Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Kockázatkezelés

Verzió 1.0

2024

Tartalomjegyzék

15.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

15.1. A szervezet:

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

15.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó kockázatmenedzsment szabályzatot, amely

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

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

15.1.1.2. a kockázatelemzési és kockázatkezelési eljárásrendet, amely a kockázatmenedzsment szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

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

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

MAGYARÁZAT

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

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

Kapcsolódó intézkedések

1.10. Kockázatkezelési stratégia

14.12. Fegyelmi intézkedések

18.67. Információ kezelése és megőrzése

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

3.1.2.1. Kockázatelemzési és kockázatkezelési eljárásrend

ISO/IEC 27001:2023 referencia

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

NIST SP 800-53 rev.5 referencia

RA-1

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

15.2. BIZTONSÁGI OSZTÁLYBA SOROLÁS

15.2. A szervezet:

15.2.1. Biztonsági osztályba sorolja az EIR-t;

15.2.2. A rendszerbiztonsági tervben dokumentálja a biztonsági osztályba sorolás eredményeit, beleértve az azt alátámasztó indoklást is.

15.2.3. Ellenőrzi, hogy a szervezet vezetője jóváhagyta a biztonsági osztályba sorolási döntést.

MAGYARÁZAT

A biztonsági osztályok leírják a szervezeti működésre, a szervezeti eszközökre és az egyénekre gyakorolt lehetséges káros hatásokat vagy negatív következményeket, ha a szervezeti információ és rendszerek a bizalmasság, a sértetlenség vagy a rendelkezésre állás elvesztése miatt veszélybe kerülnek. A szervezetek a biztonsági osztályozásba sorolási folyamatot az egész szervezetre kiterjedően végzik, közvetlenül bevonva az informatikai felelősöket, az információbiztonsági felelősöket, a rendszerek tulajdonosait, az üzleti- és ügymeneti folyamatok felelőseit, valamint az adatgazdákat. A szervezetek figyelembe veszik a lehetséges hatásokat más szervezetekre nézve, valamint ha releváns, akkor a nemzetbiztonsági hatásokkal is számolni kell a szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal összhangban. A biztonsági osztályba sorolás elősegíti a EIR(-ek) rendszerelem leltárának fejlesztését, azzal, hogy rendszerelemeket rendel az információk feldolgozásához, tárolásához és továbbításához, valamint megjeleníti az ezekhez kapcsolódó biztonsági követelményt rendszerelem leltárra vonatkozó követelménnyel együtt. A biztonsági osztálybasorolást a rendszerfejlesztési életciklus során a szervezet felülvizsgálja annak biztosítása érdekében, hogy a biztonsági osztálybasorolás pontos és releváns maradhasson.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztonsági osztályba kell sorolnia az EIR-t.

2. A biztonsági osztályba sorolás eredményeit dokumentálnia kell a rendszerbiztonsági tervben, beleértve az azt alátámasztó indoklást is. Ez azt jelenti, hogy az érintett szervezetnek részletesen le kell írnia, hogy milyen potenciális káros hatásokat vett figyelembe, és hogy ezek alapján milyen biztonsági osztályba sorolta az EIR-t.

3. A szervezet vezetőjének vagy meghatalmazott képviselőjének jóvá kell hagynia a biztonsági osztályba sorolási döntést. A biztonsági osztályba sorolást szervezeti szinten kell végrehajtani, az információbiztonsági felelős(ök), az adatvédelmi tisztviselő(k), az EIR tulajdonosok, az alapfeladatok és üzleti folyamatok tulajdonosai, valamint az adatgazdák közvetlen bevonásával.
4. A szervezetnek az EIR fejlesztési életciklusa során rendszeresen felül kell vizsgálnia a biztonsági osztályba sorolást, hogy biztosítsa a biztonsági osztályok pontosságát és relevanciáját.

Kapcsolódó intézkedések

6.36. Rendszerelem leltár
11.4. Adathordozók tárolása
13.2. Rendszerbiztonsági terv
13.10. Biztonsági követelmények kiválasztása
13.11. Biztonsági követelmények testre szabása
1.7. Vállalati architektúra
15.4. Kockázatértékelés
15.10. Sérülékenységmonitorozás és szkennelés
15.20. Kockázatokra adott válasz

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

3.1.2.2. Biztonsági osztályba sorolás

ISO/IEC 27001:2023 referencia

A.5.12

NIST SP 800-53 rev.5 referencia

RA-2

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

15.3. BIZTONSÁGI OSZTÁLYBA SOROLÁS – HATÁSSZINTEK SÚLYOZÁSA

15.3. A szervezet elvégzi a szervezeti EIR-ek működési hatása szerinti rangsorolását annak érdekében, hogy még részletesebben meghatározhassa a rendszerek hatásszintjeit.

MAGYARÁZAT

Azok az érintett szervezetek, amelyek részletesebb hatásalapú kategóriákat szeretnének létrehozni a kockázatalapú döntéshozatalhoz, azok további alcsoportokra oszthatják az EIR-eket az eredeti EIR-kategorizálás alapján. Például egy közepes hatású EIR-en végrehajtott hatásalapú prioritizálás három új alcsoportot eredményezhet: alacsony-közepes EIR-ek, közepes-közepes EIR-ek és magas-közepes EIR-ek. A hatásalapú prioritizálást arra is lehet használni, hogy meghatározza azokat az EIR-eket, amelyek a jelek szerint nagyobb érdeklődést váltanak ki a támadókból, vagy kritikus veszteséget jelentenének egy állami vállalat vagy szervezet számára, amit néha magas értékű vagyontárgynak (ún. "high value asset") neveznek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az üzleti hatáselemzés hatókörét.
2. A szervezetnek a meghatározott szempontjai alapján el kell végeznie az üzleti hatáselemzést, amely képes támogatni a kockázatalapú döntéshozatalt, valamint az üzletmenet-folytonossági szabályzat és tervek elkészítését.
3. A szervezet vezetésének biztosítania kell, hogy az üzleti hatáselemzés elvégzéséhez és annak eredményeiből származó szükséges intézkedések elvégzéséhez biztosítja a szükséges erőforrást és anyagi ráfordítást.

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

RA-2(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

15.4. KOCKÁZATELEMZÉS

15.4. A szervezet:

15.4.1. Rendszerszintű kockázatelemzést végez, amely magába foglalja:

15.4.1.1. a rendszerre vonatkozó fenyegetések és sérülékenységek azonosítását;

15.4.1.2. a jogosulatlan hozzáférés, használat, közzététel, zavarás, módosítás vagy a rendszer megsemmisítésének valószínűségének és káros hatásainak megállapítását, valamint az általa feldolgozott, tárolt vagy továbbított információkra és minden kapcsolódó információra vonatkozóan;

15.4.1.3. személyes adatok feldolgozásából eredő, egyénekre vetített kedvezőtlen hatások valószínűségének és mértékének megállapítását.

15.4.2. Integrálja a szervezet, a szervezeti célok vagy üzleti folyamatok szempontjából végzett kockázatelemzés eredményeit és a kockázatkezelési döntéseket a rendszerszintű kockázatelemzésekkel.

15.4.3. Dokumentálja a kockázatelemzés eredményeit a kockázatelemzési jelentésben és a szervezet által meghatározott dokumentumokban.

15.4.4. Meghatározott gyakorisággal áttekinti a kockázatelemzés eredményeit.

15.4.5. Megismerteti a kockázatelemzés eredményeit a meghatározott személyekkel vagy szerepkörökkel.

15.4.6. Meghatározott gyakorisággal frissíti a kockázatelemzést vagy minden olyan esetben, amikor jelentős változások történnek a rendszerben, annak működési környezetében, vagy más olyan körülményekben, amelyek befolyásolhatják a rendszer biztonsági állapotát.

MAGYARÁZAT

A kockázatértékelések figyelembe veszik a fenyegetéseket, a sérülékenységeket, a káresemények bekövetkezésének valószínűségét, valamint a szervezet működésére és eszközeire, az egyénekre, más szervezetekre és a nemzetre gyakorolt hatásokat. A kockázatértékelések a külső felek által jelentett kockázatokat is figyelembe veszik, beleértve a szervezet által megbízott, rendszereket üzemeltető vállalkozókat, a szervezeti rendszerekhez hozzáféréssel rendelkező személyeket, a szolgáltatókat és a kiszervezett tevékenységeket.

A szervezetek a kockázatkezelési hierarchia mindhárom szintjén [azaz a szervezet szintjén, a célok és üzleti (ügymeneti) folyamatok szintjén vagy az EIR szintjén] és a rendszerfejlesztési

életciklus bármely szakaszában végezhetnek kockázatértékelést. A kockázatértékeléseket a kockázatkezelési keretrendszer különböző lépéseiben is el lehet végezni, beleértve az előkészítést, a kategorizálást, a biztonsági követelmények kiválasztását, a biztonsági intézkedések végrehajtását, a biztonsági követelmények és intézkedések értékelését, az engedélyezést és a felügyeletet. Fontos, hogy a kockázatértékelés folyamatos tevékenység, melyet a rendszerfejlesztési életciklus során rendszeresen el kell végezni.

A kockázatértékelések a rendszerrel kapcsolatos információkkal is foglalkozhatnak, beleértve a rendszertervet, a rendszerbiztonsági tervet, a rendszer tervezett felhasználását, a tesztelési eredményeket és az ellátási lánchoz kapcsolódó információkat vagy vagyontárgyakat. A kockázatértékelések fontos szerepet játszhatnak a biztonsági követelmények kiválasztásában, különösen a testreszabás alkalmazása során és a képességek meghatározásának legkorábbi szakaszaiban.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek rendszer szintű kockázatértékelést kell végeznie, amely magába foglalja az EIR-re vonatkozó fenyegetések és sérülékenységek azonosítását, melyben megállapítja a jogosulatlan hozzáférés, használat, közzététel, zavarás, módosítás vagy az EIR megsemmisítésének valószínűségét és káros hatásait, valamint az általa feldolgozott, tárolt vagy továbbított információkra és minden kapcsolódó információra vonatkozóan. Meg kell állapítania továbbá a személyes adatok feldolgozásából eredő, egyénekre vetített kedvezőtlen hatások valószínűségét és mértékét.
2. A szervezetnek össze kell hangolnia a szervezet, a szervezeti célok vagy alapfunkciók szempontjából végzett kockázatértékelés eredményeit és a kockázatkezelési döntéseket az EIR szintű kockázatértékelésekkel.
3. A szervezetnek dokumentálnia kell a kockázatértékelés eredményeit a kockázatértékelési jelentésben és a szervezet által meghatározott dokumentumokban.
4. A szervezetnek gondoskodnia kell róla, hogy a kockázatértékelés eredményeit a meghatározott személyekkel vagy szerepkörökkel megismertesse.
5. A szervezetnek meghatározott gyakorisággal felül kell vizsgálnia és frissítenie kell a kockázatértékelést, továbbá minden olyan esetben, amikor jelentős változások történnek az

EIR-ben, annak működési környezetében, vagy más olyan körülményekben, amelyek befolyásolhatják az EIR biztonsági állapotát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.6. Információcsere

5.11. Engedélyezés

6.15. Biztonsági hatásvizsgálatok

7.19. Biztonsági tárolási helyszín

7.23. Alternatív feldolgozási helyszín

8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

10.18. Karbantartó személyek

12.6. A fizikai belépés ellenőrzése

12.22. Látogatói hozzáférési naplók

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

3.1.2.3. Kockázatelemzés

ISO/IEC 27001:2023 REFERENCIA

6.1.2; 8.2; 9.3.2; A.8.8

NIST SP 800-53 REV.5 REFERENCIA

RA-3

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

15.5. KOCKÁZATELEMZÉS – ELLÁTÁSI LÁNC

15.5. A szervezet:

15.5.1. Felméri az ellátási lánc kockázatait a meghatározott EIR-ei, rendszerelemei és rendszerszolgáltatásai vonatkozásában.

15.5.2. Meghatározott időközönként frissíti az ellátási lánc kockázatelemzését, amikor jelentős változások történnek az érintett ellátási láncban, vagy amikor a rendszer, a működési környezet vagy más körülmények változása esetén szükségessé válhat az ellátási lánc megváltoztatására.

MAGYARÁZAT

Az ellátási láncra vonatkozó események közé tartozik a működési zavar, hibás eszközök vagy alkatrészek használata, hamis eszközök beszerzése és rendszerbe illesztése, lopás, rosszindulatú fejlesztési gyakorlatok, helytelen szállítási gyakorlatok és kártékony kódok rendszerbe jutása. Ezek az események jelentős hatással lehetnek egy EIR és annak információinak bizalmasságára, sértetlenségére vagy rendelkezésre állására, és ezért kedvezőtlenül befolyásolhatják a szervezet működését, a szervezet eszközeit, az egyéneket, más szervezeteket és a nemzetet. Az ellátási láncra vonatkozó események szándékosak vagy véletlenek is lehetnek, és bármikor bekövetkezhetnek az EIR életciklusa során. Az ellátási lánc kockázatának elemzése segíthet az érintett szervezetnek azonosítani azokat az EIR-eit vagy rendszerelemeket, amelyeknél további ellátási lánc kockázatcsökkentő intézkedések szükségesek.

Az érintett szervezetnek rendszeresen frissítenie kell az ellátási lánc kockázatértékelését, különösen akkor, ha jelentős változások történnek az érintett ellátási láncban, vagy amikor az EIR, a működési környezet vagy más körülmények változása esetén szükségessé válhat az ellátási lánc megváltoztatása. A megfelelően részletes dokumentáció vezetése segít az érintett szervezetnek nyomon követni az ilyen változásokat és időben reagálni rájuk.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie az ellátási lánc kockázatait az EIR-ei, rendszerelemei és rendszerszolgáltatásai szempontjából.

2. A szervezetnek meg kell határoznia, hogy mely EIR-ek vagy rendszerelemek esetében szükségesek további ellátási lánc kockázatcsökkentő intézkedések. Ez az elemzés segíthet az érintett szervezetnek azonosítani azokat az EIR-eket, amelyeknél nagyobb a kockázat.

3. A szervezetnek rendszeresen frissítenie kell az ellátási lánc kockázatértékelését. Ez különösen fontos, amikor jelentős változások történnek az érintett ellátási láncban, vagy amikor az EIR, a működési környezet vagy más körülmények változása esetén szükségessé válhat az ellátási lánc megváltoztatása.
4. A szervezetnek folyamatosan dokumentálnia kell az ellátási lánc kockázatértékelését és annak változásait.

Kapcsolódó intézkedések

15.2. Biztonsági osztályba sorolás
15.21. Rendszerelemek kritikusságának elemzése
1.21. Ellátási lánc kockázatkezelési stratégiája
19.2. Ellátási láncra vonatkozó kockázatkezelési szabályzat

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

RA-3(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

15.6. KOCKÁZATELEMZÉS – KÜLÖNBÖZŐ FORRÁSOKBÓL SZÁRMAZÓ INFORMÁCIÓK FELHASZNÁLÁSA

15.6. A szervezet minden lehetséges forrásból (all-source-intelligence) származó információt felhasznál a kockázatok értékelésében.

MAGYARÁZAT

Az érintett szervezet minden lehetséges forrásból (all-source intelligence) származó információt felhasznál a kockázatok értékelésében. Az all-source-intelligence magában foglalja az összes elérhető forrásból származó információt, beleértve a nyilvánosan elérhető vagy nyílt forrású információkat, és a hírszerzés különböző formáit (HUMINT, SIGINT, GEOINT stb). Az all-source-intelligence-t az EIR-ben található sérülékenységek (szándékos és véletlen) kockázatának elemzésére használják, amelyek a fejlesztési, gyártási és szállítási folyamatokból, az emberi tényezőből és a környezetből származnak. A kockázatértékelést az ellátási lánc több szintjén is el lehet végezni a beszállítókra vonatkozóan. Az érintett szervezet megállapodásokat köthet az all-source-intelligence információk vagy az abból származó döntések megosztására más szervezetekkel, amennyiben ez helyénvaló. A dokumentálás során az érintett szervezet figyelembe veszi az all-source-intelligence információkat, hogy informált döntéseket hozhasson az EIR kockázatairól.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek minden lehetséges forrásból származó információt fel kell használnia a kockázatok értékelésében.
2. A szervezetnek az EIR kockázatának elemzésére kell használnia az összes lehetséges forrásból származó információt.
3. A szervezetnek a beszállítókon is el kell végeznie a kockázatelemzést, úgy, hogy az elegendő legyen a kockázatok kezeléséhez.
4. A szervezetnek megállapodásokat kell kötnie az összes forrásból származó információ vagy a kapcsolódó döntések megosztására más szervezetekkel, amennyiben ezt helytállónak ítéli.
5. A szervezetnek dokumentálnia kell az összes lehetséges forrásból származó információ felhasználásáról és a kockázatelemzés eredményeiről.

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

RA-3(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

15.7. KOCKÁZATELEMZÉSI ÉS KOCKÁZATKEZELÉSI ELJÁRÁSREND – DINAMIKUS FENYEGETÉSFELISMERÉS

15.7. A szervezet folyamatosan értékeli az aktuális kiberfenyegetettségi helyzetét az általa meghatározott eszközökkel.

MAGYARÁZAT

Az összegyűjtött fenyegetettségi információk beépülnek az érintett szervezet információbiztonsági műveleteibe, hogy biztosítsák az eljárások frissítését a változó fenyegetettségi környezetnek megfelelően. Például magasabb fenyegetettségi szintek esetén az érintett szervezet megváltoztathatja a bizonyos műveletek végrehajtásához szükséges jogosultságokat vagy megerősítheti hitelesítési eszközeit, gyakorlatát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell határoznia azokat az eszközöket, amelyekkel értékelni kívánja a kiberfenyegetettségi helyzetét. Ez magában foglalhatja a különböző kiberbiztonsági szoftvereket, hálózati monitorozó eszközöket, valamint a fenyegetési információgyűjtő szolgáltatásokat és/vagy eszközöket.
2. A szervezetnek folyamatosan monitoroznia kell az EIR-jét, hogy azonosítsa az esetleges biztonsági réseket vagy fenyegetéseket. Ez magában foglalhatja a rendszeres naplóelemzést, a hálózati forgalom monitorozását, valamint a rendszeres biztonsági ellenőrzéseket.
3. A szervezetnek rendszeresen értékelnie kell kiberfenyegetettségi helyzetét az általa meghatározott eszközökkel. Ez magában foglalhatja a fenyegetési információgyűjtési jelentések elemzését, a kiberbiztonsági események elemzését, valamint a biztonsági események utólagos elemzését.
4. A szervezetnek reagálnia kell az észlelt fenyegetésekre. Ez magában foglalhatja a biztonsági rések azonnali javítását, a fenyegetések elhárítását, valamint a biztonsági intézkedések szükség szerinti módosítását.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kiberbiztonsági szabályzatait, eljárásrendjeit, valamint eljárásait, hogy biztosítsa azok relevanciáját és hatékonyságát a változó kiberfenyegetettségi környezetben.

Kapcsolódó intézkedések

3.2. Biztonságtudatossági 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

RA-3(3)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az eszközök meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

15.8. KOCKÁZATELEMZÉSI ÉS KOCKÁZATKEZELÉSI ELJÁRÁSREND – PREDIKTÍV ELEMZÉS

15.8. A szervezet fejlett, automatizált elemzési képességeket alkalmaz, hogy előre jelezze és azonosítsa a meghatározott EIR-ek vagy rendszerelemek kockázatait.

MAGYARÁZAT

Még egy megfelelő erőforrásokkal ellátott szervezeti biztonsági műveleti központ (Security Operations Center - SOC) vagy számítógépes incidens reagáló csapat (Computer Incident Response Team - CIRT) is könnyen feldolgozhatatlan mennyiségű információval találhatja szemben magát, amelyet a beállított biztonsági eszközök és berendezések széles körű alkalmazása generál, hacsak nem alkalmaz fejlett automatizálást és elemzőeszközöket a begyűjtött adatok elemzésére. A fejlett automatizálási és analitikai képességeket támogathatják mesterséges intelligencia megoldások, beleértve a gépi tanulást. Példák közé tartozik az automatizált fenyegetés felfedezés és válasz, ("Automated Threat Discovery and Response") amely magában foglalja a széleskörű adatgyűjtést, a kontextus alapú elemzést és az adaptív válasz képességeket. Érdemes azonban megjegyezni, hogy a kifinomult támadók (pl. APT csoportok) képesek lehetnek információt kinyerni a fejlett analitikára használt eszközökből, és átképezhetik a gépi tanuló algoritmust, hogy a saját rosszindulatú tevékenységüket ártalmatlannak minősítsék. Ennek megfelelően a gépi tanulást minden esetben emberi felügyeletnek kell kiegészítenie, hogy biztosítsa, a kifinomult támadók nem képesek elrejteni tevékenységüket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy megfelelő erőforrással ellátott biztonsági műveleti központot (SOC) vagy számítógépes incidens reagáló csoportot (CIRT).
2. A szervezetnek fejlett automatizálást és analitikai képességeket kell alkalmaznia, hogy kezelni tudja a biztonsági eszközök és berendezések által generált nagymennyiségű információt. A szervezet megfontolhatja, hogy mesterséges intelligencia megoldásokat alkalmaz a begyűjtött nagymennyiségű információ feldolgozására, a fejlett automatizálás és analitikai képességek támogatására.

4. A szervezetnek fontolóra kell vennie, hogy automatizált fenyegetés felfedezési és válaszadási képességeket ("Automated Threat Discovery and Response") alkalmazzon.
5. Amennyiben a szervezet valamilyen mesterséges intelligencia megoldást alkalmaz, úgy emellett emberi felügyeletet kell alkalmaznia, hogy biztosítsa, a kifinomult támadók nem képesek elrejteni tevékenységüket.
8. A szervezetnek folyamatosan naplóznia kell, hogy nyomon követhesse és elemezhesse az EIR-ekben történő tevékenységeket és eseményeket.

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

RA-3(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek illetve a fejlett, automatizált elemzési képességek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

15.9. SÉRÜLÉKENYSÉGEK ELLENŐRZÉSE

15.9. A szervezet:

15.9.1. Meghatározott folyamat szerint rendszeresen vagy eseti jelleggel ellenőrzi az EIR sérülékenységeit, illetve minden olyan esetben, amikor új, az EIR-t potenciálisan érintő sérülékenységeket azonosítanak és jelentenek.

15.9.2. Kijavítja a valós sérülékenységeket a meghatározott válaszidőn belül, a kockázatkezelési eljárásoknak megfelelően.

MAGYARÁZAT

A biztonsági intézkedés az EIR-ek vonatkozásában releváns sérülékenységek figyelemmel kísérését foglalja magába, valamint azok belső eljárárásrendekkel összhangban történő javítását. Ilyen tevékenységnek tekintendő az NBSZ NKI, a jelentős gyártók, valamint egyéb iparági szereplők által publikált sérülékenységek nyomonkövetése, és a kiadott biztonsági frissítések, valamint új szoftver- és firmware verziók telepítése. A sérülékenységek ellenőrzésének folyamata, amennyiben technológiai szempontból lehetséges, megvalósítható az NBSZ NKI ASR rendszerének igénybevételével az arra jogosult szervezetek esetében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A sérülékenységekről a meghatározott szerepkörben lévő személy, meghatározott rendszerességgel tájékozódik pl. a https://nki.gov.hu/figyelmeztetesek/cve-serulekenysegek/ vagy a https://cve.mitre.org/ oldalakon.

KAPCSOLÓDÓ INTÉZKEDÉSEK

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

ISO/IEC 27001:2023 REFERENCIA

NIST SP 800-53 REV.5 REFERENCIA

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

15.10. SÉRÜLÉKENYSÉGMENEDZSMENT

15.10. A szervezet:

15.10.1. Meghatározott folyamat szerint rendszeresen vagy eseti jelleggel szkenneli az EIR sérülékenységeit, illetve minden olyan esetben, amikor új, az EIR-t potenciálisan érintő sérülékenységeket azonosítanak és jelentenek.

15.10.2. Olyan sérülékenységmenedzsment eszközöket és technikákat alkalmaz, amelyek elősegítik az eszközök közötti átjárhatóságot és automatizálják a sérülékenységkezelési folyamat egyes lépéseit a következők szerint:

15.10.2.1. felsorolja a platformokat, szoftverhibákat és helytelen konfigurációkat;

15.10.2.2. ellenőrző listákat és tesztelési eljárásokat alkalmaz; és

15.10.2.3. méri az egyes sérülékenységek hatásait.

15.10.3. Elemzi a sérülékenységmenedzsment jelentéseket és a vizsgálatok eredményeit,

15.10.4. kijavítja a valós sérülékenységeket a meghatározott válaszidőn belül, a kockázatkezelési eljárásoknak megfelelően.

15.10.5. Megosztja a sérülékenységmenedzsment folyamatból és a követelmények értékeléséből származó információkat a meghatározott személyekkel vagy szerepkörökkel, hogy segítsenek kiküszöbölni a hasonló sérülékenységeket más rendszerekben.

15.10.6. Olyan sérülékenységmenedzsment eszközöket alkalmaz, amelyek képesek a vizsgálandó sérülékenységek egyszerű frissítésére.

MAGYARÁZAT

Az EIR-ek biztonsági osztálya meghatározza a sérülékenységi vizsgálatok gyakoriságát és mélységét. A szervezet meghatározza az összes EIR-e, illetve azok rendszerelemeinek szükséges biztonsági vizsgálatát, biztosítva, hogy a potenciális biztonsági réseket tartalmazó eszközök, például a hálózatra kötött nyomtatók, szkennerek és másolók se maradjanak figyelmen kívül. Az egyedileg fejlesztett szoftverek biztonsági vizsgálatai eltérő megközelítéseket igényelhetnek, például statikus elemzést, dinamikus elemzést, bináris elemzést vagy a három megközelítés valamilyen egyvelegét. A szervezetek ezeket az elemzési megközelítéseket különböző eszközökben (pl. webalkalmazás szkennerek, statikus elemző eszközök, bináris elemzők) és forráskód-vizsgálatok során is használhatják. A biztonsági vizsgálat például tartalmazhatja patch-ek vizsgálatát, olyan funkciók, portok, protokollok és

szolgáltatások vizsgálatát, amelyeknek nem szabadna elérhetőnek lenniük felhasználói eszközök által, helytelenül konfigurált vagy helytelenül működtetett konfigurációk vizsgálatát. A szervezet, vizsgálata során használja, de legalábbis figyelembe veszi a nemzetközi standardokat, úgy, mint, amelyek segítenek a sérülékenységek feltárásában és definiálásában - Common Vulnerability and Exposures (CVE), amelyek a sérülékenységek meghatározására (OVAL) használatosak, továbbá lehet a sérülékenységre vonatkozó információk javasolt forrása - Common Weakness Evaluation (CWE), valamint a Common Vulnerability Scoring System (CVSS), mely egy adott sérülékenység kockázatát segít meghatározni. A biztonsági intézkedés nem követeli meg a teljes folyamat automatizálását, mindössze annak egyes lépéseiben kell ilyen eszközöket alkalmazni. A sérülékenységek szkennelési folyamatának automatizálása, amennyiben technológiai szempontból lehetséges, megvalósítható az NBSZ NKI ASR rendszerének igénybevételével az arra jogosult szervezetek esetében.

A 15.10.1. pontban meghatározott biztonsági intézkedésnek lehet tekinteni az NBSZ NKI, vagy az arra jogosult gazdálkodó szervezet által végrehajtott Ibtv. szerinti sérülékenységvizsgálatot.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek rendszeresen vagy eseti jelleggel szkennelnie kell az EIR sérülékenységeit egy meghatározott folyamat szerint, illetve minden olyan esetben, amikor új, az EIR-t potenciálisan érintő sérülékenységeket azonosítanak és jelentenek.
2. A szervezetnek olyan sérülékenységmonitorozó eszközöket és technikákat kell alkalmaznia, amelyek elősegítik az eszközök közötti átjárhatóságot és automatizálják a sérülékenységkezelési folyamat egyes lépéseit; amelyek képesek a sérülékenységek naplózására, és annak biztosítására, hogy ezek az eszközök azonosítják és jelentik az új sérülékenységeket; képesek új szkennelési módszerek kifejlesztésére; képesek a sérülékenységek hatásának mérésére; és biztosítja, hogy ezek az eszközök, technikák és módszerek használják, de legalább figyelembe veszik a nemzetközileg elfogadott standardokat (CVE, OVAL, CWE, CVSS).
3. A szervezetnek elemeznie kell a sérülékenységmonitorozás és -szkennelés jelentéseit és azok eredményeit.
4. A szervezetnek ki kell javítnia a valós sérülékenységeket a meghatározott válaszidőn belül, és a kockázatkezelési eljárásoknak megfelelően.

5. A szervezetnek gondoskodnia kell róla, hogy a sérülékenységmonitorozási és -szkennelési folyamatból és a követelmények értékeléséből származó információkat a meghatározott személyekkel vagy szerepkörökkel megossza, hogy segítsenek kiküszöbölni a hasonló sérülékenységeket más EIR-ekben.

6. A szervezetnek olyan csatornákat és folyamatokat kell alkalmaznia, amelyek képesek a sérülékenységekről szóló jelentések fogadására a nagyközönségtől. Ez módszer lehet olyan egyszerű, mint egy folyamatosan figyelt e-mail cím vagy egy webes űrlap, amely képes fogadni a jelentéseket, beleértve a jóhiszemű kutatást és a sérülékenységek jelentését a szervezet számára.

7. A szervezetnek fontolóra kell vennie, hogy pénzügyi ösztönzőket (ún. "bug bounty" programok) alkalmaz, hogy tovább ösztönözze a külső biztonsági kutatókat a felfedezett sérülékenységek bejelentésére. A bug bounty programok a szervezet igényei alapján lehetnek privátak (meghívásos alapúak), ebben az esetben a külső biztonsági kutató(k)nak további jogosultságok biztosíthatók, illetve publikusak, amely során nem kerül többletjogosultság megadásra. A privát és publikus bug bounty programok egymással párhuzamosan is futtathatók.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.2. Biztonsági értékelések

5.14. Folyamatos felügyelet

5.20. Behatolásvizsgálat (penetration testing)

6.2. Alapkonfiguráció

6.15. Biztonsági hatásvizsgálatok

6.23. Konfigurációs beállítások

6.36. Rendszerelem leltár

15.2. Biztonsági osztályba sorolás

15.4. Kockázatértékelés

16.66. Fejlesztői biztonsági tesztelés

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

3.3.5.3. Sérülékenység teszt

ISO/IEC 27001:2023 REFERENCIA

A.8.8

NIST SP 800-53 REV.5 REFERENCIA

RA-5

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

15.11. SÉRÜLÉKENYSÉGMENEDZSMENT – SÉRÜLÉKENYSÉGI ADATBÁZIS FRISSÍTÉSE

15.11. A szervezet meghatározott gyakorisággal, valamint minden új vizsgálat megkezdése előtt, továbbá új sérülékenységek azonosítása és jelentése esetén frissíti az EIR-ben szkennelt sérülékenységek körét.

MAGYARÁZAT

A szervezet – az általa meghatározott gyakorisággal – frissíti az ismert sérülékenységek listáját, valamint minden ellenőrzés előtt és minden alkalommal, amikor releváns sérülékenységet jelentenek be.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell állítania egy rendszeres időközönkénti frissítést az EIR-ben szkennelt sérülékenységek listájához. Ez a gyakoriság lehet heti, havi, vagy akár napi, attól függően, hogy milyen gyorsan változik az EIR környezete és milyen gyakran találnak új sérülékenységeket.
2. A szervezetnek minden új szkennelés megkezdése előtt frissítenie kell az EIR-ben szkennelt sérülékenységek listáját. Ez biztosítja, hogy az új szkennelés során az összes ismert sérülékenység figyelembe legyen véve.
3. A szervezetnek azonnal frissítenie kell az EIR-ben szkennelt sérülékenységek listáját, ha új sérülékenységet azonosítanak és jelentenek. Ez lehetővé teszi, hogy az érintett szervezet gyorsan reagáljon az új sérülékenységre, és megtegye a szükséges lépéseket a sérülékenység kezelésére.
4. A szervezetnek naplóznia kell az EIR-ben szkennelt sérülékenységek listájának frissítéseit.
5. A szervezetnek rendszeresen ellenőriznie kell az EIR-ben szkennelt sérülékenységek listáját, hogy biztosítsa, hogy a lista naprakész és teljes. Ez magában foglalhatja a lista áttekintését, a hiányzó sérülékenységek hozzáadását, és a már nem releváns sérülékenységek eltávolítását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

18.37. Biztonsági riasztások és tájékoztatások

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

3.3.5.3. Sérülékenység teszt

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

RA-5(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

15.12. SÉRÜLÉKENYSÉGMENEDZSMENT – A LEFEDETTSÉG SZÉLESSÉGE ÉS MÉLYSÉGE

15.12. A szervezet meghatározza a sérülékenységmenedzsment folyamat hatókörét és mélységét.

MAGYARÁZAT

A sérülékenységszkennelés hatóköre kifejezhető az EIR-en belüli elemek százalékában, az EIR-ek egyes típusai, az EIR-ek kritikussága vagy az ellenőrizendő sérülékenységek száma szerint. Ezzel szemben a sérülékenységszkennelés lefedettségének mélysége kifejezhető a rendszertervezés azon szintjeként, amelyet a szervezet nyomon kíván követni. A szervezetek a sérülékenységszkennelés lefedettségének elégséges mértékét a kockázattűrő képességük és más tényezők figyelembevételével határozhatják meg. A szkennelő eszközök és ezen eszközök konfigurálásának módja befolyásolhatja a mélységet és a lefedettséget. A kívánt mélység és lefedettség eléréséhez több szkennelő eszközre is szükség lehet.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a sérülékenységszkennelés hatókörét. Ez lehet a rendszerelemek százalékos aránya, a rendszertípusok, a rendszerek kritikussága vagy a vizsgálandó sérülékenységek száma.
2. A szervezet ezután meghatározza a sérülékenységszkennelés mélységét. Ez kifejezhető az EIR tervezési szintjének mértékében, amelyet a szervezet monitorozni szándékozik.
3. A szervezet megállapíthatja a sérülékenységszkennelés hatókörének elegendőségét a kockázattűrő képességéhez és más tényezőkhöz képest.
4. A szervezetnek dokumentálnia kell a sérülékenységszkennelés folyamatáról és eredményeiről, hogy nyomon követhesse a változásokat és szükség esetén korrigálhassa a szkennelési stratégiát.

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

RA-5(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

15.13. SÉRÜLÉKENYSÉGMENEDZSMENT – FELFEDEZHETŐ INFORMÁCIÓK

15.13. A szervezet megállapítja, hogy milyen információk érhetők el az EIR-ről, annak kompromittálása nélkül, és ez alapján szükség esetén korrekciós intézkedéseket hajt végre.

MAGYARÁZAT

A felfedezhető információk olyan információkat tartalmazhatnak, melyeket a támadók az EIR közvetlen kompromittálása nélkül ismerhetnek meg. Ezt úgy tehetik meg, hogy információt gyűjtenek EIR által kibocsátott adatokból, vagy részletes kereséseket végeznek az online térben. A korrekciós intézkedések magukban foglalhatják a megfelelő szervezeti felelős értesítését, az információk eltávolítását, vagy az információs rendszer konfigurálását, oly módon, hogy az elérhető információk kevésbé legyenek relevánsak vagy informatívak egy támadó számára.

Ilyen biztonsági intézkedésnek lehet tekinteni az NBSZ NKI, vagy az arra jogosult gazdálkodó szervezet által végrehajtott Ibtv. szerinti sérülékenységvizsgálatot, amennyiben az kiterjedt a kompromittálás nélkül felfedhető információk gyűjtésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell, hogy milyen információk érhetők el az EIR-ről anélkül, hogy azt kompromittálnák. Ezek olyan információk melyeket az EIR bocsát ki vagy amelyek részletes, az online térben lefolytatott keresésekkel megismerhetők. A szervezet ezt többféle módon is megteheti, például időszakos OSINT (nyílt információgyűjtés) vizsgálat elvégzésével és/vagy a sötét weben (dark web) fellelhető információk folyamatos monitorozásával. Emellett a szervezet időszakosan elvégzett sérülékenységvizsgálatokkal is azonosíthatja az említett típusú információkat.
2. Miután a szervezet azonosította a felfedezhető információkat, korrekciós intézkedéseket hajt végre. Ezek az intézkedések magukban foglalhatják a megfelelő személyzet értesítését, a kijelölt információk eltávolítását, vagy az EIR módosítását annak érdekében, hogy a kijelölt információk kevésbé relevánsak vagy vonzóak legyenek kívülállók számára.

3. A szervezetnek figyelembe kell vennie, hogy ez a folyamat kizárja azokat az információkat, amelyek szándékosan felfedezhetők, és amelyek részét képezhetik egy félrevezető és információgyűjtő képességnek, amelyet a szervezet telepített (pl.: honeypot).
4. A szervezetnek dokumentálnia kell az azonosított információkat, illetve az azok ismeretében végrehajtott korrekciós intézkedéseket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.44. Információk kiszivárgásának figyelemmel kísérése

17.79. Csapdák alkalmazása

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

3.3.5.3. Sérülékenység teszt

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

RA-5(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a korrekciós intézkedések meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

15.14. SÉRÜLÉKENYSÉGMENEDZSMENT – PRIVILEGIZÁLT HOZZÁFÉRÉS

15.14. A szervezet privilegizált hozzáférést biztosít a meghatározott rendszerelemekhez a szervezet által meghatározott sérülékenységmenedzsment tevékenységek elvégzéséhez.

MAGYARÁZAT

Bizonyos esetekben a sérülékenységszkennelés jellege fokozottabb (intrusive) lehet, illetve a vizsgálat tárgyát képező információs rendszerelem bizalmas információkat, illetve személyes adatokat is tartalmazhat. A privilegizált hozzáférési jogosultság a kiválasztott rendszerelemekhez megkönnyíti az alaposabb sérülékenységszkennelést.
Ilyen biztonsági intézkedésnek lehet tekinteni az NBSZ NKI, vagy az arra jogosult gazdálkodó szervezet által végrehajtott Ibtv. szerinti sérülékenységvizsgálat, amennyiben az privilegizált hozzáférési jogosultság felhasználásával történt.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia azokat a rendszerelemeket, amelyekhez privilegizált hozzáférést kíván biztosítani a sérülékenységszkennelés elvégzéséhez.
2. A szervezetnek privilegizált hozzáférést kell biztosítania a meghatározott rendszerelemekhez a szervezet által meghatározott sérülékenységszkennelési tevékenységek elvégzéséhez.
6. A szervezetnek biztosítania kell, hogy a sérülékenységszkennelést végző személyek, csoportok vagy szolgáltatások megfelelő minőségben képesek a feladat elvégzésére, és hogy a vizsgálatok nem veszélyeztetik az EIR biztonságát vagy működését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.5.3. Sérülékenység teszt

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

RA-5(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek illetve a sérülékenységszkennelési tevékenységek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

15.15. SÉRÜLÉKENYSÉGMENEDZSMENT – AUTOMATIZÁLT TRENDELEMZÉSEK

15.15. A szervezet meghatározott automatizált mechanizmusok segítségével összehasonlítja a sérülékenységszkennelések eredményeit.

MAGYARÁZAT

A sérülékenységszkennelés eredményeit elemző automatizált mechanizmusok segíthetnek felismerni trendeket és támadási mintákat az EIR sérülékenységeinek vonatkozásában.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és alkalmaznia kell azokat a automatizált helymeghatározást támogató eszközöket, amelyek segítségével képes lesz összehasonlítja a sérülékenységszkennelések eredményeit.
2. A szervezetnek biztosítania kell, hogy ezek az automatizált mechanizmusok képesek legyenek segítséget nyújtani a szervezet számára a sérülékenységszkennelések eredményeinek összehasonlításában.
3. A szervezetnek össze kell vetnie a különböző időpontokban elvégzett sérülékenységszkennelések eredményeit, annak érdekében, hogy felismerje a trendeket és a támadási mintákat.
4. A szervezetnek biztosítania kell, hogy az automatizált mechanizmusok megfelelően működnek, és képesek továbbra is összehasonlítani a sérülékenységszkennelések eredményeit. Ez magában foglalhatja az automatizált mechanizmusok rendszeres tesztelését és karbantartását is.
5. A szervezetnek elemeznie kell az összehasonlító elemzés eredményeit, és meg kell határoznia a szükséges lépéseket a sérülékenységek kezelésére. Ez magában foglalhatja a sérülékenységek javítását, az EIR védelmi intézkedéseinek megerősítését, vagy a támadási mintákra adott válaszok kidolgozását.

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

RA-5(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

15.16. SÉRÜLÉKENYSÉGMENEDZSMENT – NAPLÓBEJEGYZÉSEK FELÜLVIZSGÁLATA

15.16. A szervezet átvizsgálja a korábbi naplóbejegyzéseket, hogy megállapítsa, hogy egy meghatározott, az EIR-ben azonosított sérülékenységet korábban kihasználták-e egy meghatározott időszakban.

MAGYARÁZAT

A korábbi naplóbejegyzéseket felülvizsgálja a szervezet annak megállapítására, hogy egy EIR-ben nemrégiben észlelt sérülékenységet korábban kihasznált-e egy támadó. A felülvizsgálat fontos információkat szolgáltathat a forenzikus elemzésekhez. A felülvizsgálat segíthet azonosítani többek között a korábbi behatolás mértékét, a támadás során alkalmazott módszereket, a kiszivárgott vagy módosított szervezeti információkat, a szervezeti célokra vagy üzleti képességekre gyakorolt hatást, valamint a támadás időtartamát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell az EIR-ben azokat a sérülékenységeket, amelyeket ki lehetett volna használni a meghatározott időszakban.
2. A szervezetnek meg kell vizsgálnia a korábbi naplóbejegyzéseket, annak érdekében, hogy megállapítsa, volt-e olyan esemény, amely a sérülékenység kihasználására utal. A felülvizsgálat eredményét a szervezetnek dokumentálnia kell.
3. Amennyiben a naplóbejegyzések felülvizsgálat alapján a szervezet megállapítja, hogy az EIR-ben azonosított sérülékenységet kihasználta egy támadó, azt a szervezetnek biztonsági eseményként kell kezelnie és a biztonsági esemény kezelésére vonatkozó szabályokat, illetve eljárásrendeket követve meg kell tennie a szervezetnek a szükséges intézkedéseket.
4. A szervezetnek fel kell használnia a naplóbejegyzések elemzésének eredményeit és szükség esetén le kell vonnia belőle a megfelelő tanulságokat, annak érdekében, hogy a jövőbeni támadásokat megelőzze.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.38. A naplóbejegyzések megőrzése

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

RA-5(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

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

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

15.17. SÉRÜLÉKENYSÉGMENEDZSMENT – ÉSZLELT INFORMÁCIÓK ÖSSZEKAPCSOLÁSA

15.17. A szervezet a sérülékenységmenedzsment eszközök kimeneteit annak érdekében korrelálja, hogy megállapítsa az összetett sérülékenységek és többlépcsős támadási vektorok jelenlétét.

MAGYARÁZAT

A támadási vektor egy olyan útvonal vagy eszköz, amelyen keresztül a támadó hozzáférhet egy EIR-hez annak érdekében, hogy kártékony kódot juttasson be és/vagy információt szivárogtasson ki. A szervezetek ún. "támadási fákat" (attack trees) használhatnak annak bemutatására, hogy a támadók rosszindulatú tevékenységei hogyan hatnak egymásra és hogyan kombinálódnak, ezáltal káros hatásokat vagy negatív következményeket idézzenek elő az EIR-ekre és a szervezetekre nézve. Az ilyen információk a sérülékenységszkennelő eszközökből származó korrelált adatokkal együtt egyértelműbbé tehetik az összetett sérülékenységekkel és többlépcsős támadási vektorokkal kapcsolatos információkat. A sérülékenységszkenneléssel kapcsolatos információk korrelációja különösen fontos, amikor a szervezetek régebbi technológiákról újabb technológiákra állnak át (pl. IPv4-ről, IPv6-ra átállás történt). Az ilyen átmenetek során előfordulhat, hogy egyes EIR-eket vagy rendszerelemek kezeletlenül (pl. frissítés nélkül) maradnak, amit kihasználhatnak a támadók.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell szereznie a megfelelő sérülékenységszkennelő eszközöket, amelyek képesek az EIR-ben található sérülékenységek azonosítására.
2. A szervezetnek rendszeresen ellenőriznie és korrelálnia kell a sérülékenységszkennelő eszközök kimeneteit, hogy az összetett sérülékenységek és többlépcsős támadási vektorok jelenlétét képesek legyenek megállapítani.
3. A szervezet alkalmazhat támadási fákat, annak bemutatására, hogyan lépnek kölcsönhatásba egymással és kombinálódnak az támadók tevékenységei.
4. A szervezetnek különösen figyelnie kell a sérülékenységszkennelő információk korrelációjára, amikor az EIR régebbi technológiákról újabb technológiákra vált.

5. A szervezetnek dokumentálnia kell a sérülékenységszkennelő eszközök kimeneteit és naplóznia kell a korrelációs eredményeket, hogy nyomon követhesse a változásokat és időben észlelhesse a potenciális biztonsági réseket.

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

RA-5(10)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

15.18. SÉRÜLÉKENYSÉGMENEDZSMENT – SÉRÜLÉKENYSÉGI INFORMÁCIÓK FOGADÁSA

15.18. A szervezet létrehoz egy csatornát, amelyen keresztül fogadhatja a szervezeti EIR-ekben és rendszerelemekben található sérülékenységekről szóló jelentéseket.

MAGYARÁZAT

A szervezet egy olyan csatornát hoz létre, melyen képes fogadni az EIR-ek vonatkozásában relevanciával bíró sérülékenységekre vonatkozó információkat. Ez a csatorna lehet az NBSZ NKI által kiadott riasztásokat, figyelmeztetéseket fogadó csatorna, vagy az ASR kapcsolattartásra szolgáló csatorna is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy csatornát, amelyen keresztül fogadhatja a szervezeti EIR-ekben és rendszerelemekben található sérülékenységekről szóló jelentéseket.
2. A szervezetnek biztosítania kell, hogy a csatorna biztonságos és bizalmas legyen.
3. A szervezetnek dokumentálnia kell minden beérkező jelentést, és rendszeresen ellenőriznie kell a csatornát, hogy időben észlelje és kezelje a jelentett sérülékenységeket.
4. A szervezetnek meg kell határoznia egy folyamatot a beérkező jelentések kezelésére, beleértve a sérülékenységek kijavítását és a jelentéstevőkkel való kommunikációt.
5. A szervezetnek biztosítania kell, hogy a sérülékenységek kijavítása megfelelően priorizált legyen, figyelembe véve a sérülékenység súlyosságát és a potenciális kockázatot az EIR számára.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

RA-5(11)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

15.19. TECHNIKAI MEGFIGYELÉSSEL SZEMBENI INTÉZKEDÉSEK

15.19. A szervezet meghatározott gyakorisággal, vagy egyes előre meghatározott események bekövetkezésekor, vagy ráutaló jelek észlelése esetén az előre meghatározott helyszíneken ellenőrzi a technikai megfigyelőeszközök jelenlétét.

MAGYARÁZAT

Ez a folyamat, amelyet a technikai megfigyelőeszközök jelenlétét ellenőrző felmérésének nevezünk, olyan szolgáltatás, amelyet képzett személyzet nyújt a technikai megfigyelőeszközök és veszélyek jelenlétének észlelésére, valamint olyan technikai biztonsági gyengeségek azonosítására, amelyeket fel lehet használni a felmért létesítménybe történő behatolásra. A technikai megfigyelőeszközök jelenlétét ellenőrző felmérés a említettek mellett segíti a szervezet biztonsági állapotának felmérését és tartalmazhat belső, valamint külső vizuális, elektronikus, illetve fizikai vizsgálatot is, melyet a szervezet objektumaiban végeznek el. A felmérés hasznos információkat szolgáltathat a kockázatelemzéshez, emellett rávilágíthat olyan szervezeti kitettségekre, melyeket kihasználhatnak a lehetséges támadók.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a technikai megfigyelőeszközök ellenőrzésének gyakoriságát, illetve az előre meghatározott eseményeket, amelyek esetén az ellenőrzést el kell végezni. Emellett a szervezetnek azt is meg kell határoznia, hogy milyen ráutaló jelek, esetén szükséges az ellenőrzést lefolytatni.
2. A szervezetnek meg kell határoznia azokat a helyszíneket, ahol a technikai megfigyelőeszközök jelenlétét ellenőrizni kell.
3. A szervezetnek ki kell dolgoznia egy folyamatot, amely meghatározza, hogyan kell elvégezni a technikai megfigyelőeszközök ellenőrzését.
4. A szervezetnek dokumentálnia kell az ellenőrzések eredményeit.

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

RA-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az helyszínek, illetve a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

15.20. KOCKÁZATOKRA ADOTT VÁLASZ

15.20. A szervezet a kockázatmenedzsment szabályokkal összhangban reagál a biztonsági értékelések, ellenőrzések és vizsgálatok megállapításaira.

MAGYARÁZAT

Az érintett szervezetnek számos lehetősége van a kockázatokra reagálni, beleértve a kockázat csökkentését új biztonsági követelmények bevezetésével, illetve a meglévő védelmi intézkedések megerősítésével. A kockázat megfelelő indoklással elfogadható, csökkenthető, megosztható vagy átadható, illetve megszüntethető. A szervezet kockázattűrő képessége befolyásolja a kockázatra adott válaszokat és intézkedéseket. A kockázatra adott válasz sorána szervezet megfelelő választ igyekszik adni a kockázatra azt megelőzően, mielőtt intézkedési tervet hozna létre és ahhoz kapcsolódó mérföldköveket határozna meg. A válasz lehet a kockázat elfogadása vagy annak megszüntetése, illetve az is lehetséges, hogy a szervezet döntése alapján a kockázatot azonnal csökkenteni kell, így nem szükséges intézkedési tervet létrehozni és ahhoz kapcsolódó mérföldköveket meghatározni. Azonban, ha a szervezet a kockázatra a kockázat csökkentésével válaszol, és az nem végezhető el azonnal, akkor létre kell hozni egy intézkedési tervet és meg kell határozni az ahhoz kapcsolódó mérföldköveket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a kockázatkezelési szabályait.
2. A szervezetnek a kockázatkezelési szabályokkal összhangban reagálnia kell biztonsági értékelések, ellenőrzések és vizsgálatok megállapításaira.
3. A szervezetnek el kell döntenie, hogy milyen választ ad a felmerült kockázatokra. A szervezet a megfelelő indoklással elfogadhatja, csökkentheti, megoszthatja vagy átadhatja, illetve meg is szüntetheti a kockázatokat.
4. A szervezet a kockázatkezelésre adott válasz eredményeként új biztonsági követelményeket is bevezethet vagy akár a meglévő védelmi intézkedéseket is erősítheti.
5. Amennyiben a szervezet a kockázat csökkentése mellett dönt és nem képes azt azonnal kivitelezni, akkor létre kell hoznia ehhez kapcsolódóan egy intézkedési tervet és meg kell határoznia az ahhoz kapcsolódó mérföldköveket.
6. A szervezetnek dokumentálnia kell a kockázatkezelési folyamatot.

Kapcsolódó intézkedések

5.9. Az intézkedési terv és mérföldkövei

9.35. Információszivárgásra adott válaszlépések

1.4. Intézkedési terv és mérföldkövei

1.19. Kockázatkezelési keretrendszer

15.2. Biztonsági osztályba sorolás

15.4. Kockázatértékelés

19.2. Ellátási láncra vonatkozó kockázatkezelési szabályzat

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

6.1.3; 8.3; 10.2

NIST SP 800-53 rev.5 referencia

RA-7

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

15.21. RENDSZERELEMEK KRITIKUSSÁGÁNAK ELEMZÉSE

15.21. A szervezet azonosítja a szervezet működése szempontjából kritikus rendszerelemeket és funkciókat - a meghatározott EIR-ekre, rendszerelemekre vagy rendszerszolgáltatásokra vonatkozó kritikussági elemzés végrehajtásával - a rendszerfejlesztési életciklus meghatározott döntési pontjain.

MAGYARÁZAT

Nem minden rendszerelem, funkció vagy szolgáltatás igényel jelentős védelmet. A rendszerek kritikusságának elemzése az ellátási lánc kockázatkezelésének fontos alapelve, mely információt nyújt a védelmi tevékenységek fontossági sorrendjének felállításához. A rendszerelemek és funkciók kritikusságának meghatározása során figyelembe kell venni azokat a hatályos jogszabályokat, irányelveket, szabályozásokat, szabványokat és ajánlásokat, amelyek tartalmazhatnak előírásokat az EIR funkcióival, a rendszer- és a rendszerelemek interfészeivel, illetve a rendszer- és a rendszerelemek függőségeivel kapcsolatban. A rendszermérnökök funkcionális alkotóelemeire bontják az EIR-t, annak érdekében, hogy azonosítsák a szervezeti célok szempontjából kritikus funkciókat és rendszerelemeket. A funkcionális alkotóelemekre történő lebontás magában foglalja azon szervezeti célok azonosítását, melyeket az EIR támogat; azoknak a funkcióknak az alkotóelemekre történő lebontását, melyek a szervezeti célokat támogatják; nyomon követését azoknak a hardver-, szoftver, és firmware elemeknek, amelyek implementálják az említett funkciókat; illetve olyan funkciók is ide értendők, amiken több rendszerelem osztozik az EIR-en belül és azon kívül. Az EIR vagy egy rendszerelem működési környezete befolyásolhatja a kritikusságot, beleértve a kapcsolatokat és a függőségeket a kiber-fizikai rendszerekkel, eszközökkel, rendszerekkel és kiadott IT szolgáltatásokkal. Azok a rendszerelemek, amelyek közvetlen hozzáférést biztosítanak a kritikus rendszerelemekhez vagy funkciókhoz, kritikusnak tekinthetők a bennük rejlő esetleges sérülékenységek miatt. A rendszerelemek és funkciók kritikusságát úgy érdemes elemezni, hogy a szervezeti célokat támogató egyes rendszerelemek és funkciók meghibásodása milyen hatást gyakorol a szervezeti célokra.

Kritikussági elemzést akkor végeznek, amikor egy architektúrát vagy rendszertervet fejlesztenek, módosítanak vagy frissítenek. Ha ilyen elemzést a rendszerfejlesztési életciklus korai szakaszában végeznek, a szervezet képes lehet módosítani az EIR-t annak érdekében,

hogy csökkentse a rendszerelemeknek és funkcióknak a kritikus jellegét, például redundancia vagy alternatív útvonalak hozzáadásával az EIR tervéhez. A rendszerelemek kritikusságának elemzése hatással lehet a külső, szerződéses fejlesztőpartnerek által megteendő védelmi intézkedésekre is. A rendszerelemek kritikusságának elemzése elvégezhető a "Biztonsági osztályba sorolás" kontroll által előírt biztonsági követelmények részeként is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először azonosítania kell azokat a rendszerelemeket és funkciókat, amelyek kritikusak a szervezet működése szempontjából. A rendszerelemek és funkciók kritikusságának meghatározása során figyelembe kell venni azokat a hatályos jogszabályokat, irányelveket, szabályozásokat, szabványokat és ajánlásokat.
2. A szervezetnek akkor kell elvégeznie a kritikusság elemzést, amikor egy architektúrát vagy rendszertervet fejlesztenek, módosítanak vagy frissítenek. A rendszerelemek kritikusságának elemzése hatással lehet a külső, szerződéses fejlesztőpartnerek által megteendő védelmi intézkedésekre is.
3. A rendszermérnököknek funkcionális alkotóelemeire kell bontaniuk az EIR-t, annak érdekében, hogy azonosítsák a szervezeti célok szempontjából kritikus funkciókat és rendszerelemeket.
4. A szervezetnek figyelembe kell vennie az EIR vagy rendszerelem működési környezetét, beleértve a kapcsolatokat és a függőségeket a kiber-fizikai rendszerekkel, eszközökkel, rendszerekkel és kiadott IT szolgáltatásokkal.
5. A rendszerelemek és funkciók kritikusságát úgy kell elemeznie a szervezetnek, hogy a szervezeti célokat támogató egyes rendszerelemek és funkciók meghibásodása milyen hatást gyakorol a szervezeti célokra.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.2. Üzletmenet-folytonossági terv
13.2. Rendszerbiztonsági terv
13.6. Információbiztonsági architektúra leírás
13.11. Biztonsági követelmények testre szabása
1.1. Információbiztonsági szabályzat
1.12. Szervezeti működés és üzleti folyamatok meghatározása

15.2. Biztonsági osztályba sorolás

16.16. Biztonságtervezési elvek

16.76.1. Fejlesztési folyamat, szabványok és eszközök

16.97. Kritikus rendszerelemek egyedi fejlesztése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.5.22

NIST SP 800-53 REV.5 REFERENCIA

RA-9

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek, rendszerelemek és rendszerszolgáltatások illetve a rendszerfejlesztési életciklusra vonatkozó döntési pontok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

15.22. FENYEGETÉS FELDERÍTÉS

15.22.1. A szervezet létrehoz és fenntart egy fenyegetés-felderítő képességet, hogy:

15.22.1.1. keresse a kompromittálódás jeleit a szervezeti EIR-ekben; és

15.22.1.2. felderítse, nyomon kövesse és elhárítsa a meglévő védelmi mechanizmusokat megkerülő fenyegetéseket.

15.22.2. Meghatározott gyakorisággal alkalmazza a fenyegetés-felderítő képességét.

MAGYARÁZAT

A fenyegetés-felderítés egy ún. aktív módszer a kiberbiztonságban, szemben a hagyományos védelmi intézkedésekkel, mint például tűzfalak, behatolás-észlelő és megelőző rendszerek, kártékony kódok karanténba helyezése egy izolált környezetben. A fenyegetés-felderítés proaktív módon keresi a fejlett fenyegetéseket az érintett szervezet EIR-jeiben, hálózataiban és infrastruktúrájában. A cél az, hogy a támadás lehető legkorábbi szakaszában kutassa fel és zavarja meg a támadókat, és mérhetően javítsa az érintett szervezet válaszadási sebességét és pontosságát. A kompromittálódás jelei közé tartozik a szokatlan hálózati forgalom, a szokatlan fájl változások, és a kártékony kód jelenléte.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy fenyegetés-felderítő képességet, ami egy aktív védelmi eszköz a hagyományos védelmi intézkedésekkel (pl.: tűzfalak, behatolásérzékelő és megelőző rendszerek, kártékony kódok karanténba helyezése és biztonsági információ- és eseménykezelő technológiák és rendszerek) szemben.

2. Aktívan keresi a kompromittálódás jeleit az EIR-ekben, a kompromittálódás jelei közé tartozik a szokatlan hálózati forgalom, a szokatlan fájl változások és a kártékony kód jelenléte.

3. Felderíti, nyomon követi és elhárítja a meglévő védelmi mechanizmusokat megkerülő fenyegetéseket.

4. A szervezetnek meghatározott gyakorisággal alkalmaznia kell fenyegetés-felderítő képességét, azaz a fenyegetés-felderítő csapatok felhasználják a meglévő fenyegetéssel kapcsolatos információkat, és új fenyegetési információkat is létrehozhatnak, amelyeket szükség esetén megosztanak.

5. A szervezetnek naplóznia kell a fenyegetés-felderítési tevékenységeket, hogy nyomon követhesse azok hatékonyságát és javíthassa a folyamatokat.

Kapcsolódó intézkedések

5.2. Biztonsági értékelések

5.14. Folyamatos felügyelet

5.20. Behatolásvizsgálat (penetration testing)

15.4. Kockázatértékelés

15.10. Sérülékenységmonitorozás és szkennelés

15.19. Technikai megfigyeléssel szembeni intézkedések

18.13. Az EIR monitorozása

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.7

NIST SP 800-53 rev.5 referencia

RA-10

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024