Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Tervezés

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

13.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

13.1. A szervezet:

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

13.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó biztonságtervezési szabályzatot, amely

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

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

13.1.1.2. A biztonságtervezési eljárásrendet, amely a biztonságtervezési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

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

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

MAGYARÁZAT

A biztonságtervezési 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 biztonságtervezési szabályzat és eljárásrendek kidolgozásával, dokumentálásával, jóváhagyásával, kiadásával és megismertetésével kapcsolatos feladatok ellátásáról.
2. A szervezetnek meg kell bizonyosodnia arról, hogy a biztonságtervezési 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 biztonságtervezési 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 biztonságtervezési szabályzatot/szabályokat, illetve a kapcsolódó eljárásrendeket a szervezet

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

KAPCSOLÓDÓ INTÉZKEDÉSEK

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

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

3.3.2.1. Biztonságtervezési szabályzat

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

PL-1

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

13.2. RENDSZERBIZTONSÁGI TERV

13.2. A szervezet:

13.2.1. Az EIR-hez rendszerbiztonsági tervet készít, amely:

13.2.1.1. Összhangban áll a szervezeti felépítéssel.

13.2.1.2. Meghatározza az EIR-t alkotó rendszerelemeket.

13.2.1.3. Meghatározza az EIR hatókörét, alapfeladatait és biztosítandó szolgáltatásait az ügymeneti és üzleti folyamatok szempontjából.

13.2.1.4. Azonosítja azokat a személyeket, akik az EIR szerepeit és felelősségeit betöltik.

13.2.1.5. Meghatározza az EIR által feldolgozott, tárolt és továbbított információtípusokat.

13.2.1.6. Megfelelően alátámasztott módon meghatározza az EIR jogszabály szerinti biztonsági osztályát.

13.2.1.7. Felsorolja az EIR-t érintő konkrét fenyegetéseket.

13.2.1.8. Meghatározza az EIR működési környezetét és más EIR-ekkel vagy rendszerelemekkel való kapcsolatait, vagy azoktól való függőségeit.

13.2.1.9. Dokumentálja a rendszerre vonatkozó biztonsági követelményeket.

13.2.1.10. Meghatározza a biztonsági alapkövetelményeket és szükség esetén az ezen felül alkalmazott kiegészítő védelmi intézkedéseket.

13.2.1.11. Meghatározza a követelményeknek megfelelő aktuális vagy tervezett védelmi intézkedéseket, intézkedésbővítéseket és azok indoklását, végrehajtja a jogszabály szerinti biztonsági feladatokat.

13.2.1.12. Tartalmazza az EIR-t érintő olyan biztonsággal kapcsolatos tevékenységeket, amelyek meghatározott személyek és csoportok között koordinációt vagy tervezést igényelnek.

13.2.1.13. Tartalmazza a EIR-t érintő olyan biztonsággal kapcsolatos tevékenységeket, amelyek meghatározott személyek és csoportok között koordinációt vagy tervezést igényelnek.

13.2.1.14. A terveket a jóváhagyó felelős áttekinti és jóváhagyja a terv végrehajtása előtt.

13.2.2. Gondoskodik arról, hogy a rendszerbiztonsági tervet a meghatározott személyek és szerepkörök megismerjék (ideértve annak változásait is).

13.2.3. Meghatározott gyakorisággal felülvizsgálja a rendszerbiztonsági tervet.

13.2.4. Frissíti a rendszerbiztonsági tervet az EIR-ben vagy annak üzemeltetési környezetében történt változások és a terv végrehajtása vagy a védelmi intézkedések értékelése során feltárt problémák esetén.
13.2.5. Gondoskodik arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető vagy módosítható.

MAGYARÁZAT

A rendszerbiztonsági terv a meghatározott hatókörön belüli EIR-re és annak rendszerelemeire terjed ki, és tartalmazza a rendszer biztonsági követelményeinek áttekintését, valamint a követelmények teljesítéséhez kiválasztott intézkedéseket. A tervek leírják minden egyes kiválasztott intézkedés tervezett alkalmazását az EIR-rel összefüggésben, kellő részletességgel ahhoz, hogy az intézkedéseket helyesen lehessen végrehajtani, és ezt követően értékelni lehessen azok hatékonyságát. A dokumentáció leírja a rendszerspecifikus és hibrid intézkedések végrehajtásának módját, valamint az EIR működésére vonatkozó terveket és elvárásokat. A rendszerbiztonsági terv a rendszerek tervezése és fejlesztése során is felhasználható az életciklus-alapú biztonsági tervezési folyamatok támogatására. A rendszerbiztonsági terv egy élő dokumentum, amelyet a szervezet a rendszerfejlesztési életciklus során folyamatosan frissít és fejleszt.
Az érintett szervezet kidolgozhat egyetlen integrált rendszerbiztonsági tervet, vagy fenntarthat külön EIR-ekre külön terveket. A rendszerbiztonsági terv a biztonsági követelményeket egy sor intézkedéshez és intézkedés-fejlesztéshez kapcsolja. A terv leírja, hogy az intézkedések és az intézkedés-fejlesztések hogyan felelnek meg a biztonsági követelményeknek, de nem tartalmaz részletes, technikai leírást az intézkedések és az intézkedés-fejlesztések kialakításáról vagy végrehajtásáról. A rendszerbiztonsági terv elegendő információt tartalmaz (beleértve a biztonsági követelmények kiválasztásának és egyes funkciókhoz való hozzárendelésének kifejezett vagy hivatkozással történő meghatározását) ahhoz, hogy lehetővé tegye a terv szándékának egyértelműen megfelelő tervezést és végrehajtást, valamint a terv végrehajtása során a szervezeti műveletekre és eszközökre, egyénekre, más szervezetekre és a nemzetre vonatkozó kockázatok későbbi meghatározását.
A rendszerbiztonsági tervnek nem szükségszerűen egyetlen dokumentum. A terv különböző dokumentumok gyűjteménye is lehet, beleértve a már létező dokumentumokat is. A hatékony

munkát támogató rendszerbiztonsági terv(ek)et széleskörűen tartalmaz az irányelvekre, eljárásokra és további dokumentumokra való hivatkozásokat. A rendszerbiztonsági terveknek nem kell részletes üzletmenet folytonossági tervekkel vagy biztonsági eseménykezelési tervekkel kapcsolatos információkat tartalmazniuk, hanem ehelyett - kifejezetten vagy hivatkozással - elegendő információt nyújthatnak annak meghatározásához, hogy mit kell megvalósítaniuk ezeknek a terveknek.

A tervezés és a koordináció kiterjed a vészhelyzetekre és a nem vészhelyzetekre (azaz a tervezett vagy nem sürgős, nem tervezett helyzetekre). Az érintett szervezetek által a biztonsággal kapcsolatos tevékenységek tervezésére és koordinálására meghatározott folyamatot adott esetben más dokumentumok is tartalmazhatják.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia egy rendszerbiztonsági tervet.
2. A szervezetnek gondoskodnia kell arról, hogy a terveket a jóváhagyó felelős áttekinti és jóváhagyja a terv végrehajtása előtt.
3. A szervezetnek gondoskodnia kell arról, hogy a rendszerbiztonsági tervet a meghatározott személyek és szerepkörök megismerjék.
4. A szervezetnek az általa meghatározott gyakorisággal vagy a meghatározott változások és/vagy események bekövetkezése, vagy probléma felmerülése esetén felül kell vizsgálnia és szükség esetén frissítenie a rendszerbiztonsági tervet.
5. A szervezetnek gondoskodnia kell arról, hogy a rendszerbiztonsági terv jogosulatlanok számára ne legyen megismerhető vagy módosítható.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés
2.60. Legkisebb jogosultság elve
2.88. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek
2.100. Távoli hozzáférés
2.115. Külső elektronikus információs rendszerek használata
5.2. Biztonsági értékelések
5.6. Információcsere

5.14. Folyamatos felügyelet

6.45. Konfigurációkezelési terv

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

3.3.2.2. Rendszerbiztonsági terv

ISO/IEC 27001:2023 REFERENCIA

7.5.1; 7.5.2; 7.5.3; 10.2; A.5.8; A.5.34

NIST SP 800-53 REV.5 REFERENCIA

PL-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

13.3. VISELKEDÉSI SZABÁLYOK

13.3. A szervezet:

13.3.1. Megfogalmazza és a szervezetre érvényes követelmények szerint dokumentálja, valamint a szervezeten belül kihirdeti az EIR-hez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelezően elvárt vagy tiltott tevékenységet.

13.3.2. Az EIR-hez való hozzáférés engedélyezése előtt dokumentált nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt, felhasználót, aki nyilatkozatával igazolja, hogy az EIR használatához kapcsolódó, rá vonatkozó biztonsági szabályokat és kötelezettségeket megismerte, saját felelősségére betartja.

13.3.3. Meghatározott gyakorisággal felülvizsgálja és frissíti az EIR-hez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelezően elvárt vagy tiltott tevékenységet, a viselkedési szabályok betartását.

13.3.4. Gondoskodik arról, hogy a viselkedési szabályok korábbi változatát megismerő személyek elolvassák és újra dokumentált nyilatkozattételt tegyenek a viselkedési szabályok elfogadásáról, azok felülvizsgálata vagy frissítése esetén.

MAGYARÁZAT

A viselkedési szabályok egyfajta hozzáférési megállapodást jelentenek a szervezeti felhasználók számára. A hozzáférési megállapodások egyéb típusai közé tartoznak a titoktartási megállapodások, az összeférhetetlenségi megállapodások és az elfogadható használati megállapodások. A szervezetek a viselkedési szabályokat az egyes felhasználói szerepkörök és felelősségi körök alapján mérlegelik, és különbséget tesznek a privilegizált felhasználókra és az általános felhasználókra vonatkozó szabályok között. A nem szervezeti felhasználók bizonyos típusaira - beleértve az állami EIR-ekből információt kapó személyeket - vonatkozó viselkedési szabályok megállapítása gyakran nem kivitelezhető, tekintettel az ilyen felhasználók nagy számára és a rendszerekkel való interakcióik korlátozott jellegére. A szervezeti és nem szervezeti felhasználókra vonatkozó viselkedési szabályokat a "rendszerhasználat jelzése" biztonsági követelmény alapján lehet megállapítani. A kapcsolódó

követelmények szakasz a szervezeti viselkedési szabályok szempontjából releváns ellenőrzések listáját tartalmazza. A "viselkedési szabályok" című követelmény meghatározott dokumentált tudomásulvételi részhez tartozik, az érintett szervezetek által végzett biztonságtudatossági képzés, valamint szerepkör alapú képzési programok által teljesíthető, ha az ilyen képzés tartalmazza a viselkedési szabályokat. A magatartási szabályok dokumentált elismerése magában foglalja az elektronikus vagy fizikai aláírásokat és az elektronikus egyetértési jelölőnégyzeteket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell fogalmaznia és dokumentálnia kell az EIR-hez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az EIR-hez kapcsolódó kötelezően elvárt vagy tiltott tevékenységet. Ezt az információt az érintett szervezeten belül ki kell hirdetni.
2. A szervezetnek dokumentált nyilatkozattételre kell kötelezni a hozzáférési jogosultságot igénylő személyt, felhasználót, mielőtt hozzáférést engedélyezne az EIR-hez. A felhasználónak nyilatkozatával igazolnia kell, hogy megismerte és saját felelősségére betartja az EIR használatához kapcsolódó biztonsági szabályokat és kötelezettségeket.
3. A szervezetnek meghatározott gyakorisággal felül kell vizsgálnia és frissítenie kell az EIR-hez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az EIR-hez kapcsolódó kötelezően elvárt vagy tiltott tevékenységet, a viselkedési szabályok betartását.
4. A szervezetnek gondoskodnia kell arról, hogy a viselkedési szabályok korábbi változatát elismerő személyek elolvassák és újra dokumentált nyilatkozattételt tegyenek a viselkedési szabályok elfogadásáról, azok felülvizsgálata vagy frissítése esetén.
5. A szervezetnek dokumentálnia kell a fenti tevékenységeket, hogy bizonyíthassa a követelményeknek való megfelelést.

Kapcsolódó intézkedések

2.2. Fiókkezelés

2.60. Legkisebb jogosultság elve

2.75.1. A rendszerhasználat jelzése

2.76. Legutóbbi bejelentkezési értesítés

2.100. Távoli hozzáférés

2.108. Vezeték nélküli hozzáférés

2.113. Mobil eszközök hozzáférés-ellenőrzése

2.115. Külső elektronikus információs rendszerek használata

3.2. Biztonságtudatossági képzés

3.9. Szerepkör alapú biztonsági képzés

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

3.3.2.4. Személyi biztonság

ISO/IEC 27001:2023 referencia

A.5.4; A.5.10; A.6.2

NIST SP 800-53 rev.5 referencia

PL-4

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

13.4. VISELKEDÉSI SZABÁLYOK – KÖZÖSSÉGI MÉDIA ÉS KÜLSŐ WEBHELYEK, ALKALMAZÁSOK HASZNÁLATÁRA VONATKOZÓ KORLÁTOZÁSOK

13.4. A szervezet a viselkedési szabályaiba a következő korlátozásokat építi be:

13.4.1. a közösségi média, közösségi oldalak és külső oldalak, valamint alkalmazások használatának korlátozása;

13.4.2. a szervezeti információk közzétételének korlátozása nyilvános weboldalakon; és

13.4.3. a szervezet által biztosított azonosító és hitelesítő adatok használatának korlátozása külső weboldalakon, illetve alkalmazásokban való fiókok létrehozásakor.

MAGYARÁZAT

A viselkedési szabályoknak ki kell terjedniük a közösségi média, a közösségi hálózatok és a külső webhelyek/alkalmazások használatára vonatkozó korlátozásokra. Abban az esetben, ha egy szervezethez köthető személy ezeket használja hivatalos feladatának ellátására vagy hivatalos ügyek intézésére a közösségi médiával és a közösségi hálózatokkal kapcsolatos hálózati üzenetváltásban szervezeti információk vesznek részt, mert az adott személy(ek) a közösségi médiához és a webhelyekhez a szervezeti EIR-en keresztül fér hozzá. Az érintett szervezetek olyan specifikus szabályokkal is foglalkoznak, amelyek megakadályozzák, hogy illetéktelen entitások közvetlenül vagy következtetés útján nem nyilvános szervezeti információkhoz jussanak a közösségi média és egyéb oldalakról. A nem nyilvános információk közé tartoznak például a személyazonosításra alkalmas információk és a rendszerfiókok adatai.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell építenie a viselkedési szabályzatába a közösségi média, közösségi oldalak és külső oldalak, valamint alkalmazások használatának korlátozásait. Ez magában foglalja a személyzet számára adott utasításokat arra vonatkozóan, hogy mikor és hogyan használhatják ezeket az oldalakat és alkalmazásokat hivatalos feladatok ellátása vagy hivatalos üzleti tevékenység során.

2. A szervezetnek korlátoznia kell a szervezeti információk közzétételét nyilvános weboldalakon. Ez azt jelenti, hogy a szervezetnek meg kell határoznia, milyen információk tekinthetők nyilvánosnak, és milyen információk bizalmasak.
3. A szervezetnek korlátoznia kell az EIR által biztosított azonosító és hitelesítő adatok használatát külső weboldalakon, illetve alkalmazásokban való fiókok létrehozásakor. Ez azt jelenti, hogy a szervezetnek meg kell határoznia, milyen adatokat használhatnak a személyzet tagjai külső weboldalakon vagy alkalmazásokban történő fióklétrehozás során.
4. A szervezetnek dokumentálnia kell a fenti korlátozásokat, és rendszeresen ellenőriznie kell, hogy a személyzet betartja-e ezeket a szabályokat. Dokumentálnia kell minden esetet, amikor a szervezethez köthető személy(ek) megsérti ezeket a szabályokat, és megfelelő intézkedéseket kell hozni a jövőbeni szabálysértések megelőzése érdekében.

Kapcsolódó intézkedések

2.124. Nyilvánosan elérhető tartalom
4.44. Információk kiszivárgásának figyelemmel kísérése

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

3.3.2.4. Személyi biztonság

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

PL-4(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

13.5. MŰKÖDÉSI KONCEPCIÓ

13.5. A szervezet:

13.5.1. Kidolgozza az EIR működési koncepcióját, amely leírja, hogy a szervezet milyen módon kívánja működtetni az EIR-t az információbiztonság szempontjából.

13.5.2. Meghatározott gyakorisággal felülvizsgálja és frissíti a működési koncepciót.

MAGYARÁZAT

A működési koncepció szerepelhet az EIR rendszerbiztonsági tervében, illetve a rendszerfejlesztési életciklus egyéb dokumentumaiban. A működési koncepció egy élő dokumentum, amelyet a rendszerfejlesztési életciklus során folyamatosan frissíteni kell. Például a rendszertervezés felülvizsgálata során a műveleti koncepciót ellenőrzik annak biztosítása érdekében, hogy az összhangban maradjon a biztonsági követelményekkel, a rendszerarchitektúrával és az üzemeltetési eljárásokkal. A működési koncepcióban bekövetkezett változások a rendszerbiztonsági tervek, a biztonsági architektúrák és más szervezeti dokumentumok, például a beszerzési előírások, a rendszerfejlesztési életciklus dokumentumai és a rendszertervezési dokumentumok folyamatos frissítésében tükröződnek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először ki kell dolgoznia az EIR működési koncepcióját. Ez a dokumentum leírja, hogy az érintett szervezet milyen módon kívánja működtetni az EIR-t az információbiztonság szempontjából. A működési koncepció tartalmazhatja az EIR rendszerbiztonsági terveit, vagy más EIR fejlesztési életciklus dokumentumokat.
2. A működési koncepciót az EIR teljes életciklusa során frissíteni kell.
3. A működési koncepció változásait tükröznie kell a rendszerbiztonsági terveknek, az EIR architektúráknak és más szervezeti dokumentumoknak, például a beszerzési specifikációk, az EIR életciklus dokumentumok és az EIR mérnöki dokumentumok folyamatos frissítéseiben.
4. A szervezetnek meghatározott gyakorisággal felül kell vizsgálnia és frissítenie kell a működési koncepciót. Ez a felülvizsgálat magában foglalhatja a dokumentációt, hogy biztosítsa a folyamatosságot és a következetességet az EIR működésében és biztonságában.

Kapcsolódó intézkedések

13.2. Rendszerbiztonsági terv

16.2. Erőforrások rendelkezésre állása

18.67. Információ kezelése és megőrzése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

8.1; A.5.8

NIST SP 800-53 rev.5 referencia

PL-7

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

13.6. INFORMÁCIÓBIZTONSÁGI ARCHITEKTÚRA LEÍRÁS

13.6. A szervezet:

13.6.1. Elkészíti az EIR információbiztonsági architektúra leírását.

13.6.1.1. Összegzi az EIR bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló követelményeket és megközelítést.

13.6.1.2. Megfogalmazza, hogy az információbiztonsági architektúra hogyan illeszkedik a szervezet általános architektúrájába, és hogyan támogatja azt.

13.6.1.3. Leírja a külső szolgáltatásokkal kapcsolatos információbiztonsági feltételezéseket és függőségeket.

13.6.2. Az általános architektúrájában bekövetkezett változtatásokra reagálva felülvizsgálja és frissíti az információbiztonsági architektúra leírást.

13.6.3. Biztosítja, hogy az információbiztonsági architektúra leírásban tervezett változtatás tükröződjön a rendszerbiztonsági tervben, a működési koncepcióban és a beszerzésekben.

MAGYARÁZAT

A rendszerszintű biztonsági architektúra összhangban áll a "vállalati architektúrára" vonatkozó biztonsági követelményben leírt, a szervezet egészére kiterjedő biztonsági architektúrával, amely a Szerkezeti architektúra szerves részét képezi és annak részeként kerül kidolgozásra. Az architektúra tartalmazza az architektúra leírását, a biztonsági funkciók elosztását, a külső interfészek biztonsággal kapcsolatos információit, az interfészeken keresztül oda-vissza cserélt információkat, valamint az egyes interfészekhez kapcsolódó védelmi mechanizmusokat. Az architektúra egyéb információkat is tartalmazhat, mint például a felhasználói szerepek és az egyes szerepekhez rendelt hozzáférési jogosultságok; a biztonsági intézkedések; a rendszer által feldolgozott, tárolt és továbbított információk típusai; az ellátási lánc kockázatkezelési követelményei; az információk és a rendszer szolgáltatásainak helyreállítási prioritásai; és egyéb védelmi igények.

A mai modern számítástechnikai architektúrákban egyre kevésbé jellemző, hogy a szervezetek az összes információs erőforrást ellenőrzésük alatt tartják. Kulcsfontosságú függőségek lehetnek külső információs szolgáltatásoktól és szolgáltatóktól. Az ilyen függőségek leírása a biztonsági architektúrákban szükséges az átfogó ügymeneti- és üzletvédelmi stratégia

kidolgozásához. A szervezeti EIR-ek alapkonfigurációjának kialakítása, fejlesztése, dokumentálása és konfiguráció-ellenőrzés alatt tartása kritikus fontosságú a hatékony architektúrák megvalósításához és fenntartásához. Az architektúrák fejlesztését az érintett szervezet vezető információbiztonsági tisztviselőjével (IBF) koordinálják annak biztosítása érdekében, hogy a biztonsági követelmények támogatásához szükséges intézkedéseket meghatározzák és hatékonyan végrehajtsák. Sok esetben előfordulhat, hogy két rendszer biztonsági architektúrája között nincs különbség.

Jelen követelmény elsősorban a szervezeti szintű, annak biztosítására, hogy az EIR(ek)-hez olyan architektúrákat fejlesszenek ki, amely architektúrák a lehető legszorosabban integrálódjanak a vállalati architektúrába.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek el kell készítenie az EIR információbiztonsági architektúra leírását.
2. A szervezetnek össze kell foglalnia az EIR bizalmasságának, sértetlenségének és rendelkezésre állásának védelmét szolgáló követelményeket és megközelítést.
3. A szervezetnek meg kell fogalmaznia, hogy az információbiztonsági architektúra hogyan illeszkedik a szervezet általános architektúrájába, és hogyan támogatja azt.
4. A szervezetnek le kell írnia a külső szolgáltatásokkal kapcsolatos információbiztonsági körülményeket és függőségeket.
5. A szervezetnek reagálnia kell az általános architektúrájában bekövetkezett változtatásokra, és felül kell vizsgálnia és frissítenie kell az információbiztonsági architektúra leírását.
6. A szervezetnek biztosítania kell, hogy az információbiztonsági architektúra leírásban tervezett változtatás tükröződjön az EIR rendszerbiztonsági tervében, a működési koncepcióban és a beszerzésekben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.2. Alapkonfiguráció
6.23. Konfigurációs beállítások
13.2. Rendszerbiztonsági terv
13.5. Működési koncepció
13.9. Központi kezelés

1.5. Elektronikus információs rendszerek nyilvántartása

1.7. Szervezeti architektúra

15.21. Rendszerelemek kritikusságának elemzése

16.3.1. A rendszer fejlesztési életciklusa

16.15. Az elektronikus információs rendszerre vonatkozó dokumentáció

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

3.3.2.5. Információbiztonsági architektúra leírás

ISO/IEC 27001:2023 REFERENCIA

A.5.8

NIST SP 800-53 REV.5 REFERENCIA

PL-8

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

13.7. INFORMÁCIÓBIZTONSÁGI ARCHITEKTÚRA LEÍRÁS – MÉLYSÉGI VÉDELEM

13.7. A szervezet az EIR információbiztonsági architektúrájának megtervezésekor mélységi védelmi megközelítést alkalmaz, amely:
13.7.1. meghatározott védelmi intézkedéseket rendel a szervezet által meghatározott helyekhez és architekturális rétegekhez; továbbá
13.7.2. biztosítja, hogy a védelmi intézkedések összehangoltan és egymást erősítve működjenek.

MAGYARÁZAT

Az érintett szervezet stratégiai megfontolásokkal helyezi el a biztonsági követelményeket az EIR biztonsági architektúrájában, így a rendszert támadóknak több biztonsági intézkedést is sikeresen meg kell kerülniük céljuk eléréséhez. Ez a támadók szempontjából nehezebbé teszi az információforrások elleni támadást, mivel növeli a munkaerőigényt; továbbá növeli a támadás időben történő felismerésének valószínűségét. A stratégikusan elhelyezett biztonsági követelmények az EIR-ben és az érintett szervezetben fontos tevékenység, amely alapos elemzést igényel. Az érintett szervezet eszközeinek értéke fontos szempont a további rétegződés biztosításában. A mélységi védelmi architektúrai megközelítések közé tartozik a modularitás és a rétegződés, az EIR és a felhasználói funkcionalitás szétválasztása, valamint a biztonsági funkció különválasztása.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a biztonsági szabályokat és követelményeket, amelyeket stratégikusan kell elhelyeznie az EIR biztonsági architektúrájában. Ez azt jelenti, hogy a támadóknak több ellenőrzési ponton kell sikeresen átjutniuk ahhoz, hogy elérjék a céljukat.
2. A szervezetnek biztosítania kell, hogy az ellenőrzési pontok összehangoltan működjenek, hogy megnehezítsék a támadók munkáját és növeljék a detektálás valószínűségét. Az ellenőrzési pontok összehangolása elengedhetetlen ahhoz, hogy egy ellenőrzési ponton történő

támadás ne okozzon káros, nem szándékolt következményeket, mint például az EIR zárolása vagy a riasztások elindítása.

3. A szervezetnek gondosan meg kell vizsgálnia az ellenőrzési pontok elhelyezését az EIR-ben. Az érintett szervezet eszközeinek becsült értéke fontos szempont a további rétegzés kialakításának meghatározásában.

4. A szervezetnek mélységi védelmi megközelítést kell alkalmaznia, amely magában foglalja a modularitást és a rétegzést, a rendszer és a felhasználói funkcionalitás szétválasztását, valamint a biztonsági funkciók különválasztását.

5. A szervezetnek dokumentálnia kell a biztonsági intézkedéseit, hogy nyomon követhesse a biztonsági eseményeket és ellenőrizhesse a biztonsági intézkedések hatékonyságát.

Kapcsolódó intézkedések

17.2. Rendszer és felhasználói funkciók szétválasztása

17.4. Biztonsági funkciók elkülönítése

17.85. A rendszerelemek esetében alkalmazott változatos információs technológiák

17.102. Elosztott feldolgozás és tárolás

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

PL-8(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

13.8. INFORMÁCIÓBIZTONSÁGI ARCHITEKTÚRA LEÍRÁS – BESZÁLLÍTÓI DIVERZIFIKÁCIÓ

13.8. A szervezet megköveteli, hogy az általa meghatározott helyeken és architektúrális rétegekben alkalmazott biztonsági megoldások különböző beszállítóktól származzanak.

MAGYARÁZAT

Az informatikai termékeknek különböző erősségei és gyengeségei vannak. A termékek széles spektrumának biztosítása kiegészíti az egyes ajánlatokat. A rosszindulatú kódok elleni védelmet kínáló gyártók például jellemzően különböző időpontokban frissítik termékeiket, és gyakran a prioritásaik és fejlesztési ütemterveik alapján fejlesztenek ki megoldásokat az ismert vírusokra, trójaiakra vagy féregprogramokra. A különböző termékek különböző helyeken történő telepítésével megnő a valószínűsége annak, hogy legalább az egyik termék észleli a rosszindulatú kódot. Több termék használata nagyobb bizonyosságot eredményezhet a személyazonosításra alkalmas információk leltározásában.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a helyeket és architektúrális rétegeket, ahol a biztonsági megoldásokat alkalmazni kívánja.
2. A szervezetnek ki kell választania különböző beszállítókat, akik a különböző helyeken és architektúrális rétegekben alkalmazandó biztonsági megoldásokat szolgáltatják.
3. A szervezetnek meg kell vásárolnia és telepítenie kell a különböző beszállítóktól származó biztonsági megoldásokat az EIR-ben meghatározott helyeken és architektúrális rétegekben.
4. A szervezetnek rendszeresen ellenőriznie kell a különböző beszállítóktól származó biztonsági megoldások hatékonyságát és dokumentálnia kell azokat az eseteket, amikor a biztonsági megoldások nem működnek megfelelően.
5. A szervezetnek folyamatosan frissítenie kell a különböző beszállítóktól származó biztonsági megoldásokat, hogy biztosítsa az EIR védelmét a legújabb fenyegetésekkel szemben.
6. A szervezetnek rendszeresen felül kell vizsgálnia a biztonsági megoldások beszállítóinak listáját, hogy biztosítsa a lehető legjobb védelmet az EIR számára.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.85. A rendszerelemek esetében alkalmazott változatos információs technológiák

19.4. Ellátási láncra vonatkozó követelmények és folyamatok

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

PL-8(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági követelmények, illetve az helyszínek és architektúrális rétegek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

13.9. KÖZPONTI KEZELÉS

13.9. A szervezet központilag kezeli a meghatározott védelmi intézkedéseket és a hozzájuk kapcsolódó folyamatokat.

MAGYARÁZAT

A központi irányítás a biztonsági intézkedések és folyamatok szervezetszintű irányítására és végrehajtására vonatkozik. Ez magában foglalja a szervezet által meghatározott, központilag irányított biztonsági intézkedések és folyamatok tervezését, végrehajtását, értékelését, engedélyezését és felügyeletét. A központilag irányított biztonsági intézkedések és folyamatok a kezdeti és folyamatos működési engedélyek alátámasztására, valamint a szervezeti folyamatos ellenőrzés részeként végzett értékelések függetlenségi követelményeinek is megfelelhetnek.

Az automatizált eszközök (pl. a biztonsági információ- és eseménykezelő eszközök vagy a vállalati biztonsági felügyeleti és kezelési eszközök) javíthatják a központilag irányított követelményekhez és folyamatokhoz kapcsolódó információk pontosságát, következetességét és hozzáférhetőségét. Az automatizálás adatösszesítési és adatkorrelációs képességeket, riasztási mechanizmusokat és összefoglaló információkat is biztosíthat a szervezeten belüli kockázatalapú döntéshozatal támogatására.

A szervezetek az erőforrások és képességek alapján meghatározzák, hogy mely biztonsági követelmények lehetnek alkalmasak a központi irányításra. Nem mindig lehetséges egy biztonsági követelmény vagy folyamat minden aspektusát központilag kezelni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell terveznie a központilag kezelt biztonsági intézkedéseket és a hozzájuk kapcsolódó folyamatokat. Ez magában foglalja a szervezet által meghatározott, központilag kezelt intézkedések és folyamatok tervezését, végrehajtását, értékelését, engedélyezését és nyomon követését.
2. A szervezetnek automatizált eszközöket kell használnia, mint például biztonsági információ- és eseménykezelő eszközöket vagy EIR biztonsági monitorozó és kezelő eszközöket. Ezek az

eszközök javíthatják a központilag kezelt intézkedésekkel és folyamatokkal kapcsolatos információk pontosságát, következetességét és elérhetőségét.

3. A szervezetnek meg kell határoznia, mely intézkedések alkalmasak a központi kezelésre a rendelkezésre álló erőforrások és képességek alapján. Nem mindig lehetséges minden intézkedés aspektusát központilag kezelni.

4. A szervezetnek dokumentálnia kell a központilag kezelt intézkedéseket és folyamatokat azok nyomon követéséhez és értékeléséhez.

Kapcsolódó intézkedések

13.6. Információbiztonsági architektúra leírás

1.10. Kockázatkezelési stratégia

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

PL-9

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági intézkedések és a hozzájuk kapcsolódó folyamatok meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

13.10. BIZTONSÁGI KÖVETELMÉNYEK KIVÁLASZTÁSA

13.10. A szervezet kiválasztja az EIR számára az 1. melléklet 1.1.3. ponttal összhangban a biztonsági követelményeket.

MAGYARÁZAT

A biztonsági alapkövetelmények a biztonsági követelmények előre meghatározott halmazai, amelyeket kifejezetten egy csoport, szervezet vagy érdekközösség védelmi igényeinek kielégítésére állítottak össze. A biztonsági alapkövetelményeket úgy választják ki, hogy azok megfeleljenek a törvények, végrehajtási rendeletek, irányelvek, szabályzatok, irányelvek, szabványok és iránymutatások által előírtak, vagy az alapkövetelmény valamennyi felhasználójára jellemző fenyegetést érintsék az biztonsági alapkövetelményre vonatkozó feltételezések alapján.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az érintett szervezet először határozza meg a szükséges biztonsági követelményeket az EIR számára. Ezek a követelmények lehetnek jogszabályok, végrehajtási rendeletek, irányelvek, szabályzatok, szabályok, szabványok és útmutatók által előírtak, vagy olyan fenyegetéseket kezelhetnek, amelyek minden felhasználóra közösek.
2. Az érintett szervezet választ egy előre meghatározott biztonsági ellenőrzési alapot, amely megfelel az EIR védelmi igényeinek. Ez az alap a kiindulópontja az információ és az EIR védelmének.
3. Az érintett szervezetnek figyelembe kell vennie az alapfeladatok és üzleti követelményeket, valamint az alkalmazandó jogszabályok, végrehajtási rendeletek, irányelvek, szabályzatok, szabályok, szabványok és útmutatók által előírt kötelezettségeket a biztonsági ellenőrzési alap kiválasztásakor.
4. Az érintett szervezetnek át kell tekintenie az EIR-en tárolt, feldolgozott és továbbított információ típusait és az információt magát, elemzi a potenciális káros hatásokat, amelyek az információ vagy az EIR elvesztése vagy kompromittálása esetén jelentkezhetnek.
5. Az érintett szervezetnek figyelembe kell vennie az EIR és szervezeti kockázatértékelések eredményeit is.

6. Az érintett szervezetnek naplót kell vezetnie a fent említett lépésekről és azok eredményeiről, hogy biztosítsa a folyamat átláthatóságát és ellenőrizhetőségét.

Kapcsolódó intézkedések

13.2. Rendszerbiztonsági terv
13.11. Biztonsági követelmények testre szabása
15.2. Biztonsági osztályba sorolás
15.4. Kockázatértékelés
16.16. Biztonságtervezési elvek

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

PL-10

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

13.11. BIZTONSÁGI KÖVETELMÉNYEK TESTRE SZABÁSA

13.11. A szervezet testre szabja a kiválasztott biztonsági követelményeket.

MAGYARÁZAT

A testreszabás lehetővé teszi a szervezetek számára, hogy a testreszabási folyamatok segítségével magukra szabják a vonatkozó követelményeket vagy egy részüket. A testreszabás megkönnyíti az ilyen specializálást, mivel lehetővé teszi a szervezetek számára, hogy olyan biztonsági követelményeket, intézkedéseket és folyamatokat dolgozzanak ki, amelyek tükrözik sajátos céljukat és üzleti (ügymeneti) funkcióikat, a környezetet, amelyben a rendszereik működnek, a rendszereiket érintő fenyegetéseket és sérülékenységeket, valamint bármely más olyan körülményt vagy helyzetet, amely hatással lehet a céljukra vagy működésükre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia kell a szervezeti biztonsági követelményeket. A szervezetnek figyelembe kell vennie a hatókörbe tartozó szempontokat. Ez azt jelenti, hogy az érintett szervezetnek figyelembe kell vennie az EIR környezetét, ahol működik, és annak specifikus igényeit.
2. A szervezetnek - amennyiben ez szükséges - ki kell választania a kiegészítő védelmi intézkedéseit. Ezek olyan biztonsági intézkedések, amelyeket akkor alkalmaznak, ha egy meglévő biztonsági védelmi intézkedés nem alkalmazható vagy nem hatékony.
3. A szervezetnek további biztonsági követelményeket kell kidolgoznia és bevezetnie, amennyiben ezt szükségesnek ítéli.
6. A szervzeetnek dokumentálnia kell a bevezetett és működő biztonsági követelményeket, hogy később értékelhesse azok hatékonyságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

13.10. Biztonsági követelmények kiválasztása
15.2. Biztonsági osztályba sorolás
15.4. Kockázatértékelés
15.21. Rendszerelemek kritikusságának elemzése

16.16. Biztonságtervezési elvek

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

PL-11

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024