Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Értékelés, engedélyezés és monitorozás

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

5.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

5.1. A szervezet:

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

5.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó biztonságértékelési szabályzatot, amely

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

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

5.1.1.2. A biztonságértékelési eljárásrendet, amely a biztonságértékelési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

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

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

MAGYARÁZAT

A biztonságértékelési 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 újra közlése nem minősülhet szervezeti szabályzatnak vagy eljárásrendnek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

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

3.3.4.1. Biztonságelemzési eljárásrend

ISO/IEC 27001:2023 referencia

5.2; 5.3; 7.5.1; 7.5.2; 7.5.3; 9.2.2; 9.3.1; 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

CA-1

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

5.2. BIZTONSÁGI ÉRTÉKELÉSEK

5.2. A szervezet:

5.2.1. Kiválasztja az elvégzendő értékelés típusának megfelelő értékelő személyt vagy csoportot.

5.2.2. Biztonságértékelési tervet készít, amely leírja az értékelés hatókörét, beleértve:

5.2.2.1. az értékelendő védelmi intézkedéseket, azok kiterjesztését és továbbfejlesztését;

5.2.2.2. a védelmi intézkedések hatékonyságának megállapításához használt értékelési eljárásokat;

5.2.2.3. az értékelési környezetet, az értékelő csoportot, az értékelő szerepköröket és feladataikat.

5.2.3. Biztosítja, hogy a biztonságértékelési tervet az engedélyezésre jogosult felelős vagy kijelölt képviselője az értékelés elvégzése előtt felülvizsgálja és jóváhagyja.

5.2.4. Meghatározott gyakorisággal értékeli az EIR és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését.

5.2.5. Elkészíti a biztonságértékelés eredményét összefoglaló jelentést.

5.2.6. Gondoskodik a biztonságértékelés eredményét összefoglaló jelentésnek a szervezet által meghatározott szerepköröket betöltő személyek által, vagy a szerepkörhöz tartozó jogosultságnak megfelelően történő megismeréséről.

MAGYARÁZAT

A szervezet biztosítja, hogy a védelmi intézkedések értékelői rendelkezzenek a szükséges készségekkel és technikai szakértelemmel a hatékony értékelési tervek kidolgozásához és a rendszerspecifikus, hibrid, közös (több szervezetet érintő, ágazati stb.) és az információbiztonsági irányítási rendszert érintő védelmi intézkedések értékelésének elvégzéséhez. A szükséges készségek közé tartozik a kockázatkezelési koncepciók és megközelítések általános ismerete, valamint a hardver, szoftver és firmware rendszerelemek átfogó ismerete és tapasztalata.

A szervezet értékeli az EIR-ek és a működési környezetük vonatkozásában alkalmazott védelmi intézkedéseket a kezdeti és folyamatos engedélyezés, a folyamatos felügyelet, az éves értékelések, a rendszertervezés és -fejlesztés, a rendszerbiztonsági tervezés, valamint a

rendszerfejlesztési életciklus részeként. Az értékelések segítenek biztosítani, hogy a szervezetek megfeleljenek az információbiztonsági követelményeknek, azonosítsák a rendszertervezési és -fejlesztési folyamat gyengeségeit és hiányosságait, az engedélyezési folyamatok részeként kockázatalapú döntések meghozatalához szükséges alapvető információkat szolgáltassanak, és megfeleljenek a sérülékenységeket csökkentő eljárásoknak. A szervezet a biztonsági tervekben dokumentált módon végzi el a megvalósított védelmi intézkedések értékelését. Az értékelések a rendszerfejlesztési életciklus során is elvégezhetők a rendszertervezési és rendszerbiztonsági tervezési folyamatok részeként. A védelmi intézkedések tervezése értékelhető az ajánlattételi felhívások kidolgozása, a válaszok értékelése és a tervezési felülvizsgálatok elvégzése során. Ha a fejlesztés során értékelik az ellenőrzések végrehajtására vonatkozó tervet és a tervnek megfelelő későbbi végrehajtást, a végső ellenőrzési tesztelés lehet egy egyszerű megerősítés a korábban elvégzett ellenőrzési értékelés felhasználásával és az eredmények összesítésével.

A szervezet kidolgozhat egyetlen, összevont biztonsági értékelési tervet az EIR-re vonatkozóan, illetve fenntarthat külön terveket is. Az összevont értékelési terv egyértelműen meghatározza az ellenőrzési értékeléssel kapcsolatos szerepeket és felelősségi köröket. Ha egy EIR értékelésében több szervezet is részt vesz, az összehangolt megközelítés csökkentheti a redundanciákat és a kapcsolódó költségeket.

A szervezet más típusú értékelési tevékenységeket, például sérülékenységszkennelést és rendszerfelügyeletet is alkalmazhat a rendszerek biztonsági helyzetének fenntartására a rendszer életciklusa során. Az értékelési jelentések a szervezet által szükségesnek ítélt megfelelő részletességgel dokumentálják az értékelési eredményeket, annak érdekében, hogy meghatározható legyen a jelentések pontossága és teljessége, valamint azt, hogy az ellenőrzések helyesen vannak-e végrehajtva, a tervezett módon működnek-e, és a kívánt eredményt hozzák-e a követelmények teljesítése tekintetében. Az értékelési eredményeket az elvégzett értékelések típusának megfelelő személyek vagy szerepkörök kapják meg. Például az engedélyezési döntések alátámasztására végzett értékeléseket az engedélyező tisztviselők, a vezető információbiztonsági tisztviselők és az engedélyező tisztviselők kijelölt képviselői kapják meg. Az éves értékelési követelmények teljesítéséhez a szervezet a következő forrásokból származó értékelési eredményeket használhatja: kezdeti vagy folyamatos rendszerengedélyezés, folyamatos felügyelet, rendszertervezési folyamatok vagy rendszerfejlesztési életciklussal

kapcsolatos tevékenységek. A szervezet biztosítja, hogy az értékelési eredmények naprakészek, az ellenőrzés hatékonyságának meghatározása szempontjából relevánsak, és az azokat készítő értékelő kellően független volt. A meglévő védelmi intézkedések értékelési eredményei újra felhasználhatók, amennyiben az eredmények még mindig érvényesek, és szükség szerint további értékelésekkel is kiegészíthetők. A kezdeti jóváhagyások után a szervezet a folyamatos ellenőrzés során értékeli a védelmi intézkedéseket. A szervezet a folyamatos értékelések gyakoriságát is a szervezetben meglévő, folyamatos felügyeleti stratégiákkal összhangban határozza meg. A külső ellenőrzések (pl.: felügyeleti szervek által lefolytatott biztonsági értékelés) nem tartoznak a biztonsági értékelések alá.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy a védelmi intézkedések értékelői rendelkezzenek a szükséges készségekkel és technikai szaktudással a hatékony értékelési tervek kialakításához és a rendszerspecifikus, hibrid, közös és programkezelési kontrollok értékeléséhez, amennyiben ez szükséges. A szükséges készségek közé tartozik az általános ismeret a kockázatkezelési koncepciókról és megközelítésekről, valamint átfogó ismeretek és tapasztalat az EIR hardver, szoftver és firmware komponenseivel kapcsolatban.
2. A szervezetnek értékelnie kell az EIR, illetve az EIR működési környezetét érintő védelmi intézkedéseket, beleértve az elsődleges és folyamatos engedélyezés, a folyamatos felügyelet, az éves értékelések, a rendszertervezés és fejlesztés, a rendszerbiztonsági tervezés és az rendszerfejlesztési életciklus részét. Az értékelések segítenek biztosítani, hogy a szervezet megfeleljen az információbiztonsági követelményeknek, azonosítsa a rendszertervezési és fejlesztési folyamatának gyengeségeit és hiányosságait, szükséges információkat szolgáltasson a kockázatalapú döntések meghozatalához az engedélyezési folyamatok során, és megfeleljen a sérülékenységek enyhítésére vonatkozó eljárásoknak.
3. A szervezetnek el kell döntenie, hogy egyetlen, összevont biztonsági értékelési tervet készít az EIR számára, vagy külön terveket tart fenn. Egy összevont értékelési terv világosan meghatározza a védelmi intézkedésekkel kapcsolatos értékelő szerepköröket.
4. A szervezetnek meg kell fontolnia más típusú értékelési tevékenységek használatát is, mint például a sérülékenységszkennelés és a rendszerfelügyelet, annak érdekében, hogy fenntartsa az EIR biztonsági állapotát az EIR életciklusa során.

5. A szervezetnek gondoskodnia kell arról, hogy az értékelési jelentések a szervezet által szükségesnek ítélt megfelelő részletességgel dokumentálja az értékelési eredményeket, annak érdekében, hogy meghatározható legyen a jelentések pontossága és teljessége, valamint az, hogy az ellenőrzések helyesen vannak-e végrehajtva, a tervezett módon működnek-e, és a kívánt eredményt hozzák-e a követelmények teljesítése tekintetében.
6. A szervezetnek gondoskodnia kell arról, hogy értékelési eredményeket az adott értékelések típusának megfelelő illetékes személyek vagy szerepkörök megkapják. Például az engedélyezési döntések támogatására végzett értékeléseket az engedélyező tisztségviselő.
7. A szervezetnek gondoskodnia kell az értékelések során feltárt kockázatok kezeléséről. Erre vonatkozóan intézkedési tervet kell készíteni, és gondoskodni kell annak folyamatos monitorozásáról, ill. az abban szereplő feladatok végrehajtásáról.

Kapcsolódó intézkedések

2.115. Külső elektronikus információs rendszerek használata
5.9. Az intézkedési terv és mérföldkövei
5.11. Engedélyezés
5.14. Folyamatos felügyelet
1.10. Kockázatkezelési stratégia
15.10. Sérülékenységmonitorozás és szkennelés
15.22.1. Fenyegetés felderítés
16.66. Fejlesztői biztonsági tesztelés
17.107. Működésbiztonság
18.8. Kártékony kódok elleni védelem

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

3.3.4.2. Biztonsági értékelések

ISO/IEC 27001:2023 referencia

9.2; 9.2.1; 9.2.2; A.5.30; A.5.36; A.8.29

NIST SP 800-53 rev.5 referencia

CA-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

5.3. BIZTONSÁGI ÉRTÉKELÉSEK – FÜGGETLEN ÉRTÉKELŐK

5.3. A 1. § (1) bekezdés hatálya alá tartozó szervezet - a honvédelmi célú rendszerek kivételével - független értékelőket vagy értékelőcsoportokat alkalmaz az EIR védelmi intézkedéseinek értékelésére.

MAGYARÁZAT

A védelmi intézkedés az Ibtv. hatálya alá tartozó szervezetek esetében alkalmazandó.

Ilyen független biztonsági értékelésnek tekintendő a kiberbiztonsági felügyeletet ellátó hatóság ellenőrzése és minden olyan hatósági eljárása is, mely az érintett EIR védelmi intézkedéseinek vizsgálatához kapcsolódik (pl.: biztonsági osztályba sorolás megfelelőségének értékelésére és nyilvántartásba vételére irányuló eljárások).

A hatóság eljárásain túlmenően az alábbiak az irányadók: A független értékelők vagy értékelőcsoportok olyan személyek vagy csoportok, akik az EIR-ek pártatlan értékelését végzik. A pártatlanság azt jelenti, hogy az értékelők mentesek minden vélt vagy valós összeférhetetlenségtől, vagyis nincs érdekeltségük az értékelt EIR-ek fejlesztésével, üzemeltetésével, fenntartásával vagy irányításával kapcsolatban, így képesek az EIR védelmi intézkedéseinek hatékonyságát pártatlanul értékelni. A pártatlanság elérése érdekében az értékelők nem teremtenek kölcsönös vagy ellentétes érdekeltséget azokkal a szervezetekkel, ahol az értékeléseket végzik, nem értékelik saját munkájukat, nem lépnek fel az általuk kiszolgált szervezetek vezetőségeként vagy alkalmazottjaként, és nem kerülnek a szolgáltatásaikat igénybe vevő szervezetek érdekérvényesítő pozíciójába.

Független értékeléseket a szervezeten belüli szereplők is végezhetnek, vagy a szervezeten kívüli köz- vagy magánszektorbeli szervezetekkel köthetnek szerződést. Az engedélyezésre jogosult tisztviselők a rendszerek biztonsági kategóriái és/vagy a szervezeti működésre, a szervezeti eszközökre vagy az egyénekre jelentett kockázat alapján határozzák meg a függetlenség szükséges szintjét. Az engedélyezésre jogosult tisztviselők azt is meghatározzák, hogy az értékelő függetlenségének szintje elegendő biztosítékot nyújt-e arra, hogy az eredmények megalapozottak és felhasználhatók-e hiteles, kockázatalapú döntések meghozatalához. Az értékelők függetlenségének meghatározása magában foglalja azt is, hogy a szerződésben szereplő értékelési szolgáltatások kellően függetlenek-e pl.: az EIR tulajdonosai nem vesznek részt közvetlenül a szerződéskötési folyamatokban, illetve nem tudják

befolyásolni az értékelést végző szakértők pártatlanságát. A rendszer tervezési és fejlesztési szakaszában a független értékelőkkel történő együttműködés hasonló a tervezési felülvizsgálatokban részt vevő független KKV-kkal való együttműködéshez.

Ha az EIR-eket tulajdonló szervezet kicsi, vagy a szervezet struktúrája megköveteli, hogy az értékeléseket olyan személyek végezzék, akik a rendszer tulajdonosainak fejlesztési, üzemeltetési vagy irányítási láncolatában vannak, az értékelési folyamatok függetlenségét úgy lehet elérni, hogy az értékelési eredményeket független szakértői csoportok gondosan felülvizsgálják és elemzik az eredmények teljességének, pontosságának, sértetlenségének és megbízhatóságának validálása érdekében. Az engedélyezési döntések támogatásától eltérő céllal végzett értékelések nagyobb valószínűséggel használhatók fel ilyen döntésekhez, ha azokat kellő függetlenséggel rendelkező értékelők végzik, ezáltal csökkentve az értékelések megismétlésének szükségességét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet alkalmazzon független értékelőket vagy értékelőcsoportokat az EIR védelmi intézkedéseinek értékelésére. Az értékelőknek pártatlanoknak kell lenniük, vagyis nem lehetnek érdekeltek az értékelés alatt álló EIR fejlesztésében, működtetésében, fenntartásában vagy kezelésében.
2. Független értékeléseket a szervezeten belüli szereplők is végezhetnek, illetve a szervezet a szervezeten kívüli köz- vagy magánszektorbeli szervezetekkel is köthet szerződést értékelés elvégzésére. Az engedélyezésre jogosult tisztviselők a rendszerek biztonsági kategóriái és/vagy a szervezeti működésre, a szervezeti eszközökre vagy az egyénekre jelentett kockázat alapján határozzák meg a függetlenség szükséges szintjét.
3. Az engedélyező hivatalos személyeknek meg kell határozniuk, hogy az értékelő függetlenségének szintje elegendő biztosítékot nyújt-e arra, hogy az eredmények megalapozottak lesznek és azok felhasználhatók-e hiteles, kockázatalapú döntések meghozatalához.
4. Ha az EIR-eket tulajdonló szervezet kicsi, vagy a szervezet struktúrája megköveteli, hogy az értékeléseket olyan személyek végezzék, akik a rendszer tulajdonosainak fejlesztési, üzemeltetési vagy irányítási láncolatában vannak, az értékelési folyamatok függetlenségét úgy biztosíthatja a szervezet, hogy az értékelési eredményeket független szakértői csoportok

gondosan felülvizsgálják és elemzik az eredmények teljességének, pontosságának, sértetlenségének és megbízhatóságának validálása érdekében.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

9.2.2; A.5.35

NIST SP 800-53 rev.5 referencia

CA-2(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

5.4. BIZTONSÁGI ÉRTÉKELÉSEK – KIBERBIZTONSÁGI AUDIT

5.4. A 1. § (2) bekezdés hatálya alá tartozó szervezet független auditorokat alkalmaz az EIR védelmi intézkedéseinek értékelésére.

MAGYARÁZAT

A védelmi intézkedés a Kibertantv. hatálya alá tartozó szervezetek esetében kötelező. A Kibertantv. 23. § (1) bekezdés szerinti intézkedés értendő alatta: „Az érintett szervezet az e törvény szerinti kiberbiztonsági követelményeknek való megfelelés bizonyítására köteles kétévente a tevékenység végzésére jogosult, független auditor (a továbbiakban: auditor) által kiberbiztonsági auditot végeztetni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A végrehajtásra irányadó rendelkezésekről az alábbi linken lehet tájékozódni: https://sztfh.hu/tevekenysegek/kiberbiztonsagi-tanusitas/kiberbiztonsagi-felugyelet/

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

9.2.2; A.5.35

NIST SP 800-53 REV.5 REFERENCIA

CA-2(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

5.5. BIZTONSÁGI ÉRTÉKELÉSEK – SPECIÁLIS ÉRTÉKELÉSEK

5.5. A szervezet a védelmi intézkedések értékelése céljából rendszeresen bejelentett, vagy bejelentés nélküli:

5.5.1. mélységi monitorozást végezhet;

5.5.2. biztonsági berendezéseket alkalmazhat;

5.5.3. automatizált biztonsági teszteseteket hajthat végre;

5.5.4. sérülékenységszkennelést végezhet;

5.5.5. rosszhiszemű felhasználó teszteket hajthat végre;

5.5.6. belső fenyegetettség értékelést végezhet;

5.5.7. teljesítmény- és terhelési teszteket hajthat végre;

5.5.8. adatvesztés vagy adatszivárgás értékelést végezhet;

5.5.9. a szervezet által meghatározott egyéb biztonsági értékeléseket végezhet.

MAGYARÁZAT

A szervezetek speciális értékeléseket végezhetnek, beleértve az ellenőrzést és hitelesítést, az EIR monitorozását, a belső fenyegetések értékelését, a rosszhiszemű felhasználó teszteket és a tesztelés egyéb formáit. A szervezet kiemelten figyel arra, hogy olyan javító intézkedéseket tegyen, melyek növelik a biztonsági szintet. Ennek részeként a speciális értékelések javíthatják a szervezet felkészültséget azáltal, hogy a szervezet a gyakorlatban is alkalmazza a rendelkezésére álló képességeket, mely során a szervezet mérheti az aktuális teljesítményszintjét. A szervezet a vonatkozó hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal összhangban végeznek speciális értékeléseket. Az engedélyezésre jogosult tisztviselők a szervezeti kockázatokkal összhangban hagyják jóvá az értékelési módszereket. A szervezet az értékelések során feltárt sérülékenységeket a kezelni kívánt sérülékenységek közé. Speciális értékeléseket a rendszerfejlesztési életciklus korai szakaszában is el lehet végezni (pl. a kezdeti tervezés, fejlesztés és egységtesztelés (unit testing) során).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy milyen speciális értékelések elvégzését tartja szükségesnek.

2. A szervezetnek döntést kell hoznia arra vonatkozóan, hogy a kiválasztott értékelést saját erőforrásból vagy külső partner bevonásával óhajtja végrehajtani.
3. Az érintett szervezetnek le kell folytatnia vagy el kell végeztetnie a kiválasztott értékelést vagy értékeléseket.
4. Az értékelő személynek vagy szervezetnek dokumentálnia kell az értékelés folyamatát, ill. eredményeit.
5. A szervezetnek fel kell dolgoznia a speciális értékelés eredményeit és az alapján kell további döntéseket hoznia pl.: szabályozások módosítása, képzési anyagok frissítése, hardver vagy szoftver beszerzése, feltárt sérülékenységek javítása stb.
6. A szervezetnek intézkedési tervet kell készíteni a szükséges javító, vagy kockázatcsökkentő intézkedések nyomon követésére.

Kapcsolódó intézkedések

12.6. A fizikai belépés ellenőrzése
18.2. Hibajavítás

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

3.3.4.3. Speciális értékelés: Az érintett szervezet a védelmi intézkedések értékelése keretében bejelentés mellett vagy bejelentés nélkül sérülékenységvizsgálatot, rosszhiszemű felhasználó tesztet, belső fenyegetettség értékelést, a biztonságkritikus egyedi fejlesztésű szoftverelemek forráskód elemzését, az érintett szervezet által meghatározott egyéb biztonsági értékeléseket végeztet.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CA-2(2)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság, illetve az egyéb értékelési formák meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

5.6. Biztonsági értékelések – Külső szervezetek eredményeinek felhasználása

5.6. A vizsgált szervezet alkalmazza a meghatározott külső szervezetek által végzett értékelések eredményeit saját EIR-eiben, feltéve, hogy azok megfelelnek a szervezet által támasztott elvárásoknak.

Magyarázat

A szervezet támaszkodhat a védelmi intézkedések más szervezetek által végzett értékelésére. Az ilyen értékelések használata és a meglévő értékelési bizonyítékok újra felhasználása csökkentheti az értékelésekhez szükséges időt és erőforrásokat azáltal, hogy korlátozza a szervezetek által elvégzendő független értékelési tevékenységeket. Azok a tényezők, amelyeket a szervezet mérlegel annak eldöntésekor, hogy elfogadja-e a külső szervezetektől származó értékelési eredményeket, eltérőek lehetnek. Ilyen tényezők többek között a szervezetnek az értékelést végző szervezettel kapcsolatos korábbi tapasztalatai, az értékelő szervezet hírneve, a benyújtott értékelési bizonyíték részletessége, valamint a szervezetre vonatkozó hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások. Az akkreditált tesztlaboratóriumok független értékelési eredményeket képesek nyújtani, amelyeket a szervezet hasznosíthat.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, hogy mely külső szervezetek által végzett értékeléseket kívánja felhasználni saját EIR-jének értékeléséhez.
2. A szervezetnek figyelembe kell vennie több tényezőt a külső szervezetek által végzett értékelések elfogadásának megfontolásakor. Ilyen tényezők lehetnek a korábbi tapasztalatok a véleményezést végző szervezettel, az értékelő szervezet hírneve, a támogató értékelési bizonyítékok részletességi szintje, valamint az alkalmazandó hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások.
3. A szervezetnek meg kell vizsgálnia, hogy az értékelési eredmények milyen mértékben felelnek meg saját elvárásainak. Ha az eredmények megfelelnek ezeknek az elvárásoknak, akkor azokat fel lehet használni az EIR értékeléséhez.

KAPCSOLÓDÓ INTÉZKEDÉSEK

16.7. Beszerzések

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

CA-2(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a külső szervezet, illetve a rendszer meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

5.7. INFORMÁCIÓCSERE

5.7. A szervezet:

5.7.1. Jóváhagyja és szabályozza az információcserét az EIR és más rendszerek között, összhangban a kapcsolódásokra és az információcserére vonatkozó biztonsági megállapodásokkal, továbbá figyelembe veszi a szolgáltatási szintre, a felhasználókra és a titoktartásra vonatkozó, valamint a szervezet által meghatározott egyéb megállapodásokat.

5.7.2. Minden egyes információcsere-megállapodás keretében dokumentálja az egyes rendszerek interfészeinek jellemzőit, biztonsági követelményeit, védelmi intézkedéseit és felelősségi körét, valamint rögzíti a megosztott információk hatásának szintjét is.

5.7.3. Rendszeres időközönként felülvizsgálja és frissíti a megállapodásokat.

MAGYARÁZAT

Az EIR és más rendszerek közti rendszerinformáció-csere követelményei a két vagy több rendszer közötti információcserére vonatkoznak. A rendszerinformáció-csere magában foglalja a bérelt vonalakon vagy virtuális magánhálózatokon keresztül történő kapcsolatokat, az internetszolgáltatókkal való kapcsolatokat, az adatbázisok megosztását vagy az adatbázis-tranzakciós információk cseréjét, a felhőszolgáltatásokkal való kapcsolatokat és cseréket, a webalapú szolgáltatásokon keresztül történő cseréket vagy a fájlok cseréjét fájlátviteli protokollokon, hálózati protokollokon, e-mailen vagy más szervezetek közötti kommunikáción keresztül. A szervezetek figyelembe veszik az új vagy megnövekedett fenyegetésekkel kapcsolatos kockázatokat, amelyek akkor merülhetnek fel, amikor az EIR-ek más rendszerekkel cserélnek információt, amelyek eltérő biztonsági követelményekkel és védelmi intézkedésekkel rendelkeznek. Ez magában foglalja a szervezeten belüli és a szervezeten kívüli rendszereket is.

Az engedélyezésre jogosult felelősök meghatározzák az EIR információcseréjéhez kapcsolódó kockázatot és a megfelelő követelményeket a kockázatcsökkentéshez.

A kiválasztott megállapodás-típusok olyan tényezőkön alapulnak, mint például a cserében érintett információ hatásszintje, az információt kicserélő szervezetek közötti kapcsolat (pl. kormányzat a kormányzat között, kormányzat a vállalkozások között, vállalkozás a vállalkozás között, kormányzat vagy vállalkozás a szolgáltató között, kormányzat vagy vállalkozás a magánszemély között), vagy a másik rendszer felhasználóinak a szervezeti EIR-hez való

hozzáférési szintje. Ha az információt cserélő rendszereknek ugyanaz az engedélyezésre jogosult felelőse, a szervezetnek nem kell megállapodásokat kidolgoznia. Ehelyett a rendszerek közötti interfész jellemzőit (pl. hogyan történik az információcsere?, hogyan védik az információt?) a vonatkozó biztonsági tervekben írják le. A szervezet a megállapodással kapcsolatos információkat beépítheti a hivatalos szerződésekbe, különösen az állami és a nem állami szervezetek (beleértve a szolgáltatókat, vállalkozókat, rendszerfejlesztőket és rendszerintegrátorokat) között létrejött információcserék esetében. A kockázati megfontolások magukban foglalják az azonos hálózatokon osztozó rendszereket is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek jóvá kell hagynia és szabályoznia kell az információcserét az EIR és más rendszerek között, összhangban a kapcsolódásokra és az információcserére vonatkozó biztonsági megállapodásokkal. Ezt figyelembe véve, a szervezetnek figyelembe kell vennie a szolgáltatási szintre, a felhasználókra és a titoktartásra vonatkozó, valamint a szervezet által meghatározott egyéb megállapodásokat.
2. A szervezetnek minden egyes információcsere-megállapodás keretében dokumentálnia kell az EIR interfészeinek jellemzőit, biztonsági követelményeit, védelmi intézkedéseit és felelősségi körét. Ezen felül rögzítenie kell a megosztott információk hatásának szintjét is.
3. A szervezetnek rendszeres időközönként felül kell vizsgálnia és frissítenie kell a megállapodásokat.
4. A szervezetnek figyelembe kell vennie a kockázatot, amelyet az új vagy növekvő fenyegetések jelenthetnek, amikor az EIR információt cserél más rendszerekkel, amelyek eltérő biztonsági követelményekkel és védelmi intézkedésekkel rendelkezhetnek.
5. Ha az információt cserélő EIR-eknek ugyanaz az engedélyező tisztviselője, akkor az érintett szervezetnek nem kell megállapodásokat készítenie. Ehelyett a rendszerek közötti interfész jellemzőit a megfelelő biztonsági tervekben kell leírni.
6. A szervezetnek be kell építenie a megállapodás információit a hivatalos szerződésekbe, különösen az állami és nem állami szervezetek (beleértve a szolgáltatókat, rendszerfejlesztőket és rendszerintegrátorokat) között létrejött információcserék esetében.
7. A szervezetnek a kockázatok mérlegelése során figyelembe kell vennie azokat az EIR-eket is, amelyek ugyanabban a hálózatban találhatóak.

Kapcsolódó intézkedések

2.28. Információáramlási szabályok érvényesítése

2.115. Külső elektronikus információs rendszerek használata

4.51. Szervezeten átívelő naplózás

5.11. Engedélyezés

8.10. Eszközök azonosítása és hitelesítése

9.9.1. Biztonsági események kezelése

13.2. Rendszerbiztonsági terv

15.4. Kockázatértékelés

16.49. Külső elektronikus információs rendszerek szolgáltatásai

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.14; A.8.21

NIST SP 800-53 rev.5 referencia

CA-3

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

5.8. INFORMÁCIÓCSERE – ÁTVITELI ENGEDÉLYEK

5.8. A szervezet az adattovábbítás elfogadása előtt gondoskodik róla és ellenőrzi, hogy a kapcsolódó rendszerek között adatokat továbbító személyek vagy rendszerek rendelkeznek-e az adatátvitelhez szükséges jogosultságokkal.

MAGYARÁZAT

Annak megelőzése érdekében, hogy jogosulatlan személyek és rendszerek információtovábbítást végezzenek a védett rendszerekben, a védett rendszer független eszközökkel ellenőrzi, hogy az információtovábbítást megkísérlő személy vagy rendszer jogosult-e erre. Az információátvitelre való jogosultság ellenőrzése a vezérlő szintű forgalomra (pl.: útválasztás (routing) és DNS) és a szolgáltatásokra (pl.: hitelesített SMTP-továbbítók) is vonatkozik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia kell azokat a személyeket és rendszereket, amelyeknek jogosultságuk van adatokat továbbítani a kapcsolódó rendszerek között.
2. A szervezetnek létre kell hoznia egy független ellenőrzési rendszert, amely képes megerősíteni, hogy az adatátvitelt végző személy vagy rendszer rendelkezik-e a szükséges jogosultságokkal.
3. A szervezetnek biztosítania kell, hogy az ellenőrzési rendszer folyamatosan működjön és rendelkezésre álljanak naplók az összes adatátviteli kísérletről, beleértve a sikeres és sikertelen próbálkozásokat is.
4. A szervezetnek rendszeresen felül kell vizsgálnia a naplókat, hogy azonosítsa az esetleges jogosulatlan adatátviteli kísérleteket és azonnal cselekedjen, ha ilyeneket talál.
5. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell az adatátviteli jogosultságokat, hogy biztosítsa, hogy csak a megfelelő személyek és rendszerek rendelkezzenek ilyen jogosultságokkal.
6. A szervezetnek biztosítania kell, hogy az adatátviteli jogosultságokkal rendelkező személyek és rendszerek beállítását végző személyek megfelelően képzettek és tisztában legyenek a jogosultságukkal és a vele járó felelősséggel.

Kapcsolódó intézkedések

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

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

CA-3(6)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

5.9. INFORMÁCIÓCSERE – ÁTHALADÓ INFORMÁCIÓCSERE

5.9. A szervezet:

5.9.1. Az "Információcsere" pont szerint meghatározott EIR-ek által azonosítja a más rendszerek felé történő információáramlást (downstream).

5.9.2. Intézkedéseket hajt végre annak biztosítása érdekében, hogy az áthaladó információáramlás (downstream) megszűnjön, amikor az ezt biztosító rendszerek védelmi intézkedéseinek ellenőrzése vagy hitelesítése nem lehetséges.

MAGYARÁZAT

Az áthaladó (downstream) információcsere, a szervezet EIR-jei és más szervezetek EIR-jei közötti információcserét jelenti. A szervezeti célok megvalósítása szempontjából kritikus rendszerek, szolgáltatások és alkalmazások, illetve a nagy értékű eszközök szempontjából szükséges az ilyen típusú információcserék azonosítása. Az áthaladó (downstream) információcserét megvalósító EIR-ekben, - amelyek közvetlenül vagy közvetve kapcsolódnak az érintett szervezet EIR-jeihez - elengedhetetlen az alkalmazott védelmi intézkedésekkel kapcsolatos átláthatóság, annak érdekében, hogy az említett információcseréből eredő biztonsági kockázatok megérthetők legyenek. A szervezeti EIR-ekre kockázati szempontból hatással lehetnek más EIR-ek, melyek részt vesznek az áthaladó (downstream) információcserében. Ezáltal a szervezeti EIR-ek érintetté válhatnak a downstream EIR-eknél meglévő kockázatok tekintetében az átmeneti kapcsolatokon és információcseréken keresztül, ami sérülékenyebbé teheti a szervezet EIR-jeit a különféle fenyegetésekkel szemben.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell azokat a szervezeti- és szervezeten kívüli EIR-eket, amelyek között áthaladó (downstream) információcsere történik.

2. A szervezetnek pontosan tisztában kell lennie azokkal az alkalmazott védelmi intézkedésekkel, amelyek az áthaladó (downstream) információcserét végző EIR-ekre vonatkoznak. Erre azért van szükség, hogy a szervezet teljeskörűen megérthesse az áthaladó (downstream) információcserével kapcsolatos biztonsági kockázatokat.

3. A szervezetnek fel kell mérnie, hogy a szervezeti EIR-ekre milyen biztonsági kockázatokat jelenthetnek az áthaladó (downstream) információcserét végző EIR-ek az átmeneti kapcsolatokon és információcseréken keresztül.
4. A szervezetnek intézkedéseket kell végrehajtania annak biztosítására, hogy az áthaladó (downstream) információáramlás megszűnjön, amikor az ezt biztosító EIR-ek biztonsági intézkedéseinek ellenőrzése vagy hitelesítése nem lehetséges.

Kapcsolódó intézkedések

17.17. A határok védelme

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

CA-3(7)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

5.10. AZ INTÉZKEDÉSI TERV ÉS MÉRFÖLDKÖVEI

5.10. A szervezet:

5.10.1. Intézkedési tervet dolgoz ki, amelyben mérföldköveket határoz meg az EIR-ben tervezett korrekciós intézkedések dokumentálására, hogy a védelmi intézkedések értékelése során feltárt gyengeségeket vagy hiányosságokat kijavítsák, valamint a rendszer ismert sérülékenységeit csökkentsék vagy megszüntessék.

5.10.2. Rendszeresen frissíti az intézkedési tervet és a mérföldköveket, figyelembe véve a védelmi intézkedések értékeléseit, a független auditokat és felülvizsgálatokat, valamint a folyamatos felügyeleti tevékenységek eredményeit.

MAGYARÁZAT

Az intézkedési tervek és mérföldkövek bármilyen típusú szervezet számára hasznosak a tervezett korrekciós intézkedések nyomon követéséhez. Az intézkedési terveket és a mérföldköveket az illetékes hatóság által meghatározott bejelentési követelményeknek megfelelően kell benyújtani a hatóság részére.

Az érintett szervezetnek olyan intézkedési tervet kell kidolgoznia, amelyben mérföldköveket határoz meg az EIR-ben tervezett korrekciós intézkedések dokumentálására. Ez azt jelenti, hogy a szervezetnek előre meg kell határoznia azokat a lépéseket, amelyeket meg kell tennie annak érdekében, hogy kijavítsa az EIR védelmi intézkedéseinek értékelése során feltárt gyengeségeket vagy hiányosságokat, valamint csökkentse vagy megszüntesse az EIR ismert sérülékenységeit.

Az érintett szervezetnek rendszeresen frissítenie kell az intézkedési tervet és a mérföldköveket, figyelembe véve az EIR védelmi intézkedéseinek értékeléseit, a független auditokat és felülvizsgálatokat, valamint a folyamatos felügyeleti tevékenységek eredményeit. Ezért a szervezetnek folyamatosan felül kell vizsgálnia és módosítania kell az intézkedési tervet és a mérföldköveket, hogy azok mindig naprakészek legyenek és tükrözzék az EIR aktuális állapotát és a védelmi intézkedések hatékonyságát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek olyan intézkedési tervet kell kidolgoznia, amelyben mérföldköveket határoz meg az EIR-ben tervezett korrekciós intézkedések dokumentálására. Ez azt jelenti, hogy a

szervezetnek előre meg kell határoznia azokat a lépéseket, amelyeket meg kell tennie annak érdekében, hogy kijavítsa az EIR védelmi intézkedéseinek értékelése során feltárt gyengeségeket vagy hiányosságokat, valamint csökkentse vagy megszüntesse a rendszer ismert sérülékenységeit.

2. A szervezetnek rendszeresen frissítenie kell a cselekvési tervet és az ahhoz köthető mérföldköveket, figyelembe véve a védelmi intézkedések értékeléseit, a független auditokat és felülvizsgálatokat, valamint a folyamatos felügyeleti tevékenységek eredményeit.

3. A szervezetnek biztosítania kell, hogy az EIR-ben tervezett, illetve megvalósított korrekciós intézkedések megfelelően dokumentálva vannak. Emellett a szervezetnek azt is biztosítania kell, hogy az említett korrekciós intézkedésekhez kapcsolódó mérföldköveket rendszeresen frissítik.

Kapcsolódó intézkedések

5.2. Biztonsági értékelések

5.14. Folyamatos felügyelet

1.4. Intézkedési terv és mérföldkövei

1.10. Kockázatkezelési stratégia

15.20. Kockázatokra adott válasz

18.2. Hibajavítás

18.67. Információ kezelése és megőrzése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

8.3; 9.3.3; 10.2

NIST SP 800-53 rev.5 referencia

CA-5

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

5.11. AZ INTÉZKEDÉSI TERV ÉS MÉRFÖLDKÖVEK – PONTOSSÁG ÉS NAPRAKÉSZSÉG AUTOMATIZÁLT TÁMOGATÁSA

5.11. A szervezet meghatározott automatizált mechanizmusok segítségével biztosítja az EIR intézkedési tervének és mérföldköveinek pontosságát, naprakészségét és elérhetőségét.

MAGYARÁZAT

Az automatizált eszközök használata segít fenntartani az intézkedési terv és a mérföldkövek pontosságát, naprakészségét és elérhetőségét, valamint megkönnyíti a biztonsági információk koordinálását és megosztását a szervezeten belül. Az ilyen koordináció és információmegosztás segít azonosítani a szervezeti EIR-ek rendszerszintű gyengeségeit vagy hiányosságait, és biztosítja, hogy a megfelelő erőforrásokat időben a legkritikusabb EIR sérülékenységekre irányítsák.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek az 5.9-es pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. A szervezetnek olyan automatizált mechanizmusokat kell alkalmaznia, amelyek segítenek fenntartani az intézkedési terv és a mérföldkövek pontosságát, naprakészségét és elérhetőségét, valamint megkönnyíti a biztonsági információk koordinálását és megosztását a szervezeten belül.

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

CA-5(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

5.12. ENGEDÉLYEZÉS

5.12. A szervezet:

5.12.1. Kijelöl egy engedélyezésért felelős személyt, aki az EIR-ért felel.

5.12.2. Kijelöl egy felelős személyt, aki a szervezeti EIR-ekre vonatkozó közös, más rendszerekből áthozott (átörökített) biztonsági követelmények elfogadásáért felel.

5.12.3. Biztosítja, hogy az engedélyezésért felelős személy az EIR használatbavételét megelőzően:

5.12.3.1. elfogadja a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények alkalmazását; és

5.12.3.2. a szervezet vezetőjével engedélyezteti a rendszer működését.

5.12.4. Biztosítja, hogy a közös biztonsági követelményekért felelős személy engedélyezze a közös, más rendszerekből áthozott (átörökített) biztonsági követelmények használatát.

5.12.5. Rendszeresen felülvizsgálja az engedélyeket.

MAGYARÁZAT

Az engedélyezések hivatalos vezetői döntések, amelyeket a felső vezetők hoznak meg. Ennek során engedélyezhetik bizonyos EIR-ek működését, közös biztonsági követelmények átörökítését szervezeti EIR-ekre, emellett elfogadhatják a közös biztonsági követelmények implementációjával járó kockázatot a szervezeti működés és eszközök, az egyének és egyéb szervezetek vonatkozásában. Az engedélyezésért felelős személyek költségvetési felügyeletet biztosítanak az érintett szervezet EIR-jei és közös védelmi intézkedései számára, vagy felelősséget vállalnak az azok által támogatott szervezeti célok és üzleti funkciók megfelelő működéséért. Az engedélyezésért felelős személyek felelősek, illetve elszámoltathatók a szervezet EIR-jeinek működésével és használatával kapcsolatos biztonsági kockázatokért.

Az engedélyezésért felelős személyek folyamatosan adnak ki engedélyeket az EIR-ekkel kapcsolatban, a megvalósított folyamatos felügyeleti programokból származó bizonyítékok alapján. A robosztus folyamatos felügyeleti programok csökkentik a különálló újraengedélyezési folyamatok szükségességét. Az átfogó folyamatos felügyeleti folyamatok alkalmazásával az engedélyezési csomagokban (pl.: felmérésekről készült jelentések, intézkedési tervek és mérföldkövek) található információk folyamatosan frissülnek. Ez naprakész információval látja el az engedélyezésért felelős személyeket, a közös biztonsági

követelmények kidolgozásáért felelős személyeket és rendszertulajdonosokat az EIR-jeik, a biztonsági követelményeik és működési környezetük biztonsági helyzetéről. Az újraengedélyezés költségeinek csökkentése érdekében az engedélyezésért felelős személyek a lehető legnagyobb mértékben kihasználhatják a folyamatos felügyeleti folyamatok eredményeit az újra engedélyezési döntések meghozatalához.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gondoskodnia kell az olyan engedélyezési folyamattal kapcsolatos feladatok ellátásáról, mely az EIR-ért felel. A kijelölt személy a felelős az EIR működésének engedélyezéséért és a közös, más EIR-ekből áthozott (átörökített) biztonsági követelmények elfogadásáért.
2. A szervezetnek gondoskodnia kell az olyan engedélyezési folyamattal kapcsolatos feladatok ellátásáról, mely a szervezeti EIR-ekre vonatkozó közös, más EIR-ekből áthozott (átörökített) biztonsági követelmények elfogadásáért felel.
3. A szervezetnek biztosítania kell, hogy a kijelölt felelős az EIR használatbavételét megelőzően elfogadja a közös, más EIR-ekből áthozott (átörökített) biztonsági követelmények alkalmazását és engedélyezi az EIR működését.
4. A szervezetnek biztosítania kell, hogy a közös biztonsági követelményekért felelős személy engedélyezze a közös, más EIR-ekből áthozott biztonsági követelmények használatát.
5. A szervezetnek rendszeresen felül kell vizsgálnia az engedélyeket. Ez a lépés biztosítja, hogy az EIR-ek biztonsági állapota naprakész maradjon, és hogy a szervezet időben észlelje és kezelje a biztonsági kockázatokat.
6. A szervezetnek nyilvántartást kell vezetnie a folyamatokról és az engedélyezési döntésekről, annak érdekében, hogy bizonyítékot tudjon szolgáltatni a folyamatos felügyeleti programokból származó eredményekről.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.2. Biztonsági értékelések

5.6. Információcsere

5.14. Folyamatos felügyelet

1.10. Kockázatkezelési stratégia

1.11. Engedélyezési folyamatok meghatározása

15.4. Kockázatértékelés

16.58. Fejlesztői változáskövetés

18.67. Információ kezelése és megőrzése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

9.3.1; 9.3.3

NIST SP 800-53 REV.5 REFERENCIA

CA-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

5.13. Engedélyezés – Közös engedélyezés – Szervezeten belüli

5.13. A szervezet olyan együttes engedélyezési folyamatot alkalmaz, amely ugyanazon szervezet több engedélyezőjét is magában foglalja.

Magyarázat

Ha ugyanabból a szervezetből több személy felelős az engedélyezésért (társengedélyezők) az EIR-el kapcsolatban, akkor az növeli a kockázatalapú döntéshozatali folyamat függetlenségének szintjét. Emellett a rendszer engedélyezési folyamatára alkalmazva megvalósítja a felelősségek szétválasztásának és a kettős jóváhagyásnak a koncepcióját. A szervezeten belüli együttes engedélyezési folyamat leginkább az összekapcsolt EIR-ek, a megosztott EIR-ek és a több tulajdonossal rendelkező EIR-ek esetében releváns.

A követelmény alkalmazásának lépései

1. A szervezetnek gondoskodnia kell az EIR-el kapcsolatos engedélyezési feladatok ellátásról. Ezt megteheti úgy, hogy több személyt jelöl ki, akik társengedélyezők lesznek az EIR-el kapcsolatos engedélyezési folyamatokban. A szervezetnek a felelős személyek meghatározásánál figyelembe kell venniük a felelősségek szétválasztásának elvét és a kettős jóváhagyás koncepcióját.
2. A szervezetnek be kell vezetnie egy olyan folyamatot, amely lehetővé teszi az engedélyezők számára, hogy együtt dolgozzanak az EIR engedélyezési folyamatán. Ez magában foglalhatja a feladatok megosztását és a kettős engedélyezést.
3. A szervezetnek biztosítania kell, hogy az engedélyezők rendelkeznek a szükséges képességekkel és ismeretekkel az EIR kockázatainak értékeléséhez és kezeléséhez.
4. A szervezetnek nyilvántartást kell vezetnie az engedélyezési folyamatról, beleértve az összes érintett személy és szervezet tevékenységét.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az engedélyezési folyamatot, hogy biztosítsa annak hatékonyságát és relevanciáját.

Kapcsolódó intézkedések

2.60. Legkisebb jogosultság elve

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CA-6(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

5.14. ENGEDÉLYEZÉS – KÖZÖS ENGEDÉLYEZÉS – SZERVEZETEK KÖZÖTTI

5.14. A szervezet a szervezetek közötti engedélyezés esetén olyan együttes engedélyezési folyamatot alkalmaz, amely magában foglalja ugyanazon szervezet több engedélyezőjét, és legalább egy olyan engedélyező szerepben lévő személyt, aki nem a saját szervezetéhez tartozik.

MAGYARÁZAT

Több engedélyezésre jogosult tisztviselő kijelölése, akik közül legalább egy külső szervezetből érkezik, hogy a rendszer társengedélyezőjeként szolgáljanak, növeli a kockázatalapú döntéshozatali folyamat függetlenségének szintjét. Ez az EIR engedélyezési folyamatára alkalmazva megvalósítja a feladatok szétválasztásának és a kettős engedélyezésnek a koncepcióját. Külső szervezetek engedélyező tisztviselőinek alkalmazása a rendszert tulajdonló vagy a rendszert befogadó szervezet engedélyező tisztviselőjével együtt akkor lehet szükséges, ha a külső szervezeteknek jogos érdeke vagy azonos érdeke fűződik az engedélyezési döntés kimeneteléhez. A szervezetközi közös engedélyezési folyamat releváns és megfelelő az összekapcsolt EIR-ek, a megosztott EIR-ek vagy szolgáltatások, valamint a több információtulajdonossal rendelkező EIR-ek esetében. A külső szervezetek engedélyező tisztviselői az engedélyezés alatt álló EIR kulcsfontosságú érdekeltjei.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először ki kell jelölnie több engedélyezőt, akik közül legalább egy külső szervezetből származik. Ezek a személyek lesznek az EIR együttes engedélyezői, ami növeli a függetlenség szintjét a kockázatalapú döntéshozatali folyamatban.
2. A szervezetnek alkalmaznia kell az engedélyezési folyamatban a feladatok szétválasztásának és a kettős engedélyezésnek az elveit.
3. A szervezetnek be kell vonnia a külső szervezetek engedélyezőit az EIR engedélyezési folyamatába, különösen akkor, ha a külső szervezeteknek jogos vagy azonos érdeke fűződik az engedélyezési döntés kimeneteléhez.

4. A szervezetnek alkalmaznia kell a szervezetközi együttes engedélyezési folyamatot, különösen akkor, ha az EIR kapcsolódik más EIR-ekhez, ha megosztott EIR-ekről vagy szolgáltatásokról van szó, és ha az EIR-nek több tulajdonosa van.
5. A szervezetnek nyilvántartást kell vezetnie az engedélyezési folyamatról, beleértve az összes érintett személy és szervezet tevékenységét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.60. Legkisebb jogosultság elve

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

CA-6(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

5.15. FOLYAMATOS FELÜGYELET

5.15. A szervezet kidolgozza a rendszerszintű folyamatos felügyeleti stratégiát és megvalósítja a folyamatos felügyeletet a szervezeti szintű stratégiával összhangban, amely magában foglalja a következőket:

5.15.1. A rendszerszintű metrikák meghatározását.

5.15.2. Rendszeres felügyelet biztosítását a védelmi intézkedések hatékonyságának értékelésére.

5.15.3. A védelmi intézkedések folyamatos értékelését.

5.15.4. Az EIR és a szervezet által meghatározott mutatók folyamatos nyomon követését.

5.15.5. A védelmi intézkedésekről gyűjtött és feldolgozott információ összegzését és kiértékelését.

5.15.6. A védelmi intézkedések értékelése és elemzése alapján végrehajtott válaszintézkedéseket.

5.15.7. az EIR biztonsági állapotáról rendszeres időközönként történő jelentés a kijelölt személyeknek.

MAGYARÁZAT

A rendszerszintű folyamatos felügyelet lehetővé teszi az EIR biztonsági helyzetének folyamatos ismeretét. A folyamatos felügyelet támogatja az érintett szervezet kockázatkezelési döntéseit. A folyamatos és folytonos kifejezések arra utalnak, hogy a szervezet a szükséges gyakorisággal értékeli és monitorozza a védelmi intézkedéseket és kockázatokat, így támogatva a kockázatalapú döntéseket. Különböző típusú védelmi intézkedések különböző felügyeleti gyakoriságot igényelhetnek. A folyamatos felügyelet eredményeként a szervezet kockázatkezelési intézkedéseket hajt végre. Amikor több olyan, funkció alapján csoportosított védelmi intézkedés hatékonyságát felügyelik, akkor a problémás védelmi intézkedések esetén, a problémát kiváltó okok elemzésre is szükség lehet. A folyamatos felügyelet lehetővé teszi a szervezet számára, hogy az EIR-ek és a közös védelmi intézkedések engedélyezését egy rendkívül dinamikus működési környezetben is fenntartsák, ahol változnak a működési célok és üzleti igények, fenyegetések, sérülékenységek és technológiák. A biztonsági információkhoz történő folyamatos hozzáférés - különféle jelentések és irányítópultok (dashboard) által - lehetővé teszi a felelős, szervezethez köthető személyek számára, hogy hatékony és

megfelelően időzített kockázatkezelési döntéseket hozzanak, beleértve a folyamatos engedélyezési döntéseket is.

Az automatizálás támogatja a hardver-, szoftver- és firmware-leltárak, engedélyezési csomagok és egyéb rendszerinformációk gyakoribb frissítését. A hatékonyságot tovább növeli, ha a folyamatos felügyelet kimenetei úgy vannak kialakítva, hogy konkrét, mérhető, megvalósítható, releváns és időszerű információkat szolgáltassanak. A folyamatos felügyeleti tevékenységet a rendszerek biztonsági kategóriáinak megfelelően kell méretezni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia egy rendszerszintű folyamatos felügyeleti stratégiát, amelyet meg is kell valósítania a gyakorlatban. A kialakítás során a szervezetnek figyelnie kell arra, hogy a rendszerszintű folyamatos felügyeleti stratégia összhangban legyen szervezeti szintű stratégiával.
2. A szervezetnek meg kell határoznia az rendszerszintű metrikákat, amelyek segítségével mérhető a védelmi intézkedések hatékonysága.
3. A szervezetnek rendszeres felügyeletet kell biztosítania a védelmi intézkedések hatékonyságának értékelésére.
4. A szervezetnek folyamatos értékelést kell végeznie az alkalmazott védelmi intézkedésekről, és nyomon kell követnie az EIR és az érintett szervezet által meghatározott mutatókat.
5.A szervezetnek össze kell gyűjtenie és fel kell dolgoznia a védelmi intézkedésekről gyűjtött információkat, majd összegeznie kell és ki kell értékelnie azokat.
6. A szervezetnek létre kell hoznia válaszintézkedéseket a védelmi intézkedések értékelése és elemzése alapján.
7. A szervezetnek rendszeres időközönként jelentést kell készíteni az EIR biztonsági állapotáról a felelős személyek számára.
8. A szervezetnek automatizálnia kell a folyamatokat, hogy gyakrabban frissíthessen a hardver, szoftver és firmware leltárakon, engedélyezési csomagokon és egyéb rendszerinformációkon.
9. A szervezetnek a folyamatos felügyeleti tevékenységeket skáláznia kell az EIR biztonsági kategóriái szerint.

Kapcsolódó intézkedések

2.2. Fiókkezelés

2.60. Legkisebb jogosultság elve

2.100. Távoli hozzáférés

3.13. A biztonsági képzésre vonatkozó dokumentációk

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.44. Információk kiszivárgásának figyelemmel kísérése

5.2. Biztonsági értékelések

5.9. Az intézkedési terv és mérföldkövei

5.11. Engedélyezés

6.7. A konfigurációváltozások felügyelete (változáskezelés)

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

9.1; 9.3.2; 9.3.3; A.5.36

NIST SP 800-53 rev.5 referencia

CA-7

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

5.16. FOLYAMATOS FELÜGYELET – FÜGGETLEN ÉRTÉKELÉS

5.16. A szervezet független értékelőket vagy értékelőcsoportokat alkalmaz az EIR-ben lévő védelmi intézkedések folyamatos ellenőrzésére.

MAGYARÁZAT

Az érintett szervezetek maximalizálják a védelmi intézkedések értékelésének értékét azzal, hogy megkövetelik, hogy az értékeléseket megfelelő függetlenségi szinttel rendelkező értékelők végezzék. A szükséges függetlenségi szint az érintett szervezet folyamatos felügyeleti stratégiáján alapul. Az értékelő függetlensége bizonyos mértékű pártatlanságot biztosít a felügyeleti folyamatban. Ennek eléréséhez az értékelők nem hoznak létre kölcsönös vagy összeférhetetlen érdekeltséget azon szervezetekkel, ahol az értékeléseket végzik, nem értékelik saját munkájukat, nem cselekszenek a szervezetek vezetői vagy alkalmazottai szerepében, és nem helyezik magukat a szervezetek szolgáltatásait igénybe vevő szervezetek érdekében fellépő pozícióba.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely esetekben szükséges a független értékelők vagy értékelőcsoportok igénybevétele az EIR védelmi intézkedéseinek folyamatos ellenőrzéséhez.
2. A szervezetnek ki kell dolgoznia egy folyamatos monitoring stratégiát, amely meghatározza a szükséges függetlenségi szintet az értékelők számára.
3. A szervezetnek meg kell bizonyosodnia arról, hogy az értékelők megfelelő mértékben függetlenek, ezáltal biztosítva a felügyeleti folyamat pártatlanságát.
4. A szervezetnek biztosítania kell, hogy az értékelők ne hozzanak létre kölcsönös vagy összeférhetetlen érdekeltséget a szervezettel.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

9.2.2

NIST SP 800-53 REV.5 REFERENCIA

CA-7(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

5.17. FOLYAMATOS FELÜGYELET – TRENDELEMZÉS

5.17. A szervezet trendelemzéseket alkalmaz, hogy a tapasztalati adatok alapján megállapítsa, szükséges-e módosítani a védelmi intézkedések végrehajtását, a folyamatos felügyeleti tevékenységek gyakoriságát, valamint a folyamatos felügyeleti folyamatban alkalmazott tevékenységtípusokat.

MAGYARÁZAT

A trendelemzések magukban foglalják a fenyegetésekkel kapcsolatos legújabb információk vizsgálatát, amelyek a szervezetben vagy a szervezet számára releváns egyéb szervezeteknél (pl. azonos iparági szereplők) bekövetkezett fenyegető események típusaira, a támadások bizonyos típusainak sikerességi arányaira, a technológiák újonnan megjelenő sérülékenységeire, a fejlődő pszichológiai manipulációs technikákra, a konfigurációs beállítások hatékonyságára, a védelmi intézkedések különböző értékeléseinek az eredményeire, valamint az auditorok megállapításaira vonatkoznak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és be kell vezetnie egy olyan trendelemzési folyamatot, amely segítséget nyújthat annak megállapításában, hogy szükséges-e módosítani a védelmi intézkedések végrehajtását, a folyamatos felügyeleti tevékenységek, gyakoriságát, valamint a folyamatos felügyeleti folyamatban alkalmazott tevékenységtípusokat.
2. A szervezet a trendelemzést többféleképpen megvalósíthatja pl.: kiberbiztonsági hírekkel kapcsolatos hírek sajtófigyelése; megbízható szervezetek által összeállított időszakosan küldött kiberbiztonsági témájú hírlevelekre történő feliratkozás; saját apparátus fenntartása, mely folyamatosan elemzi és értékeli az aktuális kiberbiztonsági trendeket stb.
3. A szervezetnek rendszeresen el kell végeznie ezeket a trendelemzéseket, hogy naprakész legyen a szervezetet érintő legújabb fenyegetésekkel és sérülékenységekkel kapcsolatban.
4. A szervezetnek a trendelemzések eredményeit fel kell használnia a védelmi intézkedések végrehajtásának módosításához, a folyamatos felügyeleti tevékenységek gyakoriságának beállításához, valamint a folyamatos felügyeleti folyamatban alkalmazott tevékenységtípusok módosításához.

5. A szervezetnek a trendelemzések eredményeit be kell építenie a szervezet kockázatkezelési folyamataiba, hogy biztosítsa a kockázatok megfelelő kezelését.
6. A szervezetnek dokumentálnia kell a trendelemzési folyamatot és az eredményeket.
7. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a trendelemzési folyamatot, hogy biztosítsa annak relevanciáját és hatékonyságát.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

9.3.2

NIST SP 800-53 rev.5 referencia

CA-7(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

5.18. Folyamatos felügyelet – Kockázatmonitorozás

5.18. A szervezet biztosítja, hogy a kockázatmonitorozás szerves része legyen a folyamatos felügyeleti stratégiának, amely a következőket tartalmazza:

5.18.1. a hatékonyság ellenőrzését;

5.18.2. a megfelelés ellenőrzését; és

5.18.3. a változások nyomon követését.

Magyarázat

A kockázatmonitorozást az érintett szervezet által meghatározott kockázattűrő képesség határozza meg. A hatékonyság ellenőrzése meghatározza a megvalósított kockázatkezelési intézkedések folyamatos hatékonyságát. A megfelelés ellenőrzése vizsgálja, hogy a szükséges kockázatkezelési intézkedésekből mik azok amik megvalósultak. Továbbá azt is vizsgálja, hogy a biztonsági követelmények közül mi az ami teljesül. A változások nyomon követése azonosítja azokat a változásokat, amelyek az érintett szervezet EIR-jében és működési környezetében történnek, és amelyek befolyásolhatják a biztonsági kockázatokat.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a szervezeti kockázattűrési szintjét, ami a kockázatmonitorozás szükséges bementi információja.

2. A szervezetnek be kell vezetnie egy hatékonyság ellenőrzési rendszert, amely meghatározza a bevezetett kockázatkezelési válasz intézkedések folyamatos hatékonyságát.

3. A szervezetnek megfelelés ellenőrzés keretében vizsgálnia kell, hogy a kockázatkezelési intézkedésekből mik azok, amik megvalósultak. Emellett ennek keretében a szervezetnek azt is vizsgálnia kell, hogy mely biztonsági követelmények teljesülnek.

4. A szervezetnek be kell vezetnie a változások nyomon követését, amely azonosítja az EIR és a működési környezet változásait, amelyek befolyásolhatják a biztonsági kockázatokat.

5. A szervezetnek nyilvántartást kell vezetnie a fent említett lépések végrehajtásáról és az eredményekről, hogy biztosítsa a folyamatos felügyeletet és a kockázatkezelési stratégia hatékonyságának értékelését.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

9.3.2

NIST SP 800-53 rev.5 referencia

CA-7(4)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

5.19. FOLYAMATOS FELÜGYELET – KÖVETKEZETESSÉG ELEMZÉSE

5.19. A szervezet az általa meghatározott intézkedéseket alkalmazza, hogy ellenőrizze a szabályzatok kialakítását, illetve a végrehajtott védelmi intézkedések azzal konzisztens működését.

MAGYARÁZAT

A biztonsági elvárások gyakran fokozatosan kerülnek bevezetésre egy EIR-ben. Ennek eredményeként a védelmi intézkedések kiválasztására és végrehajtására vonatkozó szabályok következetlenek lehetnek, és a védelmi intézkedések nem működhetnek következetes vagy koordinált módon. A következetesség és koordináció hiánya minimum azt jelenti, hogy találhatók elfogadhatatlan biztonsági rések az EIR-ben. Legrosszabb esetben azt jelenti, hogy az egyik helyen vagy egyik komponens által végrehajtott néhány védelmi intézkedés akadályozza más védelmi intézkedések működését (pl.: a hálózati forgalom titkosítása megakadályozhatja a hálózati forgalom felügyeletét). Más helyzetekben, ha nem felügyelik következetesen az összes implementált hálózati protokollt (például az IPv4 és IPv6 kettős használatát), akkor nem szándékos sérülékenységek keletkezhetnek az EIR-ben, amelyeket a támadók kihasználhatnak. Fontos ellenőrizni - tesztelés, felügyelet és elemzés útján - hogy a végrehajtott védelmi intézkedések következetesen, koordináltan és nem zavaró módon működnek-e.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a védelmi intézkedéseket, amelyeket alkalmazni kíván az EIR-ben és annak környezetében.
2. A szervezetnek a meghatározott biztonsági elvárásokat meg kell valósítania.
3. A szervezetnek biztosítania kell, hogy a szabályokat következetesen alkalmazzák.
4. A szervezetnek rendszeresen ellenőriznie kell, hogy a szabályokat ténylegesen alkalmazzák-e, és hogy az alkalmazott intézkedések konzisztens működést eredményeznek-e.

5. A szervezetnek elemzéseket és teszteket kell végeznie annak biztosítása érdekében, hogy az alkalmazott biztonsági intézkedések nem zavarják egymás működését, és hogy nincsenek biztonsági rések az EIR-ben.

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

CA-7(5)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a tevékenységek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

5.20. FOLYAMATOS FELÜGYELET – FELÜGYELET AUTOMATIZÁLT TÁMOGATÁSA

5.20. A szervezet az általa meghatározott automatizált mechanizmusok segítségével biztosítja, hogy a rendszer felügyeleti eredményei pontosak és naprakészek legyenek, valamint rendelkezésre álljanak.

MAGYARÁZAT

Az automatizált felügyeleti eszközök használata segít fenntartani a felügyeleti információk pontosságát, naprakészségét és hozzáférhetőségét. Mindez segít növelni a rendszer biztonsági helyzetének folyamatos figyelemmel kísérésének szintjét, mely támogatja a szervezeti kockázatkezelési döntéseket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek az 5.18-as pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. A szervezetnek meg kell határoznia azokat az automatizált eszközöket, amelyeket a felügyeleti folyamatokban kíván használni.
2. A szervezetnek biztosítania kell, hogy ezek az automatizált eszközök képesek legyenek pontos és naprakész információkat szolgáltatni.
3. A szervezetnek rendszeresen ellenőriznie kell az automatizált eszközök által szolgáltatott információkat.
4. A szervezetnek biztosítania kell, hogy az automatizált eszközök által szolgáltatott információk mindig rendelkezésre álljanak a szervezet számára. Ez magában foglalhatja az információk tárolását és archiválását, valamint a hozzáférés biztosítását a szükséges személyek 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

CA-7(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

5.21. BEHATOLÁSVIZSGÁLAT (PENETRATION TESTING)

5.21. A szervezet behatolásvizsgálatot végez a szervezet által meghatározott gyakorisággal a meghatározott EIR-eken vagy rendszerelemeken.

MAGYARÁZAT

A behatolásvizsgálat egy speciális vizsgálati típus, amelyet az EIR-eken vagy egyes rendszerelemeken végeznek a szakértők annak érdekében, hogy azonosítsák azokat a sérülékenységeket, amelyeket egy támadó kihasználhat. A behatolásvizsgálat túlmutat az automatizált sérülékenységvizsgálaton, és olyan személyek vagy csapatok végzik, akik kiemelkedően magas szintű képességekkel és tudással rendelkeznek a hálózati, operációs rendszer- és alkalmazásszintű biztonsági megoldásokat illetően. A behatolásvizsgálat segít megbizonyosodni arról, hogy a felderített sérülékenységek tényleg jelen vannak-e a vizsgált környezetben, illetve abban is segítséget nyújt, hogy bizonyos előre meghatározott keretek között az EIR-ek mennyire képesek ellenállni egy rosszindulatú behatolási kísérletnek. Az említett keretek közé sorolható az idő, az erőforrás és a szakértelem. A behatolásvizsgálat a létező keretekhez mérten megpróbál szimulálni egy rosszindulatú támadást, és mélyreható információt nyújt a biztonsági résekkel vagy hiányosságokkal kapcsolatosan. A behatolásvizsgálat különösen fontos lehet, ha egy szervezet egy régi technológiáról vált egy újra (pl.: IPv4 hálózati protokollról IPv6 hálózati protokollra történő átállás).

A szervezet felhasználhatja a sérülékenységvizsgálat eredményeit a behatolásvizsgálati tevékenységek támogatására. A behatolásvizsgálatot belsőleg vagy külsőleg végezhetik az EIR hardver-, szoftver- vagy firmware komponensein, és magában foglalhat fizikai és technológiai követelményeket is. A behatolásvizsgálat szabványos módszertana magában foglalja az EIR-rel kapcsolatos teljes ismereteken alapuló előzetes vizsgálatot, az előzetes vizsgálat alapján potenciális sérülékenységek előzetes azonosítását, és a vizsgálatot, amelynek célja a sérülékenységek kihasználhatóságának meghatározása. A vizsgálatot megelőzően minden félnek egyet kell értenie az úgynevezett "alkalmazási szabályok" ("rules of engagement" röviden ROE) minden pontjával. Ez a leírás tartalmazza a vizsgálattal kapcsolatos kikötéseket és szabályozásokat, melynek pontjait a vizsgáló és a vizsgálat alá eső félnek is kötelessége betartani. A szervezet figyelembe veszi a ROE megalkotásakor a rosszindulatú támadók által potenciálisan használt eszközöket, technikákat és eljárásokat.

A vizsgálatot végző szakértők a behatolásvizsgálat során felderíthetnek olyan információkat, melyek jogszabályi vagy egyéb szabályozás védelme alá esnek. A ROE, egyéb szerződések vagy más megfelelő mechanizmusok használata javasolt a hasonló információk felderítése esetén alkalmazandó teendőkre és folyamatokra, illetve arra vonatkozóan is tartalmazhatnak útmutatót, hogyan miképpen kell védeni az említett információt. A kockázatelemzés segíthet eldönteni a szervezetnek, hogy a behatolásvizsgálatot végző személyeknek mennyire kell függetlennek lenniük.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meghatározott gyakorisággal behatolásvizsgálatot kell végeznie vagy végeztetnie a meghatározott EIR-eken vagy egyes rendszerelemeken. Ez egy speciális értékelés, amelyet az EIR-eken vagy az egyes rendszerelemeken végeznek annak érdekében, hogy az azonosított sérülékenységek valóban kihasználhatók-e egy támadó által.
2. A behatolásvizsgálatot olyan személyeknek vagy csapatoknak kell végezniük, akik rendelkeznek a hálózati, operációs rendszer és/vagy alkalmazásszintű biztonság területén igazolható készségekkel és tapasztalattal.
3. A szervezetnek fel kell használnia a sérülékenységvizsgálat eredményeit a behatolásvizsgálati tevékenységek támogatására.
4. A behatolásvizsgálati forgatókönyvek végrehajtásának megkezdése előtt minden érintett félnek egyet kell értenie az úgynevezett "alkalmazási szabályokat" illetően (rules of engagement (ROE)) és annak pontjait minden érintett félnek kötelező betartania.
5. A behatolásvizsgálat során előfordulhat, hogy olyan információk kerülnek felfedésre, melyek jogszabályi vagy egyéb szabályozás védelme alá esnek, ezért a szervezetnek gondoskodnia kell az információ védelmével kapcsolatban szabályok érvényesítéséről a vizsgálat végrehajtása során.

KAPCSOLÓDÓ INTÉZKEDÉSEK

15.10. Sérülékenységmonitorozás és szkennelés
15.22.1. Fenyegetés felderítés
16.66. Fejlesztői biztonsági tesztelés
19.13. Beszerzési stratégiák, eszközök és módszerek
19.16. Beszállítók értékelése és felülvizsgálata

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

CA-8

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság, illetve a rendszerek vagy rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

5.22. Behatolásvizsgálat – Független szakértő vagy csapat

5.22. A szervezet független szakértőt vagy csapatot alkalmaz az EIR vagy a rendszerelemek behatolásvizsgálatának elvégzésére.

Magyarázat

A független behatolástesztet végző szakértők vagy csapatok képesek pártatlan behatolásvizsgálatot végezni a szervezethez köthető EIR-eken. A pártatlanság azt jelenti, hogy a behatolásvizsgálatot végző szakértőknek vagy csapatnak nem lehet semmilyen valós vagy vélt érdekeltségük a behatolásvizsgálat hatóköre alá eső EIR-ek vonatkozásában (pl.: fejlesztés, üzemeltetés, menedzselés). A "Biztonsági értékelések – Független értékelők" pont további információt nyújt a független vizsgálatokkal kapcsolatban, amelyek alkalmazhatók a behatolásvizsgálatok esetén is.

Ilyen biztonsági intézkedésnek lehet tekinteni NBSZ NKI, vagy az arra jogosult gazdálkodó szervezet által végrehajtott Ibtv. szerinti sérülékenységvizsgálatot, amennyiben az magába foglalta a behatolásvizsgálatot is.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia, hogy mely EIR vagy rendszerelemek vonatkozásában szükséges behatolásvizsgálatot végeztetni.
2. A szervezetnek meg kell keresnie egy független szakértőt vagy csapatot, aki vagy amely képes elvégezni az EIR vagy rendszerelem behatolásvizsgálatát.
3. A szervezetnek meg kell állapodnia a független szakértővel vagy csapattal a behatolásvizsgálat részleteiről (pl.: vizsgálat hatóköre, vizsgálat időpontja, vizsgálat során használt módszerek és eszközök, a vizsgálat elvárt eredménytermék).
4. A szervezetnek biztosítania kell, hogy a független szakértő vagy csapat hozzáférjen az EIR-hez vagy a rendszerelemekhez a behatolásvizsgálat elvégzéséhez.
5. A szervezetnek dokumentációt kell készítenie a behatolásvizsgálat folyamatáról és annak eredményeiről.

6. A szervezetnek elemeznie kell a behatolásvizsgálat eredményeit, és meg kell hoznia a szükséges intézkedéseket az EIR biztonságának javítása érdekében.
7. A szervezetnek rendszeresen (pl.: évente) meg kell ismételnie a behatolásvizsgálatot, hogy biztosítsa az EIR folyamatos biztonságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.2. Biztonsági értékelések

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

CA-8(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

5.23. BEHATOLÁSVIZSGÁLAT – „VÖRÖS CSAPAT” (RED TEAM) GYAKORLATOK

5.23. A szervezet meghatározott „vörös csapat” (red team) gyakorlatokat hajt végre annak érdekében, hogy szimulálja a támadók kísérleteit a szervezeti EIR-ek kompromittálására a vonatkozó szabályok szerint.

MAGYARÁZAT

A "vörös csapat" (red team) gyakorlatok kiterjesztik a behatolásvizsgálatok célkitűzéseit azáltal, hogy megvizsgálják az érintett szervezetek biztonsági helyzetét, valamint a hatékony kiberbiztonsági védekezési képességüket. A "vörös csapat" gyakorlatok a szervezeti célok és üzleti funkciók kompromittálására tett kísérleteket szimulálják a támadók szemszögéből és átfogó értékelést nyújtanak az EIR-ek és a szervezet biztonsági helyzetéről. Az említett kísérletek technológiai- és pszichológiai manipuláción alapú támadásokat is magukban foglalhatnak. A technológiai alapú támadások magukban foglalják a hardver-, szoftver- vagy firmware-elemekkel és/vagy a szervezet kitűzött céljaival és üzleti folyamataival történő interakciókat is. A pszichológiai manipuláción alapú támadások magukban foglalják az e-mailen, telefonon, kifigyelésen (shoulder surfing) vagy személyes beszélgetéseken keresztüli interakciókat. A "vörös csapat" gyakorlatok akkor hatékonyak, ha azokat behatolásvizsgálatokban jártas szakértők és csapatok végzik, akik ismerik a legújabb támadási módszereket és kellő tapasztalattal rendelkeznek a fő támadási irányvonalakkal és technikákkal kapcsolatban, illetve az ezekhez köthető eljárásokban és eszközökben. Míg a behatolásvizsgálat elsősorban "laboratóriumi", tehát bizonyos megfontolások alapján előre, külön a tesztelésre kialakított környezet keretei között valósul meg, addig a szervezet a "vörös csapat" gyakorlatokat használhatják a valós körülményeket élethűbben szimuláló, átfogóbb értékelésekhez. A "vörös csapat" gyakorlatok eredményeit a szervezet felhasználhatja a biztonságtudatossági képzések javítására, valamint a szervezet által alkalmazott védelmi intézkedések hatékonyságának felmérésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell bíznia egy "vörös csapatot" (red team), amely olyan szakértőkből áll, akik képesek élethűen szimulálni a támadók kísérleteit a szervezeti EIR-ek kompromittálására a vonatkozó szabályok szerint.
2. A szervezetnek meg kell állapodnia a "vörös csapattal" (red team) a vizsgálat részleteiről (pl.: vizsgálat hatóköre, vizsgálat időpontja, vizsgálat során használt módszerek és eszközök, a vizsgálat elvárt eredményterméke).
3. A vörös csapatnak olyan támadási technikákat kell alkalmaznia, melyek élethűen szimulálják a támadók kísérleteit pl.: technológiai-, illetve pszichológiai manipuláción alapuló támadások.
4. A vörös csapat gyakorlatait olyan személyeknek kell végrehajtaniuk, akik behatolásvizsgálatokban jártas szakértők, ismerik a legújabb támadási módszereket és kellő tapasztalattal rendelkeznek a fő támadási irányvonalakkal és technikákkal kapcsolatban, illetve az ezekhez köthető eljárásokban és eszközökben.
5. A szervezetnek biztosítania kell, hogy a vörös csapat tagjai a szimulált támadásokat valós körülmények között legyenek képesek végrehajtani, így biztosítva, hogy a lehető legátfogóbb értékelést nyújtsa a vizsgálat.
6. A szervezetnek fel kell használnia a vörös csapat gyakorlatainak eredményeit a biztonságtudatossági képzés javítására, valamint a védelmi intézkedések hatékonyságának értékelésére.

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

CA-8(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az ún. "red teaming" gyakorlat meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

5.24. BEHATOLÁSVIZSGÁLAT – FIZIKAI KÖRNYEZET

5.24. A szervezet meghatározott gyakorisággal olyan eljárásokat alkalmaz az EIR fizikai környezetének behatolásvizsgálatára, amelyek magukba foglalják a bejelentett vagy be nem jelentett, a védelmi intézkedések megkerülésére vagy kijátszására irányuló kísérleteket.

MAGYARÁZAT

A fizikai hozzáférési pontok behatolásvizsgálata információt szolgáltathat a szervezeti rendszerek működési környezetének kritikus sérülékenységeiről. Ezek az információk felhasználhatók a szervezeti rendszerek védelméhez szükséges fizikai védelmi intézkedések gyengeségeinek vagy hiányosságainak kijavítására.

Az érintett szervezetnek meghatározott gyakorisággal el kell végeznie ezeket az eljárásokat, amelyek magukba foglalják a bejelentett vagy be nem jelentett, a védelmi intézkedések megkerülésére vagy kijátszására irányuló kísérleteket. Ez azt jelenti, hogy az érintett szervezetnek rendszeresen ellenőriznie kell az EIR fizikai környezetét, hogy azonosítsa a potenciális sebezhetőségeket, és megtegye a szükséges lépéseket a védelmi intézkedések megerősítésére.

Ez a folyamat magában foglalja a naplók elemzését is, amelyek részletes információkat tartalmaznak a behatolási kísérletekről, beleértve az időpontokat, a módszereket és a kísérletek eredményeit. A naplók elemzése segíthet az érintett szervezetnek jobban megérteni a behatolási kísérletek mintázatait, és lehetővé teszi a védelmi intézkedések további finomítását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meghatározott gyakorisággal behatolásvizsgálatot kell végeznie vagy végeztetnie az EIR fizikai környezetének hozzáférési pontjainak vonatkozásában.

2. A behatolásvizsgálatot olyan személyeknek vagy csapatoknak kell végezniük, akik rendelkeznek a fizikai hozzáférési pontok behatolásvizsgálatához szükséges ismeretekkel és tapasztalattal (pl.: jártasak a pszichológiai manipuláción alapuló támadási technikákban, képesek zárat feltörni, illetve belépőkártyákat másolni stb.) A vizsgálat magában foglalhat bejelentett vagy be nem jelentett, a védelmi intézkedések megkerülésére vagy kijátszására irányuló kísérleteket.

3. A szervezetnek meg kell állapodnia a fizikai behatolásvizsgálatot végző személlyel vagy csapattal a vizsgálat részleteiről (pl.: vizsgálat hatóköre, vizsgálat időpontja, vizsgálat során használt módszerek és eszközök, a vizsgálat elvárt eredménytermék).
4. A szervezetnek biztosítania kell, hogy a fizikai behatolásvizsgálatot végző személy vagy csapat tagjai a szimulált támadásokat valós körülmények között legyenek képesek végrehajtani, így biztosítva, hogy a lehető legátfogóbb értékelést nyújtsa a vizsgálat.
5. A szervezetnek fel kell használnia a fizikai behatolásvizsgálatot végző személy vagy csapat eredményeit a biztonságtudatossági képzés javítására, valamint a védelmi intézkedések hatékonyságának értékelésére.

Kapcsolódó intézkedések

5.2. Biztonsági értékelések
12.6. A fizikai belépés ellenőrzése

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

CA-8(3)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

5.25. BELSŐ RENDSZERKAPCSOLATOK

5.25. A szervezet:

5.25.1. Engedélyezi a szervezet által meghatározott rendszerelemeknek vagy rendszerelem kategóriáknak a rendszerhez történő belső kapcsolódását.

5.25.2. Minden belső kapcsolat esetében dokumentálja az interfész jellemzőit, a biztonsági követelményeket, továbbá a kommunikációban részt vevő információ jellegét.

5.25.3. Meghatározott feltételek teljesülése esetén megszünteti a belső rendszerkapcsolatokat.

5.25.4. Meghatározott gyakorisággal felülvizsgálja minden belső kapcsolat további szükségességét.

MAGYARÁZAT

A belső rendszerkapcsolatok olyan kapcsolatok, melyek az adott szervezet rendszerelemei és egyéb, ugyanazon rendszer részét képező, de különálló rendszerelemek között állnak fenn, ideértve a fejlesztésére használt eszközöket is. Belső rendszerkapcsolatok részét képezhetik mobiltelefonok, notebookok és asztali számítógépek, tabletgépek, nyomtatók, másolók, faxgépek, szkennerek, szenzorok és szerverek. Az érintett szervezet a belső rendszerkapcsolatokat nem különálló esetenként hagyja jóvá, hanem közös jellemzőkkel és/vagy konfigurációval, valamint interfésszel rendelkező kategóriákkal dolgozik, beleérte a meghatározott feldolgozási, továbbítás és tárolási képességekkel rendelkező nyomtatókat, szkennereket és másolókat, vagy a specifikus alapkonfigurációval rendelkező okostelefonokat és táblagépeket. Egy belső rendszerkapcsolat szükségességét az érintett szervezet céljainak, vagy üzleti funkcióinak támogatásának szempontjából kell felülvizsgálni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet minden belső kapcsolat esetében dokumentálja az interfész jellemzőit, a biztonsági követelményeket, továbbá a kommunikációban részt vevő információ jellegét.
2. A szervezet leltárt készít azon kategóriákból, melyekbe a belső rendszerkapcsolatok az egyedi jellemzőik alapján rendezhetőek.
3. A szervezet meghatározza a különböző kategóriák által érintett belső rendszerkapcsolatok, valamint a kapcsolódó rendszerelemek felé támasztott biztonsági és funkcionális elvárásokat.

4. A szervezet rendszeresen felülvizsgálja a különböző kategóriákat és szükség esetén módosítja a belső rendszerkapcsolat, valamint az érintett rendszerelemek felé támasztott elvárásokat, vagy eltávolítja azokat.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

2.108. Vezeték nélküli hozzáférés

2.113. Mobil eszközök hozzáférés-ellenőrzése

6.2. Alapkonfiguráció

8.10. Eszközök azonosítása és hitelesítése

17.17. A határok védelme

18.67. Információ kezelése és 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

CA-9

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

5.26. Belső rendszerkapcsolatok – Megfelelőségi ellenőrzések

5.26. A szervezet a biztonsági szabályoknak való megfelelőség ellenőrzést végez a rendszerelemeken, a belső kapcsolatok létrehozása előtt.

Magyarázat

A megfelelőségi ellenőrzések magukban foglalják a vonatkozó alapkonfiguráció ellenőrzését.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a belső rendszerkapcsolatokra vonatkozó alapkonfigurációt.
2. Miután meghatározták az alapkonfigurációt, az érintett szervezetnek ellenőriznie kell, hogy az EIR megfelel-e ezeknek a szabályoknak. Ez magában foglalja a szoftverek, hardverek, hálózati beállítások stb. ellenőrzését.
3. Az ellenőrzés során az érintett szervezetnek nyilvántartást kell vezetnie minden feltárt hibáról, hiányosságról vagy nem megfelelőségről. Ez a nyilvántartás segít azonosítani a problémákat, és lehetővé teszi a szervezet számára, hogy javító intézkedéseket hajtson végre.
4. Az érintett szervezetnek javítania kell minden azonosított hibát, hiányosságot vagy nem megfelelőséget, mielőtt belső kapcsolatokat hozna létre az EIR-ben.

Kapcsolódó intézkedések

6.23. Konfigurációs beállítások

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

CA-9(1)

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