biztonsági események kezeléséhez és jelentéséhez az EIR felhasználói számára.

MAGYARÁZAT

A biztonsági események kezelésében a általában szervezetek helpdesk szolgáltatói és támogatási csoportjai vesznek részt, amely folyamatok támogatására a szervezetek (automatizált) jegykezelő rendszereit használják. A jegykezelő rendszerek képesek létrehozni és kezelni a hibajegyeket és ezek segítségével nyomon követni a biztonsági eseményeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy helpdesk szolgáltatói és támogatási csoportot, amely támogatást nyújt az EIR felhasználóinak a biztonsági események kezelésében.
2. A szervezetnek be kell vezetnie egy jegykezelő rendszert, amely lehetővé teszi a biztonsági események kezeléséhez köthető jegyek megnyitását és nyomon követését.
3. A szervezetnek dokumentálnia kell az összes biztonsági eseményt, beleértve azokat, amelyeket az EIR felhasználói jelentettek.
4. A szervezetnek meg kell bizonyosodnia arról, hogy az EIR felhasználói tisztában vannak azzal, hogyan jelenthetik a biztonsági eseményeket, és milyen támogatást kaphatnak az események kezelésében. Ez magában foglalhatja a képzéseket, útmutatókat, és a helpdesk szolgáltatói és támogatási csoport elérhetőségét.
6. A szervezetnek folyamatosan felül kell vizsgálnia és szükség esetén frissítenie kell a biztonsági események kezelésére és jelentésére vonatkozó szabályzatait és eljárásrendjeit annak érdekében, hogy hatékony támogassa az EIR felhasználóit a biztonsági események bejelentésében.

Kapcsolódó intézkedések

3.2. Biztonságtudatossági képzés

3.9. Szerepkör alapú biztonsági képzés

9.9.1. Biztonsági események kezelése

9.27. A biztonsági események jelentése

9.34. Biztonsági eseménykezelési terv

16.49. Külső elektronikus információs rendszerek szolgáltatásai

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

3.1.5.7. Segítségnyújtás a biztonsági események kezeléséhez

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

IR-7

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

9.32. Segítségnyújtás biztonsági események kezeléséhez – Automatizált támogatás az információk és a támogatás elérhetőségéhez

9.32. A szervezet automatizált mechanizmusokat alkalmaz, hogy növelje a biztonsági események kezelésével kapcsolatos információk hozzáférhetőségét és a támogatást.

Magyarázat

Az automatizált folyamatok "push-pull" alapú megoldásai nagy segítséget nyújthatnak a felhasználóknak a biztonsági események kezelésében. Például, ha egy felhasználó elérhet egy olyan weboldalt, ahol a biztonsági eseményhez kapcsolódó segítséget kaphat, vagy ha az automatizált mechanizmus képes proaktív módon információt küldeni a biztonsági esemény kezelésével kapcsolatban a felhasználók számára.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, milyen automatizált mechanizmusokat szeretne alkalmazni a biztonsági események kezelésével kapcsolatos információk hozzáférhetőségének és támogatásának növelése érdekében.
2. A szervezetnek ki kell dolgoznia egy rendszert, amely lehetővé teszi a felhasználók számára, hogy segítséget kapjanak a biztonsági események események kezelésében. Ez lehet például egy weboldal, ahol a felhasználók megismerhetik az adott biztonsági eseményhez köthető teendőket.
3. Az automatizált mechanizmusoknak képesnek kell lenniük proaktívan információt küldeni a felhasználóknak. Ez lehet általános- vagy célzott információátadás (pl. súgó szövegbuborékok).
4. A szervezetnek folyamatosan felül kell vizsgálnia és szükség esetén karban kell tartania az automatizált mechanizmusokat, hogy biztosítsa a biztonsági események kezelésével kapcsolatos információk hozzáférhetőségét és a támogatást.
5. A szervezetnek biztosítania kell, hogy a felhasználók képzettek és felkészültek a biztonsági események kezelésére, és tisztában vannak az automatizált mechanizmusok használatával.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.1.5.7. Segítségnyújtás a biztonsági események kezeléséhez

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IR-7(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

9.33. SEGÍTSÉGNYÚJTÁS BIZTONSÁGI ESEMÉNYEK KEZELÉSÉHEZ – KÜLSŐ SZOLGÁLTATÓKKAL VALÓ KOORDINÁCIÓ

9.33. A szervezet:

9.33.1. biztosítja, hogy a biztonsági eseménykezelő tevékenység és a rendszer védelmi képességeinek külső szolgáltatói közötti kommunikáció hatékony és zökkenőmentes legyen; és

9.33.2. azonosítja a biztonsági eseménykezelő tevékenység szereplőit a külső szolgáltatók számára.

MAGYARÁZAT

A külső szolgáltatók segítenek az EIR-ekben és a hálózatokban történő jogosulatlan tevékenységek elleni védelemben, nyomon követésben, elemzésben, észlelésben és a válaszlépések megtételében. Mielőtt bekövetkezne egy biztonsági esemény, hasznos lehet előzetes megállapodásokat kötni a külső szolgáltatókkal, melyekben tisztázzák az egyes felek szerepét és felelősségét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell térképeznie és meg kell határoznia azokat a külső szolgáltatókat, akik a biztonsági eseménykezelő tevékenységben és az EIR védelmi képességeinek kialakításában részt vesznek.
2. A szervezetnek megállapodásokat kell kötnie a külső szolgáltatókkal, melyekben tisztázzák az egyes felek szerepét és felelősségét, mielőtt bármilyen biztonsági esemény bekövetkezne. Ez magában foglalhatja a kommunikációra vonatkozó eljárásrendek, a válaszidők, a naplózás/dokumentálás és a biztonsági események kezelését érintő eljárásrendek meghatározását.
3. A szervezetnek biztosítania kell, hogy a kommunikáció a biztonsági eseménykezelő tevékenység és az EIR védelmi képességeinek külső szolgáltatói között hatékony és zökkenőmentes legyen pl.: rendszeres egyeztetések, közös képzések, folyamatos kommunikációt biztosító csatorna kialakítása.

4. A szervezetnek azonosítania kell a biztonsági eseménykezelő tevékenység szereplőit a külső szolgáltatók számára.
5. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a külső szolgáltatókkal történő kommunikációt és együttműködést annak érdekében, hogy biztosítsa a hatékony segítségnyújtást biztonsági események kezelésében.

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

IR-7(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.34. BIZTONSÁGI ESEMÉNYKEZELÉSI TERV

9.34. A szervezet:

9.34.1. A hatályos jogszabályoknak megfelelően kidolgozza a biztonsági eseménykezelési tervet, amely:

9.34.1.1. A szervezet számára iránymutatást ad a biztonsági események kezelési módjaira.

9.34.1.2. Ismerteti a biztonsági eseménykezelés struktúráját és szervezetét.

9.34.1.3. Átfogó képet nyújt arról, hogy a biztonsági eseménykezelés hogyan illeszkedik az általános szervezeti struktúrába.

9.34.1.4. Kielégíti az adott szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeit.

9.34.1.5. Meghatározza a bejelentésköteles biztonsági eseményeket.

9.34.1.6. Metrikákat alkalmaz a biztonsági eseménykezelési folyamatok működésének belső mérésére.

9.34.1.7. Meghatározza azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési folyamatok bővítésére, hatékonyabbá tételére és fenntartására.

9.34.1.8. Meghatározza a biztonsági eseményekkel kapcsolatos információmegosztás módját.

9.34.1.9. Meghatározott gyakorisággal felülvizsgálja a biztonsági eseménykezelési tervet, amelyet a szervezet által meghatározott személyek és szerepkörök jóváhagynak.

9.34.1.10. Meghatározza a biztonsági eseménykezelés felelőseit.

9.34.2. Kihirdeti a biztonsági eseménykezelési tervet a biztonsági eseményeket kezelő személyek és szervezeti egységek számára.

9.34.3. Frissíti a biztonsági eseménykezelési tervet, figyelembe véve az EIR és a szervezet változásait, vagy a terv megvalósítása, végrehajtása és tesztelése során felmerülő problémákat.

9.34.4. Ismerteti a biztonsági eseménykezelési terv változásait a szervezet által meghatározott biztonsági eseménykezelésért felelős személyzettel.

9.34.5. Gondoskodik arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető vagy módosítható.

MAGYARÁZAT

Fontos, hogy az érintett szervezet összehangolt megközelítést dolgozzon ki és alkalmazzon a biztonsági események kezelésére. A biztonsági eseményekre való reagálás szerkezetét és struktúráját a szervezeti célok és az üzleti funkciók határozzák meg. A reagálási képesség kialakításának része, hogy a szervezetek megvizsgálják a külső szervezetekkel, köztük a külső szolgáltatókkal és az ellátási láncban érintett egyéb szervezetekkel való együttműködés és információmegosztás lehetőségét. A személyes adatokat érintő biztonsági eseményekhez kapcsolódóan a szervezetnek rendelkeznie kell az értesítésre vonatkozó eljárással, amely alapján meghatározásra kerül az értesítendő szereplők köre (felügyeletet végző szervezetek, érintett személyek stb.).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia egy biztonsági eseménykezelési tervet. A tervnek ki kell elégítenie a szervezet feladatkörével, méretével, szervezeti felépítésével és funkcióival kapcsolatos egyedi igényeit. Meg kell határoznia a bejelentésköteles biztonsági eseményeket, és mérőszámokat kell alkalmaznia a biztonsági eseménykezelési folyamatok működésének belső mérésére.
2. A szervezetnek meg kell határoznia azokat az erőforrásokat és vezetői támogatást, amelyek szükségesek a biztonsági eseménykezelési folyamatok kialakítására, fenntartására, bővítésére és hatékonyabbá tételére. Emellett meg kell határoznia a biztonsági eseményekkel kapcsolatos információmegosztás módját.
3. A szervezetnek meghatározott gyakorisággal felül kell vizsgálnia a biztonsági eseménykezelési tervet, amelyet a szervezet által meghatározott személyek és szerepkörök jóváhagynak. Emellett meg kell határoznia a biztonsági eseménykezelés felelőseit.
4. A szervezetnek ki kell hirdetnie a biztonsági eseménykezelési tervet a biztonsági eseményeket kezelő személyek és szervezeti egységek számára.
5. A szervezetnek ismertetnie kell a biztonsági eseménykezelési terv változásait a szervezet által meghatározott biztonsági eseménykezelésért felelős személyzettel. Gondoskodnia kell arról, hogy a biztonsági eseménykezelési terv jogosulatlanok számára ne legyen megismerhető vagy módosítható.

6. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a biztonsági eseménykezelési tervet annak érdekében, hogy az naprakész és hatékony legyen.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés
7.2. Üzletmenet-folytonossági terv
7.13. Üzletmenet-folytonossági terv tesztelése
9.9.1. Biztonsági események kezelése
9.31. Segítségnyújtás a biztonsági események kezeléséhez
9.35. Információszivárgásra adott válaszlépések
12.17. A fizikai hozzáférések felügyelete
13.2. Rendszerbiztonsági terv
16.76.1. Fejlesztési folyamat, szabványok és eszközök
18.67. Információ kezelése és megőrzése

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

3.1.5.8. Biztonsági eseménykezelési terv

ISO/IEC 27001:2023 REFERENCIA

7.5.1; 7.5.2; 7.5.3; A.5.24

NIST SP 800-53 REV.5 REFERENCIA

IR-8

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

9.35. INFORMÁCIÓSZIVÁRGÁSRA ADOTT VÁLASZLÉPÉSEK

9.35. A szervezet az információszivárgásra az alábbi válaszokat adja:

9.35.1. Meghatározza, hogy mely személyek vagy szerepkörök felelnek az ilyen események kezeléséért.

9.35.2. Azonosítja az információszivárgásban érintett konkrét adatokat.

9.35.3. Olyan kommunikációs csatornán keresztül értesíti az információszivárgásról a meghatározott személyeket vagy szerepköröket, amely nem köthető az információszivárgáshoz.

9.35.4. Elszigeteli a jogosulatlan adatkezelésben érintett rendszert vagy rendszerelemet.

9.35.5. Eltávolítja az információkat a jogosulatlan adatkezelésben érintett rendszerből vagy rendszerelemből.

9.35.6. Azonosítja azokat a további rendszereket vagy rendszerelemeket, amelyek érintettek lehetnek a jogosulatlan adatkezelésben.

9.35.7. Végrehajtja a szervezet által meghatározott további intézkedéseket.

MAGYARÁZAT

Az információszivárgás ("information spillage") olyan esetekre utal, amikor olyan EIR-ekben helyeznek el információt, amelyek nem jogosultak ezen információk feldolgozására. Az információszivárgás akkor következik be, amikor az információról - amelyhez bizonyos besorolást vagy hatást társítanak - egy EIR-re történő átvitel során kiderül, hogy magasabb besorolással vagy nagyobb hatással rendelkezik. Ebben az esetben korrekciós intézkedésre van szükség. A válasz jellege a szivárgó információ besorolásán vagy hatásán, az EIR biztonsági képességein, a jogosulatlan adatkezelésben érintett adattároló konkrét jellegén és az engedélyezett hozzáféréssel rendelkező személyek hozzáférési engedélyein alapul. Az információszivárgás kommunikációja során ne kerüljenek említésre olyan módszerek, amelyek közvetlenül kapcsolódnak a tényleges szivárgáshoz, annak érdekében, hogy minimalizálják a jogosulatlan adatkezelés további terjedésének kockázatát, mielőtt a jogosulatlan adatkezelés elkülönítésre és megszüntetésre kerülne.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, hogy mely személyek vagy szerepkörök felelnek az információszivárgás kezeléséért.
2. A szervezetnek azonosítania kell az információszivárgásban érintett konkrét adatokat.
3. A szervezetnek olyan kommunikációs csatornán keresztül kell értesítenie az információszivárgásról a meghatározott személyeket vagy szerepköröket, amely nem köthető az információszivárgáshoz.
4. A szervezetnek el kell szigetelnie az EIR-t vagy rendszerelemet, amelyben a jogosulatlan adatkezelés történt.
5. A szervezetnek el kell távolítania az információkat az EIR-ből vagy rendszerelemből, amelyben a jogosulatlan adatkezelés történt.
6. A szervezetnek el kell távolítania az információkat a jogosulatlan adatkezelésben érintett rendszerből vagy rendszerelemből.
7. A szervezetnek azonosítania kell azokat a további EIR-eket vagy rendszerelemeket, amelyek érintettek lehetnek a jogosulatlan adatkezelésben.
8. A szervezetnek végre kell hajtania a saját maga által meghatározott további intézkedéseket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.2. Üzletmenet-folytonossági terv
9.27. A biztonsági események jelentése
15.20. Kockázatokra adott válasz

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

IR-9

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.36. Információszivárgásra adott válaszlépések – Képzés

9.36. A szervezet meghatározott gyakorisággal megtartja az információszivárgási események kezelésére vonatkozó képzést.

Magyarázat

Az érintett szervezet meghatározza az információszivárgási ("information spillage") események kezelésére vonatkozó követelményeket az eseménykezelési tervekben. Az eseménykezelési képzések rendszeres megtartása segít biztosítani, hogy az érintett szervezet munkavállalói tisztában legyenek az egyéni felelősségekkel és azzal, hogy milyen konkrét lépéseket kell megtenniük információszivárgással kapcsolatos esemény esetén.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia az információszivárgási események kezelésére vonatkozó követelményeket az eseménykezelési tervekben.
2. A szervezetnek rendszeresen képzéseket kell tartania az információszivárgási események kezeléséről.
3. A képzések során a szervezetnek meg kell bizonyosodnia arról, hogy a személyek tisztában vannak az egyéni felelősségeikkel és tudják milyen konkrét lépéseket kell tenniük, amikor információszivárgási események történnek.
4. A szervezetnek dokumentálnia kell a képzéseket, beleértve a képzés időpontját, a résztvevők listáját és a képzés tartalmát.
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a képzés anyagát annak érdekében, hogy hatékony és naprakész legyen.

Kapcsolódó intézkedések

3.2. Biztonságtudatossági képzés
3.9. Szerepkör alapú biztonsági képzés
7.10. A folyamatos működésre felkészítő képzés
9.2. Képzés a biztonsági események kezelésére

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

IR-9(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.37. INFORMÁCIÓSZIVÁRGÁSRA ADOTT VÁLASZLÉPÉSEK – SZIVÁRGÁST KÖVETŐ MŰVELETEK

9.37. A szervezet meghatározott intézkedéseket hajt végre annak érdekében, hogy az információszivárgásban érintett szervezethez köthető személyek folyamatosan el tudják látni kijelölt feladatukat, amíg az információszivárgásban érintett rendszereken javító intézkedések folynak.

MAGYARÁZAT

Az információszivárgásban ("information spillage") érintett EIR-eken végrehajtott korrektív intézkedések időigényesek lehetnek. A személyzetnek lehet, hogy nincs hozzáférése az érintett EIR-ekhez, amíg a korrektív intézkedések folyamatban vannak. Mindez kihathat a szervezet üzleti tevékenységére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azon személyek körét, akiknek munkája vagy bizonyos feladatai az EIR-el kapcsolatos információszivárgás miatt érintett lehet.
2. A szervezetnek biztosítania kell, hogy az érintett személyek folyamatosan el tudják látni feladataikat, még akkor is, ha az EIR-en javító intézkedések folynak. Ez magában foglalhatja a munkafolyamatok átirányítását, a munkakörülmények ideiglenes módosítását, vagy akár a személyzet ideiglenes áthelyezését is.
3. A szervezetnek meg kell terveznie és végre kell hajtania a szükséges javító intézkedéseket az EIR-en annak érdekében, hogy megakadályozza az információszivárgást.
4. A szervezetnek dokumentálnia kell a javító intézkedéseket, beleértve a beavatkozások időpontját, a végrehajtott műveleteket és azok eredményeit.
5. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a helyzetet annak érdekében, hogy biztosítsa a személyzet folyamatos működését és az EIR helyreállítását.

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

IR-9(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az eljárások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

9.38. Információszivárgásra adott válaszlépések – Illetéktelen hozzáférés

9.38. A szervezet meghatározott intézkedéseket alkalmaz azokkal a személyekkel szemben, akik olyan információkhoz férnek hozzá, amelyek kívül esnek hozzáférési jogosultságaikon.

Magyarázat

Az érintett szervezet biztosítja, hogy azok a személyek, akik kiszivárgott információkhoz férnek hozzá, tisztában legyenek a vonatkozó jogszabályokkal, irányelvekkel, szabályzatokkal, szabványokkal és útmutatókkal. Ez magában foglalja azokat a korlátozásokat is, amelyeket az ilyen információkhoz való hozzáférés alapján vezettet be a szervezet.
Az érintett szervezetnek szigorúan ellenőriznie kell, hogy ki férhet hozzá az EIR-hez, és azon belül milyen jogosultsággal rendelkezik az EIR-ben található információk megismerésére. Az EIR-ben tárolt információkhoz való jogosulatlan hozzáférés súlyos biztonsági kockázatot jelenthet, ezért az érintett szervezetnek megfelelő intézkedéseket kell hoznia annak érdekében, hogy megakadályozza az ilyen eseményeket.

A követelmény alkalmazásának lépései

1. A szervezetnek azonosítania kell azokat a személyeket, akik olyan információkhoz férnek hozzá, amelyek kívül esnek hozzáférési jogosultságaikon.
2. A szervezetnek olyan intézkedéseket kell alkalmaznia, amelyek megakadályozzák, hogy ezek a személyek hozzáférjenek olyan információkhoz, amelyekhez nincs jogosultságuk. Ez magában foglalhatja a hozzáférési jogosultságok szigorúbb ellenőrzését és az EIR-ben található információk védelmét.
3. A szervezetnek tájékoztatnia kell az egyéneket az információszivárgást érintő jogszabályokról, illetve belső szabályzatban foglaltakról. Ezáltal biztosítható, hogy a szervezethez köthető személyek tisztában vannak a jogosulatlan hozzáférés következményeivel, illetve az ahhoz kapcsolódó esetleges szabálysértésekkel.
4. A szervezetnek naplóznia kell a hozzáférési jogosultságokkal kapcsolatos tevékenységeket, beleértve a jogosulatlan hozzáféréseket és a hozzáférési jogosultságokkal kapcsolatos változások dokumentálását.

5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén módosítania kell a hozzáférési jogosultságokat. Ez által biztosíthatja, hogy csak a megfelelő személyek férjenek hozzá az EIR-ben tárolt információkhoz.

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

IR-9(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024