Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Rendszer- és információsértetlenség

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

18.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

18.1. A szervezet:

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

18.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó rendszer- és információsértetlenségi szabályzatot, amely

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

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

18.1.1.2. A rendszer- és információsértetlenségi eljárásrendet, amely a rendszer- és információsértetlenségi szabályok és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

18.1.2. Kijelöl egy meghatározott személyt, aki a rendszer- és információsértetlenségi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

18.1.3. Felülvizsgálja és frissíti az aktuális rendszer- és információsértetlenségi szabályzatot és a rendszer- és információsértetlenségi eljárásokat a meghatározott gyakorisággal és a meghatározott események bekövetkezését követően.

MAGYARÁZAT

A rendszer- és információsértetlenségi szabályzat és eljárások a Rendszer- és információsértetlenség követelménycsoportba tartozó védelmi intézkedésekkel foglalkoznak, amelyek az EIR-ben, illetve a szervezetekben bevezetésre kerülnek. A kockázatkezelési stratégia fontos tényező az ilyen szabályok és eljárások létrehozásában. A szabályok és eljárások hozzájárulnak a biztonság garantálásához. Ezért fontos, hogy a szervezet információbiztonsági szabályozási környezete és rendszer- és információsértetlenségi szabályzat és eljárások összhangban legyenek egymással. A szervezeti szintű biztonsági szabályzatok és eljárásrendek általában előnyösebbek, és szükségtelenné tehetik a működési célok vagy rendszerek szintjén kialakítandó szabályzatokat és eljárásokat. A szabályokat be

lehet illeszteni az általános biztonsági szabályzatba, vagy több szabályzatban is megjelenhetnek, amelyek tükrözik az érintett szervezetek összetett természetét. Eljárásokat létre lehet hozni az információbiztonsági irányítási rendszer, a működési és üzleti célok, és az EIR-ek támogatására, amennyiben azok szükségesek. Az eljárások leírják, hogy hogyan valósulnak meg a szabályok vagy a védelmi intézkedések, és hogyan vonatkoznak az eljárás tárgyát képező egyénre vagy szerepkörre. Az eljárásokat dokumentálhatják a rendszerbiztonsági tervekben, vagy egy vagy több külön dokumentumban. A rendszer- és információsértetlenségi szabályzat és eljárások frissítését kiváltó események lehetnek értékelési vagy audit megállapítások, biztonsági események vagy változások az alkalmazandó jogszabályokban, irányelvekben, szabályozásokban, szabványokban és ajánlásokban. Az elvárt védelmi intézkedések egyszerű újra közlése nem minősülhet szervezeti szabályzatnak vagy eljárásnak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az érintett szervezet dolgozzon ki, dokumentáljon, adja ki és ismertesse meg a szervezet által meghatározott személyekkel szerepkörük szerint az rendszer- és kommunikációvédelmi szabályzatot, amely tartalmazza a szervezeti-, folyamat- és EIR-szintű követelményeket. Ez a szabályzat meghatározza a célkitűzéseket, a hatókört, a szerepköröket, a felelősségeket, a vezetői elkötelezettséget, az érintett szervezeten belüli együttműködés kereteit és a megfelelőségi kritériumokat.
2. A szabályzatnak összhangban kell lennie az érintett szervezetre vonatkozó, hatályos jogszabályokkal, irányelvekkel, szabályozásokkal, szabványokkal és ajánlásokkal.
3. Az érintett szervezet dolgozzon ki egy rendszer- és kommunikációvédelmi eljárásrendet, amely elősegíti a rendszer- és kommunikációvédelmi szabályok és az ahhoz kapcsolódó ellenőrzések megvalósítását.
4. Az érintett szervezet jelöljön ki egy meghatározott személyt, aki felelős a rendszer- és kommunikációvédelmi szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért.

Kapcsolódó intézkedések

1.10. Kockázatkezelési stratégia

14.12. Fegyelmi intézkedések

16.16. Biztonságtervezési elvek

18.67. Információ kezelése és megőrzése

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

3.3.11.2. Rendszer- és információsértetlenségre vonatkozó eljárásrend

ISO/IEC 27001:2023 referencia

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

NIST SP 800-53 rev.5 referencia

SI-1

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

18.2. HIBAJAVÍTÁS

18.2. A szervezet:

18.2.1. Azonosítja, jelenti és kijavítja az EIR hibáit.

18.2.2. A hibajavítással kapcsolatos szoftverfrissítéseket telepítés előtt teszteli a hatékonyság és a potenciális mellékhatások szempontjából.

18.2.3. A biztonsági szempontból releváns szoftver- és firmware-frissítéseket a frissítések kiadását követő meghatározott időtartamon belül telepíti.

18.2.4. A hibajavítást beépíti a szervezet konfigurációkezelési folyamatába.

MAGYARÁZAT

Az érintett szervezet azonosítja azokat az EIR-eket, amelyeket bejelentett szoftversérülékenységek érintenek, majd ezekről jelentést készít és a kijelölt, IT biztonsági felelősséggel rendelkező szervezeti szereplőknek továbbítja. Biztonsági szempontból releváns szoftverfrissítések például a patch-ek, szervízcsomagok, az ún. "hotfix-ek", antivírus leírók alkalmazása. A szervezet kezeli azokat a hibákat is, amelyeket a biztonsági felmérések, folyamatos ellenőrzés, biztonsági eseménykezelés, rendszerhiba-kezelés során tárnak fel.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell az EIR hibáit, beleértve a potenciális sebezhetőségeket, amelyek ezekből a hibákból adódhatnak, és jelentenie kell ezt az információt a szervezet kijelölt személyzetének, akiknek információbiztonsági és adatvédelmi felelősségei vannak.

2. A biztonsági szempontból releváns frissítések telepítése előtt a szervezetnek tesztelnie kell a hibajavításokat a hatékonyság és a potenciális mellékhatások szempontjából. Ezek a frissítések tartalmazhatnak javítócsomagokat, szervízcsomagokat és rosszindulatú kód leírásokat.

3. A szervezetnek a frissítések kiadását követő meghatározott időtartamon belül telepítenie kell a biztonsági szempontból releváns szoftver- és firmware-frissítéseket. Az szervezet által meghatározott időszakok változhatnak számos kockázati tényező alapján, beleértve az EIR biztonsági kategóriáját, a frissítés kritikusságát, a szervezet kockázattűrését, az EIR által támogatott alapfeladatokat vagy a fenyegetési környezetet.

4. A szervezetnek be kell építenie a hibajavítást a konfigurációkezelési folyamatába, hogy a szükséges hibajavítási intézkedéseket nyomon követhesse és ellenőrizhesse.

5. A szervezetnek meg kell határoznia a hibajavítási tevékenység típusát, figyelembe véve a változások típusát, amelyeket konfigurációkezelés alá kell vonni. Bizonyos esetekben a szervezet úgy dönthet, hogy a szoftver- vagy firmware-frissítések tesztelése nem szükséges vagy nem praktikus, például egyszerű rosszindulatú kód leírások frissítése esetén. A tesztelési döntések során a szervezet figyelembe veszi, hogy a biztonsági szempontból releváns szoftver- vagy firmware-frissítések hiteles forrásból származnak-e megfelelő digitális aláírásokkal.

Kapcsolódó intézkedések

5.9. Az intézkedési terv és mérföldkövei

6.7. A konfigurációváltozások felügyelete (változáskezelés)

6.15. Biztonsági hatásvizsgálatok

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

6.23. Konfigurációs beállítások

6.36. Rendszerelem leltár

10.2. Szabályozott karbantartás

15.10. Sérülékenységmonitorozás és szkennelés

16.16. Biztonságtervezési elvek

16.58. Fejlesztői változáskövetés

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

3.3.11.3. Hibajavítás

ISO/IEC 27001:2023 referencia

A.6.8; A.8.8; A.8.32

NIST SP 800-53 rev.5 referencia

SI-2

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

18.3. Hibajavítás – Automatizált hibaelhárítás állapota

18.3. A szervezet meghatározott gyakorisággal a szervezet által meghatározott automatizált mechanizmusokat alkalmaz annak ellenőrzésére, hogy a rendszerelemek rendelkeznek-e a biztonsági szempontból releváns szoftver- és firmware-frissítésekkel.

Magyarázat

Az automatizált mechanizmusok képesek nyomon követni és meghatározni az ismert hibák jelenlétét a rendszerelemekben. Az érintett szervezet meghatározott gyakorisággal alkalmazza ezeket a mechanizmusokat, hogy ellenőrizze, vajon az EIR rendszerelemei rendelkeznek-e a biztonsági szempontból releváns szoftver- és firmware-frissítésekkel.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a gyakoriságot, amellyel ellenőrizni szeretné az rendszerelemek biztonsági frissítéseit. Ez lehet hetente, havonta, negyedévente stb., attól függően, hogy milyen gyakran jelennek meg új frissítések és milyen kritikusak ezek a szervezet számára.
2. A szervezetnek ki kell választania és be kell állítania az automatizált mechanizmusokat, amelyeket az rendszerelemek frissítéseinek nyomon követésére és ellenőrzésére használnak, illetve melyekkel ismert hibák kereshetőek a rendszerelemekben.
3. A szervezetnek rendszeresen ellenőriznie kell az automatizált mechanizmusok működését és hatékonyságát. Ez magában foglalhatja a naplók ellenőrzését, hogy biztosítsa, hogy a frissítések sikeresen telepítésre kerültek, és hogy nincsenek-e ismert hibák vagy problémák.
4. A szervezetnek biztosítania kell, hogy az rendszerelemek frissítéseit a lehető leghamarabb telepítsék, miután elérhetővé válnak. Ez különösen fontos a biztonsági frissítések esetében, amelyek javítják az ismert biztonsági réseket és sebezhetőségeket.

Kapcsolódó intézkedések

5.14. Folyamatos felügyelet

18.13. Az EIR monitorozása

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

3.3.11.3. Hibajavítás

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-2(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

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

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

18.4. HIBAJAVÍTÁS – A HIBÁK KIJAVÍTÁSÁNAK IDEJE ÉS A KORREKCIÓS INTÉZKEDÉSEKRE VONATKOZÓ REFERENCIAÉRTÉKEK

18.4. A szervezet:

18.4.1. Megállapítja a hiba azonosítása és a hiba javítása között elteltidőt.

18.4.2. Referenciaértékeket határoz meg a korrekciós intézkedések megtételéhez.

MAGYARÁZAT

Az érintett szervezet meghatározza, hogy átlagosan mennyi időbe telik a rendszerhibák kijavítása a hibák azonosítása után, és ezt követően szervezeti referenciaértékeket állapít meg a korrekciós intézkedések megtételére. A referenciaértékeket a hiba típusa vagy a potenciális sérülékenység súlyossága alapján lehet meghatározni, ha a hiba kihasználható.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell állapítania, mennyi idő telt el átlagosan egy hiba azonosítása és a hiba javítása között. Ez magában foglalja a hibák azonosítását, a hibák súlyosságának értékelését, és a hibák javítására irányuló intézkedések végrehajtását.
2. A szervezetnek referenciaértékeket kell meghatároznia a korrekciós intézkedések megtételéhez. Ezek a referenciaértékek lehetnek specifikusak a hiba típusára, vagy a potenciális sebezhetőség súlyosságára, ha a hibát ki lehet használni.

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

SI-2(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.5. HIBAJAVÍTÁS – AUTOMATIZÁLT PATCH-MENEDZSMENT ESZKÖZÖK

18.5. A szervezet a meghatározott rendszerelemeken automatizált patch-menedzsment eszközöket alkalmaz a hibajavítás megkönnyítése érdekében.

MAGYARÁZAT

A patch-menedzsmentet támogató automatizált eszközök használata segíthet biztosítani az érintett szervezet számára az újonnan megjelenő rendszerfrissítések észlelését, segíthet csökkenteni a rendszerjavítási műveletek elvégzési idejét, továbbá segíthet biztosítani a frissítések teljességét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a rendszerelemeket, amelyeknél automatizált patch-menedzsment eszközök alkalmazása szükséges / lehetséges.
2. A szervezetnek ki kell választania és be kell szereznie azokat az automatizált patch-menedzsment eszközöket, amelyek a leginkább megfelelnek a rendszerelemek igényeinek.
3. A szervezetnek telepítenie kell és be kell állítania az automatizált patch-menedzsment eszközöket a rendszerelemeken. Ez magában foglalja a szoftverfrissítések, hibajavítások és biztonsági javítások automatikus letöltését és telepítését.
4. A szervezetnek rendszeresen ellenőriznie kell az automatizált patch-menedzsment eszközök működését, hogy biztosítsa a frissítések időben történő telepítését.
5. A szervezetnek naplót kell vezetnie az automatizált patch-menedzsment eszközök által végzett műveletekről. Ez magában foglalja a sikeresen telepített frissítések, a sikertelen telepítési kísérletek és az esetleges hibák naplózását.
6. A szervezetnek rendszeresen felül kell vizsgálnia a naplókat, hogy azonosítsa és kezelje az esetleges problémákat, és biztosítsa a rendszerelemek megfelelő működését.

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

SI-2(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.6. Hibajavítás – Automatikus szoftver - és firmware frissítés

18.6. A szervezet automatikusan telepíti a meghatározott rendszerelemekre a szervezet által meghatározott biztonsági szempontból releváns szoftver- és firmware-frissítéseket.

Magyarázat

Az érintett szervezetek meg kell határozzák, hogy mely esetekben alkalmaznak automatikus szoftver- és firmware frissítéseket annak érdekében, hogy azzal biztosítsák a kritikus biztonsági frissítések mielőbbi telepítését. Ilyen esetekben fontos mérlegelni a sztenderd eljárások megkerülésével járó lehetséges kockázatokat.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, mely rendszerelemeket tekinti biztonsági szempontból relevánsnak. Ez magában foglalhatja az operációs rendszereket, alkalmazásokat, hálózati eszközöket és egyéb rendszerelemeket.
2. A szervezetnek létre kell hoznia egy frissítési politikát, amely meghatározza, hogy milyen típusú frissítések kerülnek automatikus telepítésre. Ez magában foglalhatja a biztonsági frissítéseket, a hibajavításokat és a teljesítményjavításokat.
3. A szervezetnek implementálnia kell egy automatikus frissítési rendszert. Ez lehet egy beépített funkció az EIR-ben, vagy egy külső eszköz, amely képes kezelni a frissítéseket.
4. A szervezetnek be kell állítania a frissítési rendszert úgy, hogy automatikusan telepítse a frissítéseket a meghatározott rendszerelemekre.
5. A szervezetnek rendszeresen ellenőriznie kell a frissítési rendszert, hogy biztosítsa annak megfelelő működését. Ez magában foglalhatja a naplók ellenőrzését a sikeres frissítések megerősítésére, valamint a frissítések utáni tesztelést, hogy biztosítsa az EIR stabilitását és teljesítményét.
6. A szervezetnek fel kell készülnie arra, hogy kezelje azokat a helyzeteket, amikor a frissítések problémákat okoznak az EIR-ben. Ez magában foglalhatja a frissítések visszavonását, a problémák diagnosztizálását és javítását, valamint a felhasználók támogatását a frissítésekkel kapcsolatos problémák esetén.

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

SI-2(5)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági szempontból releváns szoftver- és firmware-frissítések illetve a rendszerelemek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

18.7. HIBAJAVÍTÁS – KORÁBBI SZOFTVER- ÉS FIRMWARE-VERZIÓK ELTÁVOLÍTÁSA

18.7. A szervezet eltávolítja a szoftver- és firmware-elemek korábbi verzióit, miután azok frissített változatait telepítették.

MAGYARÁZAT

Azok a korábbi szoftver- vagy firmware-összetevők, amelyek nem kerülnek eltávolításra a rendszerből a frissítések telepítése után és elavult verziójúak, kihasználhatóak lehetnek egy esetleges támadás során, ezért az érintett szervezetnek szükséges a frissítéseket követően eltávolítani azokat. Néhány piaci megoldás képes automatikusan eltávolítani a rendszerből a szoftverek és firmware-ek korábbi verzióit, ezek használata javasolt.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy minden szoftver- és firmware-elem legfrissebb verzióját telepíti az EIR-jébe.
2. A frissítések telepítése után a szervezetnek ellenőriznie kell az EIR-jét, hogy megbizonyosodjon arról, hogy a szoftver- és firmware-elemek korábbi verziói automatikusan eltávolításra kerültek-e.
3. Ha a korábbi verziók nem kerültek automatikusan eltávolításra, a szervezetnek manuálisan kell eltávolítania őket az EIR-ből, vagy egy ezt megoldó automatizált eszközt vagy módszert szükséges bevezetnie.
4. A szervezetnek naplót kell vezetnie minden eltávolított szoftver- és firmware-elemről, hogy nyomon követhető legyen a folyamat.
5. A szervezetnek rendszeresen ellenőriznie kell az EIR-jét, hogy biztosítsa, hogy nincsenek elavult szoftver- vagy firmware-elemek.

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

SI-2(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a szoftver és firmware összetevők meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.8. KÁRTÉKONY KÓDOK ELLENI VÉDELEM

18.8. A szervezet:

18.8.1. Kártékony kódok elleni védelmi mechanizmusokat alkalmaz a rendszer belépési és kilépési pontjain, hogy felderítse és megfelelő módon eltávolítsa a kártékony kódokat.

18.8.2. A védelmi mechanizmusokat automatikusan frissíti minden olyan esetben, amikor új verziók jelennek meg összhangban a szervezet konfigurációkezelési szabályaival.

18.8.3. A kártékony kódok elleni védelmi mechanizmusokat úgy konfigurálja, hogy:

18.8.3.1. Meghatározott időközönként átvizsgálja a rendszert, és valós időben ellenőrzi a külső forrásokból származó fájlokat a végpontokon, a hálózati belépési vagy kilépési pontokon a biztonsági szabályzatnak megfelelően, amint a fájlokat letöltik, megnyitják vagy futtatják.

18.8.3.2. Kártékony kód észlelésekor blokkolja vagy karanténba helyezi a kártékony kódokat, vagy a szervezet által meghatározott egyéb intézkedéseket hajt végre; továbbá riasztást küld a szervezet által meghatározott személyeknek vagy szerepköröknek.

18.8.4. Ellenőrzi a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe veszi ezek lehetséges kihatását az EIR rendelkezésre állására.

MAGYARÁZAT

Az információs rendszerek be- és kilépési pontjai lehetnek például a tűzfalak, az elektronikus levelezőkiszolgálók, a webkiszolgálók, a proxy szerverek, a távoli hozzáférést biztosító kiszolgálók, a munkaállomások, notebook számítógépek és mobileszközök. Kártékony kód lehet például vírus, féreg, trójai vírus, vagy kémprogramok. Kártékony kód több formátumban kódolható, tárolható tömörített vagy rejtett fájlokban, vagy szteganográfiával elrejtett fájlokban. Kártékony kód különböző módokon is terjedhet, például webes hozzáférésen keresztül, elektronikus levélben, elektronikus levél csatolmányaként, hordozható tárolókon. A kártékony kód bejuttatása a rendszerbe az információs rendszer sérülékenységén keresztül is történhet. A kártékony kód elleni védelmi mechanizmusok lehetnek például az antivírus leírók és a heurisztikán alapuló rendszerek. Számos technológia és eljárás létezik a kártékony kódok hatásának csökkentésére vagy megszüntetésére. Átható konfigurációkezelés és átfogó szoftver integritási intézkedések hatékonyak lehetnek a jogosulatlan kód futásának megakadályozásában. A piacon elérhető szoftvereken felül kártékony kódot az egyedi fejlesztéssel készített szoftverek is tartalmazhatnak. Ilyenekre példa a logikai bombák,

backdoorok és egyéb kibertámadási megoldások, amelyek a szervezet üzleti céljaira és funkcióira lehetnek hatással. A hagyományos kártékony kód elleni védelmi mechanizmusok nem mindig érzékelik ezeket a támadásokat. Ezekben a helyzetekben a szervezet más biztosítékra kell, hogy támaszkodjon, például biztonságos fejlesztési (kódolási) eljárások, konfiguráció kezelés, megbízható beszerzési eljárások, monitorozási gyakorlat segíthet abban, hogy a szoftver csak a kívánt funkciókat hajtsa végre. A szervezet dönthet úgy, hogy a kártékony kód észlelésére adott válasz eltérő tevékenységeket foglalhat magában. Például, a szervezet meghatározhat teendőket a rendszeresen futtatott ellenőrzésekkel talált kód esetére, a kártékony letöltésekkel kapcsolatban, vagy amikor futtatható állományok viselkedésében ismernek fel kártékony működést. Kártékony kód elleni védelmi mechanizmus használata esetén az érintett szervezetnek olyan megoldást javasolt választania, mely egyaránt képes blokkolni, valamint független környezetben vizsgálni a kártékony kódot, képes azt karanténba helyezni - a terjedését meggátolva. Kiemelten fontos a kártékony kód elleni védelemnél a frissítések (pl. vírusdefiníciós adatbázis) gyakorisága, valamint a rendszer általi átvizsgálások ütemezhetőségi és mélységi beállítási lehetőségei.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Kártékony kódok elleni védelmi mechanizmusokat szükséges alkalmazni a rendszerek belépési és kilépési pontjain. Ezek a pontok magukban foglalhatják a tűzfalakat, távoli hozzáférési szervereket, munkaállomásokat, elektronikus levelező szervereket, web szervereket, proxy szervereket, notebook számítógépeket és mobil eszközöket.
2. Automatikusan frissíteni szükséges a védelmi mechanizmusokat minden olyan esetben, amikor új verziók jelennek meg, összhangban a szervezet konfigurációkezelési szabályaival.
3. Szükséges a megfelelő konfiguráció alkalmazása a kártékony kódok elleni védelmi mechanizmusok esetén, hogy meghatározott időközönként átvizsgálják a rendszereket, és valós időben ellenőrizzék a külső forrásokból származó fájlokat a végpontokon, a hálózati belépési vagy kilépési pontokon a biztonsági szabályzatnak megfelelően, amint a fájlokat letöltik, megnyitják vagy futtatják.
4. Kártékony kód észlelésekor szükséges blokkolni vagy karanténba helyezni a kártékony kódokat, vagy a szervezet által meghatározott egyéb intézkedéseket végrehajtani; továbbá riasztást küldeni a szervezet által meghatározott személyeknek vagy szerepköröknek.

5. Ellenőrizni szükséges a téves riasztásokat a kártékony kód észlelése és megsemmisítése során, valamint figyelembe kell venni ezek lehetséges kihatását a rendszerek rendelkezésre állására.
6. Biztosítani szükséges további védelmi intézkedéseket, mint például biztonságos kódolási gyakorlatok, konfigurációkezelés és -ellenőrzés, megbízható beszerzési folyamatok és naplózás, hogy biztosítsa, hogy az EIR nem hajt végre más funkciókat, mint amelyeket szándékozott.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.28. Információáramlási szabályok érvényesítése
2.113. Mobil eszközök hozzáférés-ellenőrzése
6.7. A konfigurációváltozások felügyelete (változáskezelés)
6.36. Rendszerelem leltár
9.9.1. Biztonsági események kezelése
10.4. Karbantartási eszközök
10.11. Távoli karbantartás
13.9. Központi kezelés
15.10. Sérülékenységmonitorozás és szkennelés
17.17. A határok védelme

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

3.3.11.4. Kártékony kódok elleni védelem

ISO/IEC 27001:2023 REFERENCIA

A.8.7

NIST SP 800-53 REV.5 REFERENCIA

SI-3

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

18.9. KÁRTÉKONY KÓDOK ELLENI VÉDELEM – FRISSÍTÉSEK PRIVILEGIZÁLT FELHASZNÁLÓK ÁLTAL

18.9. A szervezet kizárólag privilegizált felhasználó által frissíti a kártékony kódok elleni védelmi mechanizmusokat.

MAGYARÁZAT

A kártékony kódok elleni védelmi rendszereket csak a megfelelő hozzáférési jogosultsággal és megfelelő szaktudással rendelkező felhasználó frissítheti, ezzel az érintett szervezet csökkenti a jogosulatlan módosításokból eredő kockázatokat, valamint elkerülheti a rendszer nem kívánt félreparaméterezését.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először ki kell jelölnie egy vagy több privilegizált felhasználót, akik felelősek lesznek a kártékony kódok elleni védelmi mechanizmusok frissítéséért.
2. A kijelölt privilegizált felhasználóknak megfelelő képzést kell kapniuk a kártékony kódok elleni védelmi mechanizmusok kezeléséről és frissítéséről, beleértve a frissítések telepítésének legjobb gyakorlatait és a potenciális problémák megoldását.
3. A szervezetnek be kell vezetnie egy szabályrendszert, amely előírja, hogy a kártékony kódok elleni védelmi mechanizmusokat kizárólag a privilegizált felhasználók frissíthetik az EIR-ben.
4. A szervezetnek naplózásra van szüksége, hogy nyomon követhesse, mikor és milyen frissítéseket hajtottak végre a privilegizált felhasználók. Ez segít azonosítani a potenciális biztonsági réseket és megelőzni a jövőbeni biztonsági eseményeket.
5. A szervezetnek rendszeresen ellenőriznie kell a privilegizált felhasználók tevékenységét, hogy biztosítsa a kártékony kódok elleni védelmi mechanizmusok megfelelő frissítését.
6. Végül, de nem utolsósorban, a szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kártékony kódok elleni védelmi mechanizmusokkal kapcsolatos politikáit és eljárásait, hogy biztosítsa azok hatékonyságát és relevanciáját.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

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

SI-3(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.10. Rosszindulatú kód elleni védelem – Tesztelés és ellenőrzés

18.10. A szervezet:

18.10.1. meghatározott gyakorisággal teszteli a rosszindulatú kódok elleni védelmi mechanizmusait úgy, hogy ártalmatlan kódot juttat be a rendszerbe; és

18.10.2. ellenőrzi, hogy a kód észlelése és a kapcsolódó biztonsági események jelentése megtörténik-e.

Magyarázat

Az érintett szervezet az ártalmatlan, ugyanakkor a vírusvédelmi rendszerek által felismerhető kódok bejuttatásával ellenőrizni tudja a reagálóképességet, valamint az alkalmazott vírusvédelmi rendszer teljeskörűségét.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a rosszindulatú kódok elleni védelmi mechanizmusainak tesztelési gyakoriságát. Ez lehet például heti, havi vagy éves gyakoriság, attól függően, hogy milyen gyakran változnak a kódok és milyen gyorsan kell reagálni a változásokra.
2. Az szervezetnek be kell juttatnia egy ártalmatlan kódot az EIR-be. Ez a kód nem okoz kárt, de a védelmi mechanizmusoknak észlelniük kell, mint potenciális fenyegetést.
3. Az szervezetnek ellenőriznie kell, hogy a kód észlelése megtörtént-e. Ez azt jelenti, hogy a védelmi mechanizmusoknak jelenteniük kell a kód bejutását, és a kapcsolódó biztonsági eseményeket is naplózniuk kell.
4. A szervezetnek ellenőriznie kell, hogy a biztonsági események jelentése megtörtént-e. Ez azt jelenti, hogy a védelmi mechanizmusoknak jelenteniük kell a kód bejutását, és a kapcsolódó biztonsági eseményeket is naplózniuk kell.
5. Ha a teszt sikeres, a szervezetnek folytatnia kell a tesztelést a megadott gyakorisággal. Ha a teszt nem sikeres, a szervezetnek felül kell vizsgálnia és módosítania kell a védelmi mechanizmusokat, hogy megfeleljenek a követelményeknek.

6. A szervezetnek dokumentálnia kell a tesztelési folyamatot és az eredményeket, hogy bizonyíték legyen a megfelelőségről, és hogy a jövőbeni tesztelések során referenciaként szolgáljon.

Kapcsolódó intézkedések

5.2. Biztonsági értékelések

5.14. Folyamatos felügyelet

15.10. Sérülékenységmonitorozás és szkennelés

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

SI-3(6)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

18.11. KÁRTÉKONY KÓDOK ELLENI VÉDELEM – JOGOSULATLAN PARANCSOK ÉSZLELÉSE

18.11. Az EIR:

18.11.1. felismeri a meghatározott hardverelemeken a nem engedélyezett operációsrendszer parancsokat a rendszermag (kernel) alkalmazásprogramozási interfészen (API) keresztül; és

18.11.2. figyelmeztetést ad ki, naplózza a végrehajtási kísérletet, és megakadályozza a parancs végrehajtását.

MAGYARÁZAT

Az EIR képes felismerni a nem engedélyezett operációsrendszer parancsokat a meghatározott hardverelemeken a rendszermag (kernel) alkalmazásprogramozási interfészein (API) keresztül. Ez a képesség nem csak a kernel-alapú interfészekre korlátozódik, hanem más kritikus interfészekre is alkalmazható, beleértve a virtuális gépek és privilegizált alkalmazások interfészeit is. A nem engedélyezett operációsrendszer parancsok magukban foglalják a rendszermag funkciókhoz tartozó parancsokat azoktól a rendszerfolyamatoktól, amelyek normális működésük folyamán nem indítanak ilyen parancsokat, valamint azokat a parancsokat, amelyek gyanúsak, még akkor is, ha az adott típusú parancsok indítása elfogadható a folyamatok számára.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, hogy mely hardverelemeket tekinti kritikusnak, és mely operációsrendszer parancsokat tekinti nem engedélyezettnek ezen elemek esetén. Ez magában foglalhatja a rendszermag funkciókhoz tartozó parancsokat, amelyeket nem megbízható folyamatok indítanak, valamint azokat a parancsokat is, amelyek gyanúsak, még akkor is, ha az adott típusú parancsok indítása elfogadható a folyamatok számára.
2. A szervezetnek az EIR-t úgy kell konfigurálnia, hogy felismerje a nem engedélyezett operációsrendszer parancsokat a rendszermag (kernel) alkalmazásprogramozási interfészen (API) keresztül. Ez magában foglalhatja a parancstípusok, parancsosztályok vagy konkrét parancspéldányok kombinációjának meghatározását.

3. A szervezetnek be kell állítania az EIR-t, hogy figyelmeztetést adjon ki, naplózza a végrehajtási kísérletet, és megakadályozza a parancs végrehajtását. Ez magában foglalhatja különböző intézkedések meghatározását különböző típusú, osztályú vagy példányú rosszindulatú parancsok esetén.

4. A szervezetnek rendszeresen ellenőriznie kell az EIR-t, hogy biztosítsa, hogy a nem engedélyezett parancsok felismerése és a végrehajtási kísérletek naplózása megfelelően működik.

5. Végül, a szervezetnek folyamatosan frissítenie kell az EIR-t, hogy képes legyen felismerni az új típusú nem engedélyezett parancsokat, és naplózni a végrehajtási kísérleteket.

Kapcsolódó intézkedések

4.2. Naplózható események

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.40. Naplóbejegyzések létrehozása

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

SI-3(8)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

18.12. KÁRTÉKONY KÓDOK ELLENI VÉDELEM – KÁRTÉKONY KÓDOK ELEMZÉSE

18.12. A szervezet:

18.12.1. meghatározott eszközöket és technikákat alkalmaz a kártékony kódok jellemzőinek és viselkedésének elemzésére; és

18.12.2. a kártékony kódok elemzéséből származó eredményeket beépíti a szervezet hibajavítási eljárásaiba és a biztonsági események kezelésére vonatkozó eljárásokba.

MAGYARÁZAT

Az érintett szervezet a kártékony kódok elemzésére szolgáló eszközök alkalmazásával mélyebb betekintést nyer a rosszindulatú támadók tevékenységébe, valamint a kártékony kódok konkrét példányainak funkciójába és céljába. A kártékony kódok jellemzőinek megértése elősegíti a szervezet hatékony válaszát a jelenlegi és jövőbeli fenyegetésekre. A szervezet kártékony kódok elemzését végrehajthatja visszafejtési technikák alkalmazásával vagy a végrehajtás alatt álló kód viselkedésének megfigyelésével.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először ki kell választania és be kell szereznie a kártékony kódok elemzéséhez szükséges eszközöket és technikákat. Ezek az eszközök segítenek a szervezetnek mélyebben megérteni a támadók által használt módszereket, valamint a kártékony kódok funkcióját és célját.
2. A szervezetnek meg kell határoznia a kártékony kódok elemzésének folyamatát. Ez magában foglalhatja a visszafejtési technikák alkalmazását, vagy a végrehajtás alatt álló kód viselkedésének monitorozását.
3. A szervezetnek rendszeresen el kell végeznie a kártékony kódok elemzését, hogy naprakész információval rendelkezzen a jelenlegi és jövőbeli fenyegetésekről.
4. A szervezetnek be kell építenie a kártékony kódok elemzéséből származó eredményeket a hibajavítási eljárásaiba és a biztonsági események kezelésére vonatkozó eljárásokba. Ez azt jelenti, hogy az elemzés eredményeit felhasználják a hibák javítására, a biztonsági események kezelésére és a jövőbeli fenyegetések megelőzésére.

5. A szervezetnek naplót kell vezetnie a kártékony kódok elemzésének eredményeiről, a hibajavítási eljárásokról és a biztonsági események kezeléséről. A napló segít a szervezetnek nyomon követni a kártékony kódokkal kapcsolatos tevékenységeket, és bizonyítékot szolgáltat a kiberbiztonsági követelményeknek való megfelelésről.

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

SI-3(10)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.13. AZ EIR MONITOROZÁSA

18.13. A szervezet:

18.13.1. Monitorozza a rendszert, hogy észlelje:

18.13.1.1. A támadásokat és a potenciális támadásokra utaló jeleket összhangban a meghatározott felügyeleti célokkal;

18.13.1.2. Az engedély nélküli helyi, hálózati és távoli kapcsolatokat.

18.13.2. Azonosítja a rendszer jogosulatlan használatát a meghatározott technikák és módszerek alkalmazásával.

18.13.3. Aktiválja a belső felügyeleti képességeket vagy telepíti a felügyeleti eszközöket:

18.13.3.1. az egész rendszerre kiterjedően a szervezet által meghatározott információk gyűjtése érdekében; illetve

18.13.3.2. a rendszeren belül ad-hoc módon meghatározott helyeken a szervezet által meghatározott információk gyűjtése érdekében.

18.13.4. Elemzi az észlelt eseményeket és rendellenességeket.

18.13.5. Módosítja a rendszerfelügyeleti tevékenység szintjét, amikor változik a szervezeti műveletekkel, az eszközökkel, az egyénekkel, a külső szervezetekkel kapcsolatos kockázati szint.

18.13.6. Jogi állásfoglalást kér a rendszerfelügyeleti tevékenységekről.

18.13.7. Biztosítja a szervezet által meghatározott rendszerfelügyeleti információkat a meghatározott személyeknek vagy szerepköröknek a szervezet által meghatározott gyakorisággal.

MAGYARÁZAT

A rendszerek monitorozása magában foglalja a külső és belső monitorozást. A külső monitorozás a rendszer külső interfészeinél bekövetkező események megfigyelését jelenti. A belső monitorozás a rendszeren belül bekövetkező események megfigyelését jelenti. Az érintett szervezetek monitorozzák a rendszereket a napló tevékenységek valós idejű megfigyelésével vagy más rendszeraspektusok, például hozzáférési minták, hozzáférési jellemzők és más műveletek megfigyelésével. A monitorozási lehetővé teszi a megfelelő döntések meghozatalát, az irányítást és az események észlelését. A rendszerek monitorozását számos eszköz és technika segítségével érik el, beleértve az behatolás észlelő és megelőző rendszereket, a kártékony kód

elleni védelmi szoftvereket, a szkennelő eszközöket, a napló rekord monitorozó szoftvereket és a hálózat monitorozó szoftvereket.

A biztonsági architektúrától függően a monitorozó eszközök elosztása és konfigurációja befolyásolhatja a kulcsfontosságú belső és külső határokon, valamint a hálózat más helyein a hálózati áteresztőkészség késleltetésének bevezetése miatt az áteresztőképességet. Ha szükséges az áteresztőképesség kezelése, az ilyen eszközöket olyan stratégiával helyezik el és telepítik, hogy a szervezet által meghatározott szervezeti szintű biztonsági architektúra részeként jelenjenek meg. A monitorozó eszközök stratégiailag megfontolt helyei közé tartoznak a kiválasztott hálózati határok és a kulcsfontosságú szerverek és szerverfarmok, amelyek kritikus alkalmazásokat támogatnak. Az összegyűjtött információ a szervezet monitorozási céljainak és a rendszerek képességeinek függvényében kerül összeállításra. A figyelembe vett tranzakciók különleges típusai közé tartozik a HTTP proxy-kat megkerülő HTTP forgalom. Az EIR monitorozása a szervezet folyamatos monitorozási és biztonsági eseményválasz programjainak szerves része, és az EIR monitorozásból származó kimenet bemenetként szolgál ezekhez a programokhoz.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Szükséges az EIR monitorozása, hogy észlelésre kerüljenek a támadások és a potenciális támadásokra utaló jelek, összhangban a meghatározott szervezeti célokkal. Ez magában foglalja a külső és belső monitorozást is.
2. Azonosítani szükséges a rendszerek jogosulatlan használatát a meghatározott technikák és módszerek alkalmazásával.
3. Aktiválni szükséges az EIR belső felügyeleti képességeit vagy telepíteni a megfelelő felügyeleti eszközöket az egész EIR-re kiterjedően a szervezet által meghatározott információk gyűjtése érdekében; illetve az EIR-en belül ad-hoc módon meghatározott helyeken a szervezet által meghatározott információk gyűjtése érdekében.
4. Elemezni szükséges az észlelt eseményeket és rendellenességeket.
5. Módosítani szükséges az EIR felügyeleti tevékenység szintjét, amennyiben változik a szervezeti műveletekkel, az eszközökkel, az egyénekkel, a külső szervezetekkel kapcsolatos kockázati szintje.
6. Jogi állásfoglalást szükséges kérni az EIR felügyeleti tevékenységeiről.

7. Biztosítani szükséges a szervezet által meghatározott EIR felügyeleti információkat a meghatározott személyeknek vagy szerepköröknek a szervezet által meghatározott gyakorisággal.
8. A naplózás fontos része az EIR felügyeletének, melynek során figyelemmel kell kísérni a rendszerben történő eseményeket és tevékenységeket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

2.75.1. A rendszerhasználat jelzése

2.100. Távoli hozzáférés

4.2. Naplózható események

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.22. Naplóbejegyzések csökkentése és jelentéskészítés

4.25. Naplóinformációk védelme

4.40. Naplóbejegyzések létrehozása

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

3.3.11.5. Az elektronikus információs rendszer felügyelete

ISO/IEC 27001:2023 REFERENCIA

A.8.16

NIST SP 800-53 REV.5 REFERENCIA

SI-4

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

18.14. AZ EIR MONITOROZÁSA – BEHATOLÁSÉRZÉKELŐ RENDSZER

18.14. A szervezet az egyedi behatolásérzékelő eszközöket egy rendszerszintű behatolásérzékelő rendszerbe konfigurálja és csatlakoztatja.

MAGYARÁZAT

Az egyedi behatolásérzékelő eszközök összekapcsolása egy rendszerszintű behatolásérzékelő rendszerbe (IDS) további lefedettséget és hatékony észlelési képességeket biztosít. Az behatolásérzékelő eszközben található információ széles körben megosztható az érintett szervezetben, így a rendszerszintű észlelési képesség robosztusabbá és erőteljesebbé válik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az egyedi behatolásérzékelő eszközök kiválasztása.
2. A szervezetnek meg kell terveznie és implementálnia kell egy rendszert, amely képes kezelni és integrálni az egyedi behatolásérzékelő eszközöket.
3. A szervezetnek konfigurálnia kell az egyedi behatolásérzékelő eszközöket, hogy azok megfelelően kommunikáljanak a közös rendszerben. Ez magában foglalhatja a kommunikációs protokollok, hitelesítési mechanizmusok és adatátviteli formátumok beállítását.
4. A szervezetnek csatlakoztatnia kell az egyedi behatolásérzékelő eszközöket a rendszerhez. Ez magában foglalhatja a fizikai csatlakoztatást, hálózati beállításokat és a szoftveres integrációt.
5. A szervezetnek tesztelnie kell a rendszer működését, hogy biztosítsa az egyedi behatolásérzékelő eszközök megfelelő integrációját és működését.

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

SI-4(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.15. AZ EIR MONITOROZÁSA – AUTOMATIZÁLT ESZKÖZÖK ÉS MECHANIZMUSOK VALÓS IDEJŰ ELEMZÉSHEZ

18.15. Az EIR automatizált eszközöket és mechanizmusokat alkalmaz, amelyek támogatják az események majdnem valós idejű elemzését.

MAGYARÁZAT

Az érintett szervezet automatizált eszközöket alkalmaz az események szinte valós idejű elemzésének támogatására. Az automatizált eszközök közé tartoznak például a munkaállomás alapú, hálózati alapú, átvitel alapú vagy tároláson alapuló eseményfigyelő eszközök vagy biztonsági és eseménykezelő technológiák, amelyek valós idejű elemzést adnak a szervezeti információs rendszerek által generált figyelmeztetésekről és/vagy értesítésekről.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell szereznie azokat az automatizált eszközöket és mechanizmusokat, amelyek támogatják az események majdnem valós idejű elemzését. Ezek közé tartoznak a host-alapú, hálózat-alapú, szállítás-alapú vagy tárolás-alapú eseményfigyelő eszközök és mechanizmusok, vagy a biztonsági információ- és eseménykezelő technológiák (SIEM), amelyek valós idejű elemzést biztosítanak az EIR által generált riasztásokról és értesítésekről.
2. A szervezetnek figyelembe kell vennie, hogy az automatizált monitorozási technikák nem várt adatvédelmi kockázatokat hozhatnak létre, mivel az automatizált ellenőrzések csatlakozhatnak külső vagy egyébként nem kapcsolódó rendszerekhez. Ezeknek a rendszereknek a rekordjainak összehasonlítása nem várt következményekkel járhat.
3. A szervezetnek értékelnie és dokumentálnia kell ezeket a kockázatokat az adatvédelmi hatásvizsgálatukban, és olyan döntéseket kell hozniuk, amelyek összhangban vannak az adatvédelmi programtervükkel.
4. A szervezetnek naplózásra van szüksége, hogy nyomon követhesse az EIR-ben történő eseményeket és változásokat. A naplózás segít azonosítani a potenciális biztonsági problémákat és azok forrását.

5. Végül, de nem utolsósorban, a szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR kiberbiztonsági protokolljait és gyakorlatait, hogy biztosítsa azok hatékonyságát és relevanciáját a változó kiberbiztonsági környezetben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.11.5. Az elektronikus információs rendszer felügyelete

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-4(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

18.16. AZ EIR MONITOROZÁSA – AUTOMATIZÁLT ESZKÖZÖK ÉS MECHANIZMUSOK INTEGRÁCIÓJA

18.16. A szervezet automatizált eszközök és mechanizmusok segítségével integrálja a behatolásellenőrző berendezéseket a hozzáférés- és áramlásszabályozási mechanizmusokba.

MAGYARÁZAT

Az érintett szervezet automatizált eszközök és mechanizmusok segítségével integrálja a behatolásellenőrző berendezéseket a hozzáférés- és folyamatszabályozási mechanizmusokba. Ez lehetővé teszi a gyors reagálást a támadásokra, mivel lehetségessé válik a mechanizmusok újrakonfigurálása a támadások izolálása és megszüntetése érdekében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell szereznie azokat az automatizált eszközöket és mechanizmusokat, amelyek képesek integrálódni az EIR hozzáférés- és folyamatszabályozási mechanizmusaiba, és ezeket biztonsági szempontból felügyelni.
2. A szervezetnek ki kell választania és telepítenie kell a megfelelő behatolásellenőrző berendezéseket, amelyek képesek észlelni és jelenteni a potenciális biztonsági fenyegetéseket.
3. A szervezetnek be kell állítania és konfigurálnia kell az automatizált eszközöket és mechanizmusokat, hogy megfelelő védelmet nyújtsanak az EIR folyamatainak támadásai ellen.
4. A szervezetnek tesztelnie kell az integrált rendszert, hogy biztosítsa annak hatékonyságát és megbízhatóságát a behatolások észlelésében és kezelésében.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-4(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.17. AZ EIR MONITOROZÁSA – BEJÖVŐ ÉS KIMENŐ KOMMUNIKÁCIÓS FORGALOM

18.17. A szervezet:

18.17.1. A bejövő és kimenő kommunikációs forgalomra vonatkozóan kritériumokat állít fel a szokatlan vagy nem engedélyezett tevékenységek és körülmények azonosítására.

18.17.2. Meghatározott időközönként ellenőrzi a bejövő és kimenő kommunikációs forgalmat a szokatlan vagy jogosulatlan tevékenységek vagy körülmények tekintetében.

MAGYARÁZAT

Az érintett szervezet automatizált módon figyeli a bejövő és kimenő kommunikációs forgalmat az olyan mintázatok felismerése érdekében, melyek szokatlan, jogosulatlan tevékenységre utalnak a hálózaton.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először kritériumokat kell felállítania a bejövő és kimenő kommunikációs forgalom szokatlan vagy nem engedélyezett tevékenységeinek és körülményeinek azonosítására. Ez magában foglalhatja a belső forgalmat, amely jelzi a rosszindulatú kód jelenlétét vagy a legitim kód vagy hitelesítő adatok jogosulatlan használatát az EIR-en belül, vagy a rendszerelemek között terjedő jeleket, a külső rendszerekhez történő jelzéseket, és az információ jogosulatlan exportját.
2. Miután a kritériumokat felállították, a szervezetnek rendszeresen ellenőriznie kell a bejövő és kimenő kommunikációs forgalmat a szokatlan vagy jogosulatlan tevékenységek és körülmények tekintetében. Ez magában foglalhatja a naplók ellenőrzését és elemzését, hogy azonosítsák a potenciálisan kompromittált rendszereket vagy rendszer elemeket.
3. A szervezetnek továbbá biztosítania kell, hogy a kritériumok és az ellenőrzési folyamatok naprakészek és hatékonyak maradjanak a változó kiberbiztonsági fenyegetésekkel szemben. Ez magában foglalhatja a kritériumok és az ellenőrzési folyamatok rendszeres felülvizsgálatát és frissítését.
4. Végül, de nem utolsósorban, a szervezetnek megfelelő intézkedéseket kell tennie a szokatlan vagy jogosulatlan tevékenységek és körülmények kezelésére, amikor azokat azonosítják. Ez

magában foglalhatja a potenciálisan kompromittált EIR-ek vagy rendszerelemek izolálását, a rosszindulatú kód eltávolítását, és a jogosulatlan hozzáférés megakadályozását.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.3.11.5. Az elektronikus információs rendszer felügyelete

ISO/IEC 27001:2023 referencia

A.8.16

NIST SP 800-53 rev.5 referencia

SI-4(4)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

18.18. AZ EIR MONITOROZÁSA – RENDSZER ÁLTAL GENERÁLT RIASZTÁSOK

18.18. Az EIR riasztást küld a meghatározott személyeknek vagy szerepköröknek, amikor a rendszer által generált meghatározott indikátorok a rendszer potenciális kompromittálódására utaló jeleket mutatnak.

MAGYARÁZAT

Az információs rendszer figyelmezteti a szervezet által meghatározott személyeket vagy szerepköröket, ha a szervezet által meghatározott kompromittálásra utaló jelek észlelhetőek.
A riasztások több forrásból is előállhatnak, beleértve például a kártékony kód elleni védelmi mechanizmusokat, behatolásérzékelő vagy megelőző mechanizmusokat, vagy határvédelmi eszközöket, például tűzfalak, átjárók és routerek. A figyelmeztetéseket telefonon, elektronikus levélben vagy rövid szöveges üzenetek formájában is lehet továbbítani. Az értesítési listán szereplő szervezeti személyek lehetnek például rendszergazdák, egyéb rendszer felelősök vagy az információs rendszer biztonsági tisztviselői.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia azokat a személyeket vagy szerepköröket, akiknek riasztást kell küldeni, amikor az EIR potenciális kompromittálódásra utaló jeleket mutat. Ez magában foglalhatja az EIR adminisztrátorokat, rendszer felelősöket, üzleti tulajdonosokat, információs felelősöket, a szervezet felső szintű információbiztonsági tisztviselőit, adatvédelmi tisztviselőket vagy biztonsági tisztviselőket.
2. A szervezetnek be kell állítania az EIR-ben azokat az indikátorokat, amelyek a potenciális kompromittálódást jelezni tudják. Ezek az indikátorok származhatnak különböző forrásokból, beleértve a napló rekordokat, a rosszindulatú kód védelmi mechanizmusokból, az behatolás észlelési vagy megelőzési mechanizmusokból, vagy határvédelmi eszközökből, mint például tűzfalak, átjárók és routerek.
3. A szervezetnek be kell állítania az EIR-ben a riasztások automatikus generálását, amelyeket telefonon, elektronikus levélben vagy szöveges üzenetben lehet továbbítani.

4. A szervezetnek figyelemmel kell kísérnie az EIR által generált riasztásokat, és összpontosítania kell az EIR-en kívüli információforrásokra is, mint például a gyanús tevékenységekről szóló jelentések és a potenciális belső fenyegetésekről szóló jelentések.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.5. Naplózás tárkapacitása

4.7. Naplózási hiba kezelése

12.17. A fizikai hozzáférések felügyelete

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

3.3.11.5. Az elektronikus információs rendszer felügyelete

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-4(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök illetve a rendszer potenciális kompromittálódására vonatkozó indikátorok meghatározása

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

18.19. AZ EIR MONITOROZÁSA – AUTOMATIKUS VÁLASZ GYANÚS ESEMÉNYEKRE

18.19. A szervezet:

18.19.1. tájékoztatja a felmerült gyanús eseményekről a biztonsági események kijelölt kezelőit, akiket névvel vagy munkakörükkel azonosítanak; és

18.19.2. előre meghatározott és a rendszer működését csak minimálisan befolyásoló intézkedéseket hajt végre a gyanús események megszüntetése érdekében.

MAGYARÁZAT

Az érintett szervezetnek kötelessége tájékoztatni a biztonsági események kijelölt kezelőit minden felmerült gyanús eseményről. Ez azt jelenti, hogy ha bármilyen szokatlan, gyanús tevékenységet észlelnek az EIR-ben, akkor azonnal értesíteniük kell a felelős személyeket vagy csoportokat, akiket névvel vagy munkakörükkel azonosítanak. Ez lehet egy biztonsági csapat, egy IT menedzser, vagy bármely más személy vagy csoport, aki a szervezetben a biztonsági események kezeléséért felelős.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell azonosítania és kijelölnie azokat a személyeket, akik felelősek lesznek a biztonsági események kezeléséért. Ezeket a személyeket névvel vagy munkakörükkel kell azonosítani.
2. A szervezetnek be kell vezetnie egy protokollt, amely szerint a gyanús eseményekről tájékoztatást kell adni a kijelölt kezelőknek. Ez a tájékoztatás lehet azonnali vagy rendszeres időközönként történő jelentés formájában.
3. A szervezetnek előre meg kell határoznia azokat az intézkedéseket, amelyeket a gyanús események megszüntetése érdekében hajtanak végre. Ezeknek az intézkedéseknek minimálisan kell befolyásolniuk az EIR működését.
4. A szervezetnek biztosítania kell, hogy a kijelölt kezelők képesek legyenek gyorsan és hatékonyan reagálni a gyanús eseményekre, és megfelelően alkalmazzák az előre meghatározott intézkedéseket.

5. A szervezetnek naplót kell vezetnie a gyanús eseményekről és a hozzájuk kapcsolódó intézkedésekről. Ez a napló segíthet a jövőbeni események kezelésében, és bizonyítékul szolgálhat a kiberbiztonsági követelményeknek való megfelelésről.
6. Végül, de nem utolsósorban, a szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a gyanús események kezelésére vonatkozó protokolljait és intézkedéseit, hogy biztosítsa azok hatékonyságát és relevanciáját.

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

SI-4(7)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

18.20. AZ EIR MONITOROZÁSA – A FELÜGYELETI ESZKÖZÖK ÉS MECHANIZMUSOK TESZTELÉSE

18.20. A szervezet meghatározott gyakorisággal teszteli a behatolásfelügyeleti eszközöket és mechanizmusokat.

MAGYARÁZAT

A behatolásfigyelő (IDS) eszközök és mechanizmusok tesztelése szükséges annak biztosításához, hogy az eszközök és mechanizmusok megfelelően működnek, és továbbra is megfelelnek a szervezetek felügyeleti céljainak. A tesztelés gyakorisága és alaposssága a szervezetek által használt eszközök és mechanizmusok típusától és a telepítési módszereitől függ.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek leltárba kell vennie a behatolásfelügyeleti eszközöket és mechanizmusokat.
2. A szervezetnek ki kell választania a megfelelő tesztelési módszereket és eszközöket, amelyek segítségével ellenőrizheti a behatolásfelügyeleti eszközök és mechanizmusok működését.
3. A szervezetnek meg kell határoznia a behatolásfelügyeleti eszközök és mechanizmusok tesztelésének gyakoriságát. Ez a gyakoriság függ a használt eszközök és mechanizmusok típusától, valamint a telepítési módszerektől.
4. A szervezetnek rendszeresen el kell végeznie a teszteket a szervezet által meghatározott gyakorisággal. A tesztelés során a szervezetnek ellenőriznie kell, hogy az EIR-ben használt behatolásfelügyeleti eszközök és mechanizmusok megfelelően működnek-e, és továbbra is kielégítik-e a felügyeleti célokat.

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

SI-4(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.21. AZ EIR MONITOROZÁSA – AZ TITKOSÍTOTT KOMMUNIKÁCIÓ LÁTHATÓSÁGA

18.21. A szervezet intézkedéseket tesz arra, hogy a meghatározott titkosított kommunikációs forgalom átlátható legyen a meghatározott rendszerfelügyeleti eszközök és mechanizmusok számára.

MAGYARÁZAT

Az érintett szervezetek egyensúlyt teremtenek a kommunikációs forgalom titkosításának szükségessége és a forgalom monitorozásának szempontjából szükséges átláthatóság között. A szervezetek meghatározzák, hogy az átláthatósági követelmény alkalmazandó-e a belső titkosított adatforgalomra, a külső célpontok felé irányuló titkosított adatforgalomra, vagy ezek valamely részhalmazára.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, hogy mely titkosított kommunikációs forgalmakat szükséges átláthatóvá tenni a felügyeleti eszközök és mechanizmusok számára. Ez lehet belső titkosított forgalom, külső célpontokra irányuló titkosított forgalom, vagy ezeknek egy részhalmaza.
2. A szervezetnek ki kell dolgoznia egy stratégiát, amely lehetővé teszi a titkosított kommunikációs forgalom monitorozását az üzleti célok keretei között anélkül, hogy veszélyeztetné az adatok bizalmas jellegét. Ez magában foglalhatja a titkosítási kulcsok kezelését, a titkosított csatornák felügyeletét, és a titkosított adatok teljes, vagy részleges dekódolását a naplózás céljából.
3. A szervezetnek implementálnia kell a kiválasztott stratégiát, beleértve a szükséges hardver és szoftver beállításait, valamint a személyzet képzését a titkosított kommunikációs forgalom kezelésére és monitorozására.

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

SI-4(10)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a titkosított kommunikációs forgalom illetve a rendszerfelügyeleti eszközök és mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

18.22. AZ EIR MONITOROZÁSA – KOMMUNIKÁCIÓS FORGALOM ELTÉRÉSEINEK ELEMZÉSE

18.22. A szervezet elemzi a kimenő kommunikációs adatforgalmat a rendszer külső csatlakozási pontjain és a rendszer kijelölt belső pontjain, hogy felfedezze a rendellenességeket.

MAGYARÁZAT

Az érintett szervezet elemzi a kimenő kommunikációs adatforgalmat a rendszer külső csatlakozási pontjain és a szervezet által meghatározott belső pontokon, melyek magukban foglalhatják az alhálózatokat és az alrendszereket. A szervezet rendszerelemeiben található rendellenességek közé tartoznak a nagyméretű fájlátvitellel járó műveletek, a hosszú ideig fennmaradó hálózati kapcsolatok, a váratlan helyekről történő információhoz való hozzáférési kísérletek, a szokatlan protokollok és portok használata, a nem monitorozott hálózati protokollok használata, valamint a gyanús külső címekkel történő kommunikációs kísérletek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a rendszer külső csatlakozási pontjait valamint az EIR belső pontjait, melyek magukban foglalhatják az alhálózatokat és az alrendszereket.
2. A szervezetnek stratégiát kell terveznie, melynek segítségével hatékonyan képes megfigyelni a rendellenességeket a kimenő forgalomban.
3. A szervezetnek implementálnia kell a kiválasztott stratégiát, beleértve a szükséges hardver és szoftver beállításait.
4. A szervezetnek figyelnie kell a rendellenességekre és észlelés esetén szükségszerűen elvégezni a meghatározott intézkedéseket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-4(11)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a belső rendszerpontok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.23. AZ EIR MONITOROZÁSA – AUTOMATIKUSAN GENERÁLT SZERVEZETI RIASZTÁSOK

18.23. A rendszer a meghatározott automatizált mechanizmusok használatával riasztást küld a kijelölt személyeknek vagy munkaköröknek, ha olyan meghatározott, nem megfelelő vagy szokatlan tevékenységek történnek, amelyek biztonsági következményekkel járó tevékenységekre utalnak.

MAGYARÁZAT

Az EIR riasztásokkal kapcsolatos értesítési listáján szereplő személyek közé tartoznak a rendszergazdák, a küldetés- vagy üzleti felelősök, az EIR felelősök, a legfelsőbb szintű információbiztonsági tisztviselő, a legfelsőbb szintű adatvédelmi tisztviselő, az EIR biztonsági tisztviselők vagy adatvédelmi tisztviselők. Az automatizáltan generált riasztások azok a biztonsági riasztások, amelyeket az érintett szervezet generál és automatizált eszközökkel továbbít. A szervezet által generált riasztások forrásai olyan elemekre összpontosítanak, mint például a gyanús tevékenységek és a belső fenyegetések.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy riasztási értesítési listát, amely tartalmazza az EIR adminisztrátorokat, a misszió vagy üzleti felelősöket, az EIR tulajdonosokat, a legfelsőbb szintű információbiztonsági tisztviselőt, a legfelsőbb szintű adatvédelmi tisztviselőt, az EIR biztonsági tisztviselőket és az adatvédelmi tisztviselőket.
2. A szervezetnek automatizált riasztásokat kell generálnia, amelyeket automatizált eszközökkel továbbít.
3. A szervezet által generált riasztások forrásai más entitásokra összpontosítanak, mint például a gyanús tevékenységekről szóló jelentések és a belső fenyegetésekre vonatkozó potenciális jelentések.
4. A szabályozásban meghatározott EIR által generált riasztások az EIR-en belüli információforrásokra összpontosítanak, mint például a napló rekordok.

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

SI-4(12)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök illetve az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

18.24. AZ EIR MONITOROZÁSA – FORGALMI ÉS ESEMÉNYMINTÁK ELEMZÉSE

18.24. A szervezet:

18.24.1. elemzi a rendszer kommunikációs forgalmát és az eseménymintákat;

18.24.2. a jellemző forgalmi és eseménymintákat megjelenítő profilokat dolgoz ki; és

18.24.3. ezeket a forgalmi és eseményprofilokat használja fel a rendszerfelügyeleti eszközök hangolásához.

MAGYARÁZAT

A gyakori kommunikációs forgalmi és eseményminták azonosítása segíthet a rendszerfelügyeleti eszközöknek hatékonyabban azonosítani a gyanús vagy szokatlan forgalmat és eseményeket. Az ilyen információk segíthetnek csökkenteni a hamis pozitív és hamis negatív eredmények számát a felügyelet során.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek eseménymintákat kell készítenie a jellemző forgalmi és eseménymintákról. Ezek az eseményminták segítenek elkülöníteni a normális és a gyanús tevékenységeket a rendszeren belül.

2. A szervezetnek el kell végeznie a rendszerfelügyeleti eszközök beállítását a jellemző és rendellenes eseményminták alapján, úgy, hogy az események azonosítása és kezelése hatékony legyen.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.16

NIST SP 800-53 REV.5 REFERENCIA

SI-4(13)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.25. AZ EIR MONITOROZÁSA – VEZETÉK NÉLKÜLI BEHATOLÁST ÉRZÉKELŐ RENDSZER

18.25. A szervezet egy vezeték nélküli behatolást érzékelő rendszert használ, amely képes felismerni a nem engedélyezett vezeték nélküli eszközöket, valamint észlelni a támadási kísérleteket és a rendszer potenciális kompromittálását vagy sérülését.

MAGYARÁZAT

A vezeték nélküli jelek túlsugározhatnak a szervezeti létesítmények határain. A szervezetek proaktívan keresik az illetéktelen vezeték nélküli kapcsolatokat, beleértve az illetéktelen vezeték nélküli hozzáférési pontok alapos vizsgálatát. A vezeték nélküli átvizsgálások nem korlátozódnak a rendszereket tartalmazó létesítményeken belüli területekre, hanem a létesítményeken kívüli területekre is kiterjednek annak ellenőrzése érdekében, hogy az illetéktelen vezeték nélküli hozzáférési pontok nem kapcsolódnak-e a szervezeti rendszerekhez.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a szervezeti létesítmények határait, hogy tisztább képpel tudja megtervezni a vezeték nélküli behatolásérzékelő rendszerek képességeit.
2. A szervezetnek biztosítania kell, hogy a rendszer megfigyelésére használt vezeték nélküli behatolásérzékelő rendszer megfelelően működik és képes felismerni a nem engedélyezett vezeték nélküli eszközöket a szervezeti létesítmények határain belül és kívül is.
3. A szervezetnek proaktívan kell keresnie az engedély nélküli vezeték nélküli kapcsolatokat a létesítmények határain belül és kívül is.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.108. Vezeték nélküli hozzáférés

8.10. Eszközök azonosítása és hitelesítése

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

SI-4(14)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

18.26. AZ EIR MONITOROZÁSA – VEZETÉK NÉLKÜLI ÉS VEZETÉKES KOMMUNIKÁCIÓ

18.26. A szervezet egy behatolásérzékelő rendszert alkalmaz a vezeték nélküli kommunikációs forgalom megfigyelésére, amint az áthalad a vezeték nélküli hálózatból a vezetékes hálózatba.

MAGYARÁZAT

A vezeték nélküli hálózatok eredendően kevésbé biztonságosak, mint a vezetékes hálózatok. A vezeték nélküli hálózatok például érzékenyebbek a lehallgatásra vagy a forgalomelemzésre, mint a vezetékes hálózatok. Ha párhuzamosan vezeték nélküli és vezetékes kommunikáció is használatban van, a vezeték nélküli hálózat a vezetékes hálózatba való bejutás bejáratává válhat. Tekintettel arra, hogy a vezeték nélküli hozzáférési pontokon keresztül történő jogosulatlan hálózati hozzáférés lehetősége nagyobb, mint a rendszer fizikai határain belülről történő jogosulatlan vezetékes hálózati hozzáférésé, a vezeték nélküli és vezetékes hálózatok közötti átmenő forgalom további megfigyelésére lehet szükség a rosszindulatú tevékenységek felderítéséhez. A behatolásjelző rendszerek (IDS) alkalmazása segít annak biztosításában, hogy a forgalom ne tartalmazzon rosszindulatú kódot a vezetékes hálózatra való átmenet előtt.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell a vezetéknélküli és vezetékes hálózatok közötti hálózathatárokat, mely pontokon az áthaladó forgalom megfigyelése szükséges.
2. A szervezetnek be kell szereznie egy behatolásérzékelő rendszert (IDS), mely képes a vezeték nélküli hálózatból a vezetékes hálózatba átmenő forgalom megfigyelésére.
3. A szervezetnek konfigurálnia kell a behatolásérzékelő rendszert, hogy észlelje a potenciálisan káros tevékenységeket, például a nem engedélyezett hozzáférést, a gyanús forgalmi mintákat és a potenciálisan káros kódokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.108. Vezeték nélküli hozzáférés

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

SI-4(15)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.27. AZ EIR MONITOROZÁSA – FELÜGYELETI INFORMÁCIÓK ÖSSZEHANGOLÁSA

18.27. A szervezet összekapcsolja a rendszerben alkalmazott felügyeleti eszközökből és mechanizmusokból származó információkat.

MAGYARÁZAT

A különböző rendszerfelügyeleti eszközökből és mechanizmusokból származó információk korrelálása átfogóbb képet adhat a rendszertevékenységről. A rendszerfelügyeleti eszközök és mechanizmusok - köztük a rosszindulatú kódok elleni védelmi szoftverek, a hosztok és a hálózatok felügyelete - korrelációja a szervezet egészére kiterjedő felügyeleti áttekintést biztosíthat, és egyébként nem látható támadási mintákat tárhat fel. A különféle felügyeleti eszközök és mechanizmusok képességeinek és korlátainak megértése, valamint az ezen eszközök és mechanizmusok által generált információk maximális kihasználása segíthet a szervezeteknek hatékony felügyeleti programok kidolgozásában, működtetésében és fenntartásában. A felügyeleti információk korrelációja különösen fontos a régebbi technológiákról az újabbakra való áttérés során.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell értenie a különböző felügyeleti eszközök és mechanizmusok képességeit és korlátait, valamint azt, hogyan lehet maximalizálni az általuk generált információk használatát.
2. A szervezetnek össze kell kapcsolnia azokat a felügyeleti eszközöket és mechanizmusokat, amelyek általában izoláltan működnek - beleértve a kártékony kódok elleni védelmi szoftvereket, valamint a hosztok és a hálózatok felügyeletére alkalmas eszközöket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.16

NIST SP 800-53 REV.5 REFERENCIA

SI-4(16)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.28. AZ EIR MONITOROZÁSA – INTEGRÁLT HELYZETFELISMERÉS

18.28. A szervezet összekapcsolja a fizikai, ellátási lánc és kiberbiztonsági tevékenységek megfigyelése során gyűjtött információkat az integrált, a teljes szervezetre kiterjedő átfogóbb helyzetfelismerés érdekében.

MAGYARÁZAT

A több különböző forrásból származó megfigyelési információk korrelálása segít az integrált helyzetfelismerés elérésében. A fizikai, kiber- és ellátási láncot figyelő tevékenységek kombinációjából származó integrált helyzetfelismerés növeli a szervezetek képességét a kifinomult támadások gyorsabb felderítésére és az ilyen támadások végrehajtásához alkalmazott módszerek és technikák vizsgálatára. A több tevékenységből származó megfigyelési információk összekapcsolása segíthet feltárni azokat a támadásokat, amelyek az érintett szervezetek ellen több támadási vektoron keresztül indítanak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és összegyűjtenie a fizikai, ellátási lánc és kiberbiztonsági tevékenységek során keletkező megfigyelési információkat. Ez magában foglalhatja a hálózati forgalom, a rendszerek állapota, a felhasználói tevékenység, az események és a biztonsági események naplózását.
2. A szervezetnek ezután össze kell kapcsolnia a több forrásból származó információkat egy központosított rendszerben, mely így átfogó képet adhat a különböző tevékenységekből származó események összességéről.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.51. Szervezeten átívelő naplózás

12.17. A fizikai hozzáférések felügyelete

19.2. Ellátási láncra vonatkozó kockázatkezelési szabályzat

19.8. Rendszerelemek és kapcsolódó adatok eredetisége

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

SI-4(17)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.29. AZ EIR MONITOROZÁSA – KIMENŐ FORGALOM ELEMZÉSE

18.29. A szervezet elemzi a kimenő kommunikációs forgalmat a rendszer külső interfészeinél, valamint a meghatározott belső rendszerpontokon, hogy észlelje az információ rejtett kiszivárogtatását.

MAGYARÁZAT

A szervezet által meghatározott belső pontok közé tartoznak az alhálózatok és alrendszerek. Az információk kiszivárgására használható rejtett eszközök közé tartozik a steganográfia.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia azokat a belső pontokat és külső interfészeket, ahol a kommunikációs forgalmat elemezni kívánja.
2. A szervezetnek meg kell határoznia az információ kiszivárogtatására használható eszközöket és mechanizmusokat, melyeket a megfigyelés során a rendszernek meg kell találnia.
3. A szervezetnek implementálnia kell egy rendszert, amely a meghatározott szempontok alapján képes analizálni a kimenő kommunikációs forgalmat a fontos belső pontokon és a külső interfészeken.

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

SI-4(18)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a belső rendszerpontok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.30. AZ EIR MONITOROZÁSA – AZ EGYÉNEK KOCKÁZATÁNAK FELÜGYELETE

18.30. A szervezet meghatározott kiegészítő felügyeletet alkalmaz azokra az egyénekre, akiket a meghatározott források alapján nagyobb kockázatot jelentő személyekként azonosítottak.

MAGYARÁZAT

Az egyének által jelentett fokozott kockázatra utaló jelek különböző forrásokból, többek között személyzeti nyilvántartásokból, hírszerző ügynökségekből, bűnüldöző szervezetekből és egyéb forrásokból szerezhetők be. Az egyének megfigyelését az ilyen megfigyelést végző vezetői, jogi, biztonsági, adatvédelmi és humánerőforrás-tisztviselőkkel koordinálják. A megfigyelést az alkalmazandó törvényekkel, végrehajtási utasításokkal, irányelvekkel, szabályzatokkal, szabályokkal, szabványokkal és iránymutatásokkal összhangban végzik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először azonosítania kell azokat az egyéneket, akik fokozott kockázatot jelentenek.
2. A szervezetnek meg kell terveznie a fokozott kockázatot jelentő személyek felügyeletét lehetővé tevő stratégiát a menedzsmenttel, jogi, biztonsági, adatvédelmi és humán erőforrásokkal foglalkozó tisztségviselőkkel együttműködve a mindenkori törvényeknek, végrehajtási rendeleteknek, irányelveknek, szabályzatoknak, szabályoknak, szabványoknak és útmutatóknak megfelelően.
3. A szervezetnek szükség esetén alkalmaznia kell a fokozott kockázatot jelentő személyek felügyeletére vonatkozó stratégiákat.

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

SI-4(19)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kiegészítő felügyelet illetve a források meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.31. AZ EIR MONITOROZÁSA – PRIVILEGIZÁLT FELHASZNÁLÓK

18.31. A szervezet meghatározott kiegészítő felügyeletet alkalmaz a privilegizált felhasználók esetében.

MAGYARÁZAT

A privilegizált felhasználók több bizalmas információhoz férnek hozzá - beleértve a biztonsággal kapcsolatos információkat is - mint az általános felhasználók. Az ilyen információkhoz való hozzáférés azt jelenti, hogy a privilegizált felhasználók potenciálisan nagyobb kárt okozhatnak a rendszerekben és a szervezetekben, mint a nem privilegizált felhasználók. Ezért a privilegizált felhasználók további felügyeletének bevezetése segít annak biztosításában, hogy a szervezetek a lehető legkorábban azonosítani tudják a rosszindulatú tevékenységet, és megfelelő intézkedéseket hozhassanak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell, kik minősülnek privilegizált felhasználóknak az EIR-ben.
2. Az érintett rendszernek meg kell határoznia bizonyos kiegészítő felügyeleti intézkedéseket, melyeket a megfigyelés során a privilegizált felhasználókra szükséges érvényesíteni.
3. A szervezetnek alkalmaznia kell a privilegizált felhasználók megfigyelésre meghatározott kiegészítő intézkedéseket a létező megfigyelési intézkedések mellé.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.108. Vezeték nélküli hozzáférés

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

SI-4(20)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kiegészítő felügyelet meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

18.32. AZ EIR MONITOROZÁSA – PRÓBAIDŐSZAKOK

18.32. A szervezet meghatározott kiegészítő felügyeletet alkalmaz az egyénekkel szemben a szervezet által meghatározott próbaidőszakuk alatt.

MAGYARÁZAT

A próbaidő alatt a munkavállalók nem rendelkeznek állandó munkaviszonnyal a szervezeten belül. Ezen státusz vagy a rendszeren tárolt információhoz való hozzáférés nélkül további monitorozás segíthet a potenciálisan rosszindulatú tevékenységek vagy a nem megfelelő viselkedés azonosításában.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek leltárat kell készíteni a mindenkori próbaidős státuszban lévő alkalmazottakról, melyet rendszeresen frissíteni kell a munkaviszony változásainak fényében.
2. Az érintett rendszernek meg kell határoznia bizonyos kiegészítő felügyeleti intézkedéseket, melyeket a próbaidős státuszú felhasználókra szükséges érvényesíteni.
3. A szervezetnek alkalmaznia kell a próbaidős státuszú felhasználók megfigyelésre meghatározott kiegészítő intézkedéseket a létező megfigyelési intézkedések mellé.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.108. Vezeték nélküli hozzáférés

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

SI-4(21)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a próbaidőszak illetve a kiegészítő felügyelet meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.33. AZ EIR MONITOROZÁSA – ENGEDÉLY NÉLKÜLI HÁLÓZATI SZOLGÁLTATÁSOK

18.33. A szervezet:

18.33.1. észleli azokat a hálózati szolgáltatásokat, amelyeket a szervezet által meghatározott engedélyezési és jóváhagyási folyamatok alapján nem engedélyeztek vagy nem hagytak jóvá; és

18.33.2. naplózza a nem engedélyezett hálózati szolgáltatások észlelését, és egyben riasztást küld a szervezet által kijelölt személyeknek vagy szerepköröknek, annak észlelésekor.

MAGYARÁZAT

Az engedély nélküli vagy jóváhagyás nélküli hálózati szolgáltatások közé tartoznak a szolgáltatásorientált architektúrákban található olyan szolgáltatások, amelyek nem rendelkeznek szervezeti ellenőrzéssel vagy érvényesítéssel, és ezért megbízhatatlanok lehetnek, vagy rosszindulatú csalóként szolgálhatnak az érvényes szolgáltatások számára.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia kell azokat a hálózati szolgáltatásokat, amelyeket engedélyeznek és jóváhagynak a működéshez.
2. A szervezetnek alkalmaznia kell olyan rendszerelemeket, amelyek képesek észlelni és azonosítani azokat a hálózati szolgáltatásokat, amelyek nem felelnek meg az előzőleg meghatározott engedélyezési és jóváhagyási folyamatoknak.
3. A szervezetnek be kell állítania a naplózási funkciót a fentebb említett rendszerelemben, hogy naplózza a nem engedélyezett hálózati szolgáltatások észlelését.
4. A szervezetnek be kell állítania a riasztási funkciót a fentebb említett rendszerelembe, hogy riasztást küldjön a szervezet által kijelölt személyeknek vagy szerepköröknek, amikor a nem engedélyezett hálózati szolgáltatások jelenlétét észlelik.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.26. Legszűkebb funkcionalitás

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

SI-4(22)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

18.34. AZ EIR MONITOROZÁSA – HOSZTALAPÚ ESZKÖZÖK

18.34. A szervezet meghatározott hosztalapú felügyeleti mechanizmusokat alkalmaz a szervezet által meghatározott rendszerelemeken.

MAGYARÁZAT

A hoszt-alapú felügyelet a hosztról gyűjt információkat. A rendszerelemek, amelyekben az állomás-alapú felügyelet megvalósítható, a szerverek, számítógépek és mobil eszközök közé tartoznak. A szervezetek fontolóra vehetik több termékfejlesztő vagy gyártó hoszt-alapú felügyeleti mechanizmusainak alkalmazását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely rendszerelemeket kívánja felügyelni. Ezek lehetnek szerverek, számítógépek, notebookok, mobil eszközök stb.
2. A szervezetnek ki kell választania a megfelelő hoszt-alapú felügyeleti mechanizmusokat. Ezek lehetnek különböző termékfejlesztők vagy szállítók által kínált megoldások.
3. A szervezetnek telepítenie kell a kiválasztott hoszt-alapú felügyeleti mechanizmusokat a meghatározott rendszerelemeken.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.108. Vezeték nélküli hozzáférés

2.113. Mobil eszközök hozzáférés-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

SI-4(23)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek, illetve az hosztalapú felügyeleti mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.35. AZ EIR MONITOROZÁSA – KOMPROMITTÁLÓDÁS JELEI

18.35. A szervezet felismeri, összegyűjti és a kijelölt személyeknek vagy szerepköröknek továbbítja a meghatározott forrásokból származó kompromittálódásra utaló jeleket.

MAGYARÁZAT

A kompromittálódásra utaló jelek (Indicators of compromise - IOC) a behatolásokból származó törvényszéki leletek, amelyeket a szervezeti rendszereken a hoszt vagy a hálózat szintjén azonosítanak. Az IOC-k értékes információkat szolgáltatnak a veszélyeztetett rendszerekről. Az IOC-k közé tartozhat a rendszerleíró kulcsok értékeinek létrehozása. A hálózati forgalomra vonatkozó IOC-k olyan egységes erőforrás-helymeghatározó (Uniform Resource Locator - URL) vagy protokollelemeket tartalmaznak, amelyek rosszindulatú kódot tartalmazó parancs- és vezérlőkiszolgálókra utalnak. Az IOC-k gyors terjesztése és elfogadása javíthatja az információbiztonságot azáltal, hogy csökkenti azt az időt, amíg a rendszerek és szervezetek sebezhetőek ugyanannak a sérülékenység kihasználásnak vagy támadásnak. A fenyegetésjelzők, aláírások, taktikák, technikák, eljárások és a kompromittáltság egyéb mutatói kormányzati és nem kormányzati együttműködéseken keresztül érhetők el, beleértve az Incidensreagáló és Biztonsági Csapatok Fórumát, az Egyesült Államok Számítógépes Vészhelyzeti Készenléti Csoportját, a Védelmi Ipari Bázis Kiberbiztonsági Információmegosztási Programját és a CERT Koordinációs Központot.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek össze kell gyűjtenie a kompromittálódásra utaló jeleket (Indicators of compromise - IOC) és egy könnyen kezelhető és frissen tartható nyilvántartásba kell őket vezetnie, hogy az releváns állapotban tartható legyen a későbbiekben.
2. A szervezetnek alkalmaznia kell eszközöket vagy mechanizmusokat, melyek képekesek összegyűjteni a kompromittálódásra utaló jeleket.
3. A szervezetnek alkalmaznia kell eszközöket vagy mechanizmusokat, melyek képesek továbbítani a kijelölt személyeknek vagy szerepköröknek a kompromittálódásra utaló jelekre utaló információkat.

Kapcsolódó intézkedések

2.108. Vezeték nélküli hozzáférés

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

SI-4(24)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök, illetve a források meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

18.36. AZ EIR MONITOROZÁSA – HÁLÓZATI FORGALOM ELEMZÉSÉNEK OPTIMALIZÁLÁSA

18.36. Az EIR biztosítja a hálózati forgalom átláthatóságát mind a külső, mind a szervezet működése szempontjából kritikus belső rendszerinterfészeken, a felügyeleti eszközök hatékonyságának optimalizálása érdekében.

MAGYARÁZAT

A titkosított forgalom, az aszimmetrikus útválasztási architektúrák, a kapacitás- és késleltetési korlátok, valamint a régebbi technológiákról az újabbakra való áttérés a szervezetek számára vakfoltokat eredményezhetnek a hálózati forgalom elemzése során. A adatok gyűjtése, dekódolása, előfeldolgozása és csak a releváns forgalom elküldése a felügyeleti eszközöknek elősegíti az eszközök hatékonyságát és használatát, valamint optimalizálja forgalom elemzését.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell és számon kell tartania mind a külső, mind a szervezet működése szempontjából kritikus belső rendszerinterfészeket, amelyeken az áthaladó forgalom átláthatóságát biztosítani kell.
2. A szervezetnek gyűjtenie, dekódolnia kell és előfeldolgozást kell végezni a releváns forgalmon és csak ezt a forgalmat továbbítania a felügyeleti eszközöknek. Ez segít optimalizálni a hálózati forgalom elemzését és javítja az eszközök hatékonyságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-4(25)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.37. BIZTONSÁGI RIASZTÁSOK ÉS TÁJÉKOZTATÁSOK

18.37. A szervezet:

18.37.1. Folyamatosan fogadja a meghatározott külső szervezetektől a biztonsági figyelmeztetéseket, tanácsokat és iránymutatásokat.

18.37.2. Szükség esetén belső biztonsági riasztásokat, tanácsokat és iránymutatásokat készít.

18.37.3. Biztonsági riasztásokat, tanácsokat és iránymutatásokat ad ki a meghatározott személyeknek vagy szerepkörökben dolgozóknak, a kijelölt szervezeti egységeknek és a kijelölt külső szervezeteknek.

18.37.4. A biztonsági iránymutatásokat az azokban foglaltak szerint alkalmazza.

MAGYARÁZAT

A Kormányzati Eseménykezelő Központ biztonsági riasztásokat tesz közzé és tanácsokat ad a helyzetismeret elősegítése érdekében. A biztonsági irányelveket a BM vagy más kijelölt szervezetek adják ki, amelyeknek felelőssége és hatásköre az ilyen irányelvek kiadása. Az irányelvek betartása elengedhetetlen, mivel sok esetben kritikus jelentőségűek, és ha nem hajtják végre időben, az az érintett szervezet működésére és eszközeire, az egyénekre, más szervezetekre és az egész nemzetre nézve is káros hatással lehet. A külső szervezetek közé tartoznak a beszállítói lánc partnerei, külső missziós vagy üzleti partnerek, külső szolgáltatók és más, egyenrangú vagy támogató szervezetek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy folyamatosan fogadja a meghatározott külső szervezetektől a biztonsági figyelmeztetéseket, tanácsokat és iránymutatásokat. Ez magában foglalhatja a kapcsolattartást hivatalos szervezetekkel, melyek ilyen jellegű információkat szolgáltatnak.

2. A szervezetnek alkalmaznia kell a biztonsági iránymutatásokat az azokban foglaltak szerint. Ez magában foglalhatja a biztonsági irányelvek és eljárások frissítését, valamint a biztonsági intézkedések végrehajtását és ellenőrzését az EIR-en.

Kapcsolódó intézkedések

1.16. Szakmai csoportokkal és közösségekkel való kapcsolattartás

15.10. Sérülékenységmonitorozás és szkennelés

18.2. Hibajavítás

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

3.3.11.6. Biztonsági riasztások és tájékoztatások

ISO/IEC 27001:2023 referencia

A.5.6; A.8.8

NIST SP 800-53 rev.5 referencia

SI-5

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

18.38. Biztonsági riasztások és tájékoztatások – Automatizált figyelmeztetések és tanácsok

18.38. A szervezet biztonsági riasztásokat és tanácsokat tesz közzé az egész szervezeten belül a meghatározott, automatizált mechanizmusok segítségével.

Magyarázat

Az érintett szervezet rendszereiben és működési környezetében bekövetkező jelentős számú változás szükségessé teszi a biztonsági információk széles körű terjesztését azoknak a szervezeti egységeknek, amelyek közvetlenül érdekeltek az érintett szervezet küldetésének és üzleti funkcióinak sikerében. A biztonsági riasztások és tanácsok által szolgáltatott információk alapján változásokra lehet szükség a kockázatkezelés három szintjéből egy vagy több szinten, beleértve a kormányzati szintet, a küldetési és üzleti folyamat szintjét, valamint az EIR szintjét.

A követelmény alkalmazásának lépései

1. A szervezetnek létre kell hoznia egy automatizált mechanizmust, amely képes a biztonsági figyelmeztetések és tanácsok közzétételére az egész szervezeten belül. Ez lehet egy belső hírlevél, e-mail rendszer, vagy akár egy dedikált biztonsági portál.
2. A szervezetnek rendszeresen frissítenie kell a biztonsági figyelmeztetéseket és tanácsokat, hogy a legújabb fenyegetésekre és kockázatokra hívja fel a figyelmet. Ez magában foglalhatja a legújabb vírusok, trójai programok, adathalász támadások és egyéb kiberbiztonsági fenyegetések ismertetését.
3. A szervezetnek ki kell dolgoznia egy stratégiát, amely segítségével alkalmazásra kerülnek a figyelmeztetések és tanácsok által azonosított kockázatok kezeléséhez szükséges hardveres és szoftveres rendszerek.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.3.11.6. Biztonsági riasztások és tájékoztatások

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-5(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

18.39. BIZTONSÁGI FUNKCIÓK ELLENŐRZÉSE

18.39. Az EIR:

18.39.1. Ellenőrzi a meghatározott biztonsági funkciók helyes működését.

18.39.2. Az előírt gyakorisággal a megfelelő jogosultsággal rendelkező felhasználók utasítására végrehajtja a meghatározott rendszerállapot-változásokat kezelő funkciók (például: indítás, újraindítás, leállítás) ellenőrzését.

18.39.3. Figyelmezteti a meghatározott személyeket vagy szerepköröket a fentiek sikertelensége esetén.

18.39.4. Amennyiben rendellenességeket észlel, leállítja vagy újraindítja a rendszert, illetve a szervezet által meghatározott alternatív intézkedéseket hajt végre

MAGYARÁZAT

Az információs rendszerek átmeneti állapotai közé tartozik például a rendszer indítása, újraindítása, leállítása és megszakítása. Az információs rendszerek által nyújtott értesítések közé tartoznak például a rendszergazdáknak szóló elektronikus figyelmeztetések, a helyi számítógépes konzolok üzenetei és/vagy a hardverjelzések, például a fények. Az információbiztonsági funkciók ellenőrzése a biztonsági funkciók ellenőrzésével szemben annak ellenőrzése, hogy az információbiztonsági funkciók a jóváhagyott módon működnek-e, vagy az információbiztonsági szempontok az elvártak alapján vannak alkalmazva.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a biztonsági funkciók helyes és elvárt működését.

2. A szervezetnek biztosítania kell, hogy az állapot-változásokat kezelő funkciók, mint például az indítás, újraindítás, leállítás rendszeresen ellenőrizve vannak.

3. Szükség esetén a szervezetnek figyelmeztetnie kell a meghatározott személyeket vagy szerepköröket, ha a fent említett ellenőrzések sikertelenek.

4. Amennyiben rendellenességeket észlel, leállítja vagy újraindítja a rendszert, illetve a szervezet által meghatározott alternatív intézkedéseket hajt végre.

KAPCSOLÓDÓ INTÉZKEDÉSEK

5.14. Folyamatos felügyelet

6.15. Biztonsági hatásvizsgálatok

6.23. Konfigurációs beállítások

18.42. Szoftver- és információsértetlenség

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

3.3.11.7. A biztonsági funkcionalitás ellenőrzése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

18.40. A BIZTONSÁGI FUNKCIÓK ELLENŐRZÉSE – AUTOMATIZÁLÁSI TÁMOGATÁS ELOSZTOTT TESZTELÉSHEZ

18.40. A szervezet automatizált mechanizmusokat alkalmaz a biztonsági funkciók elosztott tesztelésének támogatására.

MAGYARÁZAT

Az funkciók elosztott tesztelésének irányítását támogató automatizált mechanizmusok használata segít biztosítani a tesztelés integritását, időszerűségét, teljességét és hatékonyságát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a kiberbiztonsági funkciókat, amelyeket tesztelni kíván. Ezek a funkciók lehetnek például hálózati védelem, adatvédelem, vagy rendszerfelügyelet.
2. A szervezetnek ki kell választania vagy fejlesztenie kell automatizált mechanizmusokat, amelyek képesek támogatni a kiválasztott biztonsági funkciók elosztott tesztelését. Ezek a mechanizmusok lehetnek például szoftverek, eszközök vagy szolgáltatások, amelyek automatikusan elvégzik a tesztelési feladatokat.
3. A szervezetnek alkalmaznia kell ezeket az automatizált mechanizmusokat, melyeknek képesnek kell lenniük kommunikálni a különböző rendszerkomponensekkel és a tesztelési feladatok elvégzésére.

KAPCSOLÓDÓ INTÉZKEDÉSEK

18.2. Hibajavítás

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

SI-6(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.41. BIZTONSÁGI FUNKCIÓK ELLENŐRZÉSE – JELENTÉS AZ ELLENŐRZÉS EREDMÉNYÉRŐL

18.41. A szervezet jelentést készít a biztonsági funkciók ellenőrzésének eredményeiről a szervezet által meghatározott személyeknek vagy szerepköröknek.

MAGYARÁZAT

A biztonsági és adatvédelmi funkciók ellenőrzésének eredményeiben várhatóan érintett szervezeti személyek közé tartoznak a rendszerbiztonsági tisztviselők, az ügynökségek vezető információbiztonsági tisztviselői és az adatvédelmi tisztviselők.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely személyek vagy szerepkörök felelnek a biztonsági funkciók ellenőrzésének eredményeiért.
2. A szervezetnek rendszeresen ellenőriznie kell az EIR biztonsági funkcióit, hogy biztosítsa azok megfelelő működését.
3. A szervezetnek jelentést kell készítenie a biztonsági funkciók ellenőrzésének eredményeiről, beleértve az esetleges problémákat vagy anomáliákat, és javaslatokat tesz a problémák megoldására.
4. A szervezetnek el kell juttatnia az ellenőrzés eredményeiről készült jelentést a szervezet által meghatározott személyeknek vagy szerepköröknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

18.13. Az EIR monitorozása

19.8. Rendszerelemek és kapcsolódó adatok eredetisége

19.13. Beszerzési stratégiák, eszközök és módszerek

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

SI-6(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.42. SZOFTVER- ÉS INFORMÁCIÓSÉRTETLENSÉG

18.42. A szervezet:

18.42.1. sértetlenségellenőrző eszközöket alkalmaz, hogy észlelje a jogosulatlan változtatásokat a meghatározott szoftverekben, firmware-ekben és információkban; és

18.42.2. meghatározott intézkedéseket hajt végre, amikor engedély nélküli változásokat észlel a szoftverekben, firmware-ekben vagy az információkban.

MAGYARÁZAT

Jogosulatlan változtatások a szoftverekben, firmware-ekben vagy információkban keletkezhetnek hibából kifolyólag, vagy rosszindulatú tevékenység eredményeképpen. A szoftverek közé tartoznak például az operációs rendszerek (belső komponenseikkel, mint például a kernellel, illesztőprogramokkal együtt), a köztes szoftverek és az alkalmazások. A firmware interfészek közé tartozik az Egységes Kiterjeszthető Firmware Interfész (UEFI) és az Alapvető Bemeneti/Kimeneti Rendszer (BIOS). Az információk magukban foglalhatják a személyesen azonosítható információkat és a metaadatokat, amelyek tartalmazzák az információkhoz kapcsolódó biztonsági és adatvédelmi attribútumokat. Az érintett szervezet automatikusan ellenőrizheti a rendszerelemek integritását például paritás ellenőrzéssel, ciklikus redundancia ellenőrzésekkel, vagy kriptográfiai hash-ekkel és az ezekhez kapcsolódó eszközökkel.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek telepítenie és alkalmaznia kell a sértetlenségellenőrző eszközöket.

2. A szervezetnek be kell állítania a sértetlenségellenőrző eszközöket, hogy automatikusan monitorozzák a rendszerelemek sértetlenségét.

3. A szervezetnek meg kell határoznia és dokumentálnia kell azokat az intézkedéseket, amelyeket akkor hajtanak végre, amikor jogosulatlan változásokat észlelnek a megfigyelt rendszerelemeken.

4. A szervezetnek végre kell hajtania az előre meghatározott intézkedéseket amennyiben a sértetlenségellenőrző mechanizmusok jelzést generálnak.

Kapcsolódó intézkedések

2.28. Információáramlási szabályok érvényesítése

6.7. A konfigurációváltozások felügyelete (változáskezelés)

6.26. Legszűkebb funkcionalitás

6.36. Rendszerelem leltár

10.4. Karbantartási eszközök

10.11. Távoli karbantartás

15.10. Sérülékenységmonitorozás és szkennelés

16.16. Biztonságtervezési elvek

16.49. Külső elektronikus információs rendszerek szolgáltatásai

16.58. Fejlesztői változáskövetés

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

3.3.11.8. Szoftver- és információsértetlenség

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SI-7

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

18.43. SZOFTVER-, FIRMWARE- ÉS INFORMÁCIÓSÉRTETLENSÉG – SÉRTETLENSÉG ELLENŐRZÉSE

18.43. Az EIR meghatározott gyakorisággal sértetlenségellenőrzést végez a meghatározott szoftvereken, firmware-eken és információkon, a rendszer indításakor, az átmeneti rendszerállapotokban vagy a biztonsági szempontból releváns események esetén.

MAGYARÁZAT

A biztonsági szempontból releváns események közé tartozik például egy olyan új fenyegetés azonosítása, mely érinti a szervezet információs rendszereit, vagy egy új hardver, szoftver vagy firmware telepítése. Az átmeneti állapotok közé tartozik például a rendszer indítása, újraindítása, leállítása és megszakítása.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek leltárat kell készíteni szoftverekről, firmware-ekről és információkról, melyeken meghatározott gyakorisággal sértetlenségellenőrzést kell végeznie.
2. A szervezetnek meg kell határoznia a gyakoriságot, amellyel sértetlenségellenőrzést kell végezni a meghatározott szoftvereken, firmware-eken és információkon.
3. A szervezetnek a meghatározott gyakorisággal el kell végeznie a sértetlenségellenőrzést a meghatározott szoftvereken, firmware-eken és információkon.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.11.8. Szoftver- és információsértetlenség

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-7(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a szoftverek, firmware-ek és információk illetve az átmeneti állapotok vagy biztonsági szempontból releváns események meghatározása

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

18.44. SZOFTVER-, FIRMWARE- ÉS INFORMÁCIÓSÉRTETLENSÉG – AUTOMATIKUS ÉRTESÍTÉSEK AZ SÉRTETLENSÉG MEGSZŰNÉSÉRŐL

18.44. A szervezet olyan automatizált eszközöket alkalmaz, amelyek értesítik a kijelölt személyeket vagy szerepköröket, amennyiben a sértetlenségellenőrzés során eltéréseket észlelnek.

MAGYARÁZAT

Az automatizált eszközök használata a sértetlenség sérülésének jelzésére és a személyzet időben történő tájékoztatására a hatékony kockázatkezelés elengedhetetlen előfeltétele. A sértetlenség sérüléséről értesítést kaphatnak például a vállalkozás tulajdonosai és résztulajdonosai, az információs rendszerek gazdái, a rendszergazdák, a szoftverfejlesztők, a rendszerintegrátorok és az információbiztonsági tisztviselők.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell szereznie olyan automatizált eszközöket, melyek képesek arra, hogy a sértetlenségellenőrzés során talált eltérésekről értesítéseket küldjenek a kijelölt személyeknek.
2. A szervezetnek meg kell határoznia, hogy mely személyek vagy szerepkörök kapjanak értesítést a sértetlenségellenőrzés során talált eltérésekről.
3. A szervezetnek el kell végeznie a szükséges beállításokat, melyek által a rendszerek a kijelölt személyeknek vagy szerepköröknek értesítést küldenek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.11.8. Szoftver- és információsértetlenség

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-7(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

18.45. SZOFTVER-, FIRMWARE- ÉS INFORMÁCIÓSÉRTETLENSÉG – KÖZPONTILAG KEZELT SÉRTETLENSÉGELLENŐRZŐ ESZKÖZÖK

18.45. A szervezet központilag menedzselt sértetlenségellenőrző eszközöket használ.

MAGYARÁZAT

A központilag kezelt sértetlenségellenőrzési eszközök nagyobb következetességet biztosítanak az ilyen eszközök alkalmazása során, és elősegíthetik az sértetlenségellenőrzési tevékenységek átfogóbb lefedettségét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a sértetlenségellenőrző eszközök központi menedzsmentjére irányuló stratégiát. Ez a stratégia magába foglalhatja például az eszközök típusát, az eszközök által elvégzett intézkedéseket és azok szükségességének feltételeit, valamint az eszközökért felelős személyeket és szerepköröket.
2. A szervezetnek be kell állítania és konfigurálnia kell a stratégia által meghatározott eszközöket és szerepköröket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.3. Naplóbejegyzések tartalma
18.2. Hibajavítás
18.56. Kéretlen üzenetek elleni védelem

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

SI-7(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.46. SZOFTVER- ÉS INFORMÁCIÓSÉRTETLENSÉG – AUTOMATIKUS REAGÁLÁS

18.46. Az EIR automatikusan leáll, vagy újraindul, vagy végrehajtja a szervezet által meghatározott intézkedéseket, amennyiben a sértetlenségellenőrzés során rendellenességet észlel.

MAGYARÁZAT

Az információs rendszer automatikusan leállítja vagy újraindítja az információs rendszert és/vagy végrehajtja a szervezet által meghatározott intézkedéseket, amikor sértetlenségellenőrzés során rendellenességet észlel.

A szervezet különböző integritás-ellenőrzési és eltérési válaszokat határozhat meg:

az információ típusa (pl. firmware, szoftver, felhasználói adat) szerint;

(ii) meghatározott információk/kritériumok alapján; vagy

(iii) a kettő kombinációjaként.

A konkrét biztosítékok automatikus bevezetése a szervezeti információs rendszerekbe jelentheti például a változtatások visszaállítását, az információs rendszer megállítását vagy az ellenőrzési riasztások kiváltását, ha kritikus biztonsági fájlok jogosulatlan módosításaira derül fény.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a különböző sértetlenségellenőrzési válaszokat az információ típusa, a specifikus információ vagy mindkettő kombinációja alapján.

2. A szervezetnek be kell állítania a megfelelő intézkedések automatikus végrehajtását a sértetlenségellenőrzési jelzések alapján.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.11.8. Szoftver- és információsértetlenség

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-7(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

18.47. SZOFTVER- ÉS INFORMÁCIÓSÉRTETLENSÉG – KRIPTOGRÁFIAI VÉDELEM

18.47. Az EIR kriptográfiai mechanizmusokat alkalmaz a szoftverek, firmware-ek és az információk jogosulatlan módosításainak észlelésére.

MAGYARÁZAT

Az sértetlenség védelmére használt kriptográfiai mechanizmusok közé tartozik a digitális aláírás és az aszimmetrikus kriptográfiát alkalmazó aláírt hash értékek kiszámítása és alkalmazása, a hash generálásához használt kulcs titkosságának védelme, valamint a nyilvános kulcs használata a hash-információ ellenőrzésére. A kriptográfiai mechanizmusokat alkalmazó szervezetek a kriptográfiai kulcskezelési megoldásokat is figyelembe veszik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia a stratégiát, melyet a szoftverek, firmware-ek és az információk jogosulatlan módosításainak észlelésére tervez használni. Ez magában foglalja a szükséges kriptográfiai mechanizmusok kiválasztását, működésének megértését és biztonságos használatának megtervezését.
2. A szervezetnek alkalmaznia kell a választott kriptográfiai mechanizmusokat a szoftverek, firmware-ek és az információk jogosulatlan módosításainak észlelésére.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

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

SI-7(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.48. SZOFTVER- ÉS INFORMÁCIÓSÉRTETLENSÉG – ÉSZLELÉS ÉS A VÁLASZADÁS INTEGRÁLÁSA

18.48. A szervezet a rendszer biztonsága szempontjából releváns jogosulatlan változtatások észlelését integrálja a szervezet biztonsági eseményeket kezelő rendszerébe.

MAGYARÁZAT

Az észlelés és a válaszadás integrálása segít biztosítani, hogy az észlelt eseményeket nyomon kövessék, monitorozzák, korrigálják és elérhetők legyenek naplózási célokra. A naplózási adatok megőrzése fontos ahhoz, hogy hosszabb időszakon keresztül azonosítani és megkülönböztetni lehessen a kártékony tevékenységeket, valamint az esetleges jogi intézkedésekhez. A biztonsági szempontból releváns változások közé tartoznak a meghatározott konfigurációs beállítások jogosulatlan módosításai vagy a jogosultságok jogosulatlan megemelése.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell egy olyan biztonsági eseményeket kezelő rendszert, amely képes észlelni a jogosulatlan változtatásokat. Ilyen változtatások lehetnek például a konfigurációs beállítások jogosulatlan módosításai, vagy a rendszer jogosultsági szintjeinek engedély nélküli emelése.
2. A szervezetnek integrálnia kell a jogosulatlan változtatások észlelését a már létező, az EIR különböző eseményeinek naplózására alkalmas rendszerbe.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.2. Naplózható események

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

9.9.1. Biztonsági események kezelése

9.25. A biztonsági események nyomonkövetése

18.13. Az EIR monitorozása

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

SI-7(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszer biztonsága szempontjából releváns változtatások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

18.49. SZOFTVER- ÉS INFORMÁCIÓSÉRTETLENSÉG – NAPLÓZÁS ÉS RIASZTÁS

18.49. A sértetlenség potenciális sérülésének észlelésekor az EIR a következő lépéseket hajtja végre: esemény naplózása, riasztás küldése a felhasználóknak, meghatározott személyek vagy szerepkörök értesítése, további műveletek végrehajtása.

MAGYARÁZAT

A szervezetek a válaszintézkedéseket olyan szoftvertípusok, konkrét szoftverek vagy információk alapján választják ki, amelyek esetében az sértetlenség potenciális sérülése áll fenn.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a válaszintézkedéseket a potenciális sértetlenségi megsértések alapján, amelyek a szoftvertípusokra, specifikus szoftverekre vagy információkra vonatkoznak.
2. A szervezetnek össze kell állítania egy intézkedési stratégiát, mely alapján a rendszer sértetlenségi szabálysértést észlelve, naplózza az esemény időpontját, típusát, és a megsértett elemeket, riasztást küld az események kezelésében érintett felhasználóknak, majd elvégzi a további, a szervezet által meghatározott intézkedéseket.
3. A szervezetnek be kell állítania a rendszert, hogy kövesse a meghatározott stratégiát sértetlenségi szabálysértést észlelve.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.2. Naplózható események

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.40. Naplóbejegyzések létrehozása

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

SI-7(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek vagy szerepkörök illetve a más tevékenységek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.50. SZOFTVER-, FIRMWARE- ÉS INFORMÁCIÓSÉRTETLENSÉG – BOOT FOLYAMAT ELLENŐRZÉSE

18.50. Az EIR ellenőrzi a meghatározott rendszerelemek rendszerindítási folyamatának (boot) sértetlenségét.

MAGYARÁZAT

Az rendszerelemek rendszerindítási folyamatának sértetlenségének ellenőrzése kritikus a rendszerelemek megbízható, ismert állapotban történő indításához. A sértetlenség ellenőrző mechanizmusok biztosítják, hogy csak megbízható kód fut a rendszerindítási folyamatok során.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia azokat a rendszerelemeket, amelyek rendszerindítási folyamatát (boot) ellenőrizni szeretné sértetlenség szempontjából.
2. A szervezetnek implementálnia kell egy integritás-ellenőrző mechanizmust, amely biztosítja, hogy csak megbízható kód fut a rendszerindítási folyamat során.

KAPCSOLÓDÓ INTÉZKEDÉSEK

18.39. Biztonsági funkciók 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

SI-7(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.51. SZOFTVER-, FIRMWARE- ÉS INFORMÁCIÓSÉRTETLENSÉG – BOOT FIRMWARE VÉDELME

18.51. A szervezet meghatározott mechanizmusokat alkalmaz a rendszerindító (boot) firmware sértetlenségének védelme érdekében a meghatározott rendszerelemekben.

MAGYARÁZAT

A rendszerindító firmware jogosulatlan módosítása kifinomult, célzott támadásra utalhat. Az ilyen típusú célzott támadások tartós szolgáltatásmegtagadást vagy rosszindulatú kód tartós jelenlétét eredményezhetik. Ez akkor fordulhat elő, ha a firmware sérült, vagy ha a rosszindulatú kód be van ágyazva a firmware kódjába. Az rendszerelemek úgy védhetik a rendszerindító firmware integritását, hogy a firmware módosítások alkalmazása előtt ellenőrzik minden frissítés és a firmware integritását és hitelességét, és megakadályozzák, hogy a jogosulatlan folyamatok módosítsák a rendszerindító firmware-t.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia azokat a mechanizmusokat, amelyeket a rendszerindító (boot) firmware sértetlenségének védelmére alkalmazni fog. Ez magában foglalhatja például az összes firmware frissítés ellenőrzését, mielőtt azokat alkalmaznák.
2. A szervezetnek telepítenie és alkalmaznia kell azon mechanizmusokat, melyekkel a rendszerindító (boot) firmware sértetlensége biztosítható.

KAPCSOLÓDÓ INTÉZKEDÉSEK

18.39. Biztonsági funkciók 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

SI-7(10)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek illetve a mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.52. SZOFTVER-, FIRMWARE- ÉS INFORMÁCIÓSÉRTETLENSÉG – FELHASZNÁLÓ ÁLTAL TELEPÍTETT SZOFTVER

18.52. A szervezet megköveteli a sértetlenségellenőrzés elvégzését a meghatározott felhasználók által telepíthető szoftvereken a végrehajtás előtt.

MAGYARÁZAT

Az érintett szervezetek a végrehajtás előtt ellenőrzik a felhasználók által telepített szoftverek sértetlenségét, hogy csökkentsék a rosszindulatú kódok vagy a jogosulatlan módosításokból származó hibákat tartalmazó programok végrehajtásának valószínűségét. A szervezetek mérlegelik a szoftverek sértetlenségének ellenőrzésére irányuló megközelítések gyakorlatiasságát, beleértve a szoftverfejlesztők és szállítók által biztosított megbízható ellenőrzőösszegek (checksum) elérhetőségét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, hogy mely felhasználók által telepített szoftverelemeket szükséges ellenőrzés alá vonni végrehajtás előtt.
2. A szervezetnek szükséges létrehoznia egy stratégiát, mely meghatározza az integritás ellenőrzésére szolgáló intézkedéseket.
3. A szervezetnek be kell vezetnie a létrehozott stratégia által meghatározott intézkedéseket az érintett rendszerelemeken.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.49. Felhasználó által telepített szoftver

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

SI-7(12)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a felhasználó által telepített szoftver meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.53. SZOFTVER-, FIRMWARE- ÉS INFORMÁCIÓSÉRTETLENSÉG – KÓDOK HITELESÍTÉSE

18.53. A szervezet kriptográfiai mechanizmusokat alkalmaz a meghatározott szoftver- vagy firmware-elemek hitelesítésére a telepítés előtt.

MAGYARÁZAT

A kriptográfiai hitelesítés magában foglalja annak ellenőrzését, hogy a szoftver- vagy firmware-összetevőket a szervezetek által elismert és jóváhagyott tanúsítványokkal digitálisan aláírták-e. A kódaláírás hatékony módszer a rosszindulatú kódok elleni védelemre. A kriptográfiai mechanizmusokat alkalmazó szervezetek megfontolják a kriptográfiai kulcskezelési megoldásokat is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely szoftver- vagy firmware-elemeket kell hitelesíteni a telepítés előtt, valamint azt, hogy milyen kriptográfiai mechanizmusokat alkalmazzanak a hitelesítési folyamat megvalósítására.
2. A szervezetnek kriptográfiai mechanizmusokat kell alkalmaznia a meghatározott szoftver- vagy firmware-elemek hitelesítésére. Ez magában foglalja a digitális aláírások használatát, amelyeket a szervezet által elismert és jóváhagyott tanúsítványokkal hitelesítenek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

6.18. A változtatásokra vonatkozó hozzáférés korlátozások
17.49. Kriptográfiai kulcs előállítása és kezelése
17.53. Kriptográfiai védelem

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

SI-7(15)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a szoftver vagy firmware elemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

18.54. SZOFTVER-, FIRMWARE- ÉS INFORMÁCIÓSÉRTETLENSÉG – IDŐKORLÁT A FOLYAMAT VÉGREHAJTÁSÁRA

18.54. A szervezet tiltja a meghatározott időnél hosszabb folyamatok felügyelet nélküli végrehajtását.

MAGYARÁZAT

A felügyelet nélküli folyamatvégrehajtás időbeli korlátozásának célja, hogy olyan folyamatokra korlátozzon, amelyeknél meghatározható a tipikus vagy szokásos végrehajtási idő, illetve olyan helyzetekre, amelyekben a szervezetek túllépik ezeket az időszakokat. A felügyelet magában foglalja az operációs rendszerek időzítőit, az automatizált válaszokat, valamint a rendszerfolyamatok rendellenességei esetén a kézi felügyeletet és reagálást.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a folyamatokat, amelyeknél meghatározható a tipikus vagy normál végrehajtási időszak.
2. A szervezetnek be kell állítania időzítőket a rendszerelem operációs rendszerében, amelyek figyelemmel kísérik a folyamatok végrehajtási idejét.
3. A szervezetnek automatikus válaszokat kell beállítania, amelyek aktiválódnak, ha egy folyamat végrehajtási ideje meghaladja a meghatározott időszakot. Ezek az automatikus válaszok például leállíthatják a folyamatot, vagy értesítést küldhetnek a rendszerfelügyelőnek.
4. A szervezetnek manuális felügyeletet és választ is biztosítania kell, ha folyamatvégrehajtási anomáliák fordulnak elő. Ez azt jelenti, hogy a rendszerfelügyelőnek képesnek kell lennie azonosítani és kezelni azokat a helyzeteket, amikor egy folyamat végrehajtási ideje meghaladja a meghatározott időszakot.

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

SI-7(16)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az idő intervallum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.55. SZOFTVER-, FIRMWARE- ÉS INFORMÁCIÓSÉRTETLENSÉG – BEÉPÍTETT VÉDELEM

18.55. A szervezet meghatározott követelményeket alkalmaz az alkalmazások beépített védelmének (RASP) biztosítására, azok futása közben.

MAGYARÁZAT

A futásidejű alkalmazás-önvédelem a szoftver sebezhetőségének felderítésére és megakadályozására szolgál futásidejű eszközökkel, a végrehajtás alatt álló szoftverből származó információk felhasználásával. A futásidejű alkalmazás-önvédelem különbözik a hagyományos rendszerhatár alapú védelemtől, például a tűzfalaktól, amelyek a kontextus ismerete nélkül, csak a hálózati információk felhasználásával képesek a támadások felderítésére és blokkolására. A futásidejű alkalmazás-önvédelmi technológiája csökkentheti a szoftverek támadásokkal szembeni érzékenységét azáltal, hogy figyelemmel kíséri a bemeneteket, és blokkolja azokat, amelyek lehetővé teszik a támadásokat. Segíthet továbbá megvédeni a futásidejű környezetet a nem kívánt változtatásoktól és manipulációktól. Ha veszélyt észlel, a futásidejű alkalmazás-önvédelmi technológiája megakadályozhatja a kihasználást és egyéb intézkedéseket tehet. A futásidejű alkalmazás-önvédelmi megoldások felügyeleti vagy védelmi üzemmódban is telepíthetők.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a futásidejű alkalmazás-önvédelmi (Runtime application self-protection - RASP) technológiát, melyet alkalmazni kíván, a rendszerelemeket melyek érintettek a védelem szempontjából, valamint azokat a felhasználókat és szerepköröket, akiket szükség esetén értesíteni kell az esetleges figyelmeztetések esetén.
2. A szervezetnek implementálnia kell a választott futásidejű alkalmazás-önvédelmi technológiát az érintett rendszerelemeken.
3. A szervezetnek be kell állítania a futásidejű alkalmazás-önvédelmi technológiát úgy, hogy az monitorozza az adott rendszerelem bemeneteit, és blokkolja azokat a bemeneteket, amelyek támadásokat tesznek lehetővé, valamint értesíti az érdekelt személyeket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

18.78. Memóriavédelem

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

SI-7(17)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.56. KÉRETLEN ÜZENETEK ELLENI VÉDELEM

18.56. A szervezet:

18.56.1. olyan levélszemét elleni védelmet valósít meg az EIR belépési és kilépési pontjain, amelyek felismerik és kezelik az ilyen üzeneteket; és

18.56.2. új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat a konfigurációkezelési szabályokkal összhangban.

MAGYARÁZAT

Az EIR belépési és kilépési pontjai közé tartoznak például a tűzfalak, az elektronikus levelezőszerverek, a webkiszolgálók, a proxy szerverek, a távoli hozzáférést biztosító kiszolgálók, a munkaállomások, notebook számítógépek és mobileszközök. A kéretlen üzenetek többféle médiumon keresztül közlekedhetnek, például email, email csatolmányok vagy webes tartalmak. A levélszemét elleni védelmi mechanizmusok közé tartoznak például a szignatúra definíciók.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az érintett szervezetnek meg kell határoznia az EIR belépési és kilépési pontjait, melyeken kértelen üzenetek elleni védelmet szükséges megvalósítani.
2. Az érintett szervezetnek meg kell határoznia egy stratégiát, amely alapján a védelmi rendszerek képesek felismerni és kezelni a kéretlen üzeneteket.
3. Az érintett szervezetnek implementálnia kell egy kértelen üzenetek elleni védelmi rendszert az EIR belépési és kilépési pontjain a korábban meghatározott stratégia alapján.
4. Amikor új verziók válnak elérhetővé, az érintett szervezetnek frissítenie kell a levélszemét elleni védelmi mechanizmusokat a konfigurációkezelési szabályokkal összhangban.

KAPCSOLÓDÓ INTÉZKEDÉSEK

13.9. Központi kezelés

17.12. Szolgáltatásmegtagadással járó támadások elleni védelem

17.17. A határok védelme

17.107. Működésbiztonság

18.8. Kártékony kódok elleni védelem

18.13. Az EIR monitorozása

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

3.3.11.9. Kéretlen üzenetek elleni védelem

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-8

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

18.57. KÉRETLEN ÜZENETEK ELLENI VÉDELEM – AUTOMATIKUS FRISSÍTÉSEK

18.57. A szervezet meghatározott gyakorisággal automatikusan frissíti a levélszemét elleni védelmi mechanizmusokat.

MAGYARÁZAT

A levélszemét elleni védelem automatikus frissítési mechanizmusainak használata segít biztosítani, hogy a frissítések rendszeresen megtörténjenek, és a védelmi rendszerek naprakész védelmet nyújtsák az érintett rendszerelemeknek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek szükséges, hogy legyen egy automatikus frissítési mechanizmusa, amely képes frissíteni a kéretlen üzenetek elleni védelmi eszközöket.
2. A szervezetnek meg kell határoznia a gyakoriságot, amellyel az automatikus frissítési mechanizmusok frissítik a kéretlen üzenetek elleni védelmet.
3. A szervezetnek alkalmaznia kell a frissítési gyakoriságra vonatkozó beállításokat az automatikus frissítési mechanizmusokra, hogy a kéretlen üzenetek elleni védelmi eszközök naprakészek legyenek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.11.9. Kéretlen üzenetek elleni védelem

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-8(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

18.58. KÉRETLEN ÜZENETEK ELLENI VÉDELEM – FOLYAMATOS TANULÁSI KÉPESSÉG

18.58. A szervezet tanulási képességgel ellátott levélszemét elleni védelmi mechanizmusokat alkalmaz, hogy hatékonyabban tudja azonosítani a jogos kommunikációs forgalmat.

MAGYARÁZAT

A levélszemét elleni védelmi mechanizmusok tanulási képességei közé tartoznak a Bayes-szűrők, amelyek adott forgalmat spamként vagy legitimként azonosító bemenetek alapján frissítik a védelmi mechanizmusok paramétereit, így pontosabban képesek elkülöníteni a különböző típusú kommunikációs forgalmakat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet olyan kéretlen üzenetek elleni védelmi mechanizmusokat alkalmaz, amelyek tanulási képességgel rendelkeznek.

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

SI-8(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.59. BEMENETI INFORMÁCIÓ ELLENŐRZÉS

18.59. A szervezet ellenőrzi a meghatározott beviteli információk érvényességét.

MAGYARÁZAT

A bemeneti adatok érvényes szintaxisának és szemantikájának ellenőrzésével megtudható, hogy a bemenetek megfelelnek-e a meghatározott formai és a tartalmi követelményeknek, ide tartoznak a karakter számok, az elfogadott karakterek, számtartományok és elfogadható értékek. Például, ha a szervezet azt határozza meg, hogy egy adott alkalmazásban egy mező számára csak az 1-100 közötti számértékek az elfogadható bemenetek, akkor a 387, abc, vagy %K% értékek érvénytelen bemenetek, és nem fogadhatóak el bemeneteként.

Az érvényes bemenetek valószínűleg mezőről mezőre változnak egy szoftveralkalmazáson belül. A szoftveralkalmazások jellemzően jól meghatározott protokollokat követnek, amelyek strukturált üzeneteket (azaz parancsokat vagy lekérdezéseket) használnak a szoftver modulok vagy rendszerelemek közötti kommunikációhoz. A strukturált üzenetek nyers vagy strukturálatlan adatokat is tartalmazhatnak metaadatokkal vagy vezérlési információkkal. Ha a szoftveralkalmazások a támadó által megadott bemeneteket használnak strukturált üzenetek létrehozásához az üzenetek megfelelő kódolása nélkül, akkor a támadó kártékony parancsokat vagy speciális karaktereket juttathat be a rendszerbe. Az így szennyezett kimenetet fogadó modul vagy összetevő hibás műveleteket hajt végre, vagy helytelenül értelmezi az adatokat. Az értelmező modulok előtti bemenetek előzetes szűrése megakadályozza a tartalom véletlen parancsként való értelmezését. A bemeneti adatok ellenőrzése segít a pontos és helyes bemenetek biztosításában és az olyan jellegű támadások megakadályozásában, mint például a Cross Site Scripting (XSS) és különböző befecskendezéses támadások (Injection).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely rendszerelemek mely mezői által kezelt bemeneti adatait szükséges ellenőrizni.
2. A szervezetnek meg kell határoznia a meghatározott rendszerelemek beviteli adatainak érvényes szintaxisát és szemantikáját, beleértve a karakterkészletet, a hosszt, a numerikus tartományt és az elfogadható értékeket a meghatározott bemeneti mezőkre.

3. A szervezetnek alkalmaznia kell a meghatározott rendszerelemek és bemeneti mezők által kezelt beviteli adatok ellenőrzését a meghatározott szempontok alapján.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.11.10. Bemeneti információ ellenőrzés: Az elektronikus információs rendszer ellenőrzi a meghatározott információ belépési pontok érvényességét.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-10

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszer beviteli információk meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

18.60. Bemeneti információ ellenőrzés – Manuális felülírási képesség

18.60. A szervezet:

18.60.1. a meghatározott beviteli információk ellenőrzésénél biztosítja az alapkövetelmények manuális felülbírálati lehetőségét;

18.60.2. a meghatározott jogosult személyekre korlátozza a manuális felülbírálati lehetőség használatát; és

18.60.3. ellenőrzi a manuális felülbírálat lehetőségének használatát.

Magyarázat

Bizonyos helyzetekben, például a vészhelyzeti tervekben meghatározott intézkedések során szükség lehet a bemeneti adatok érvényesség vizsgálatának kézi felülbírálhatóságára. A kézi felülbírálást csak korlátozott körülmények között és a szervezet által meghatározott, arra jogosult személyek használják.

A követelmény alkalmazásának lépései

1. A szervezetnek biztosítania kell a beviteli információk ellenőrzésének manuális felülbírálati lehetőségét.

2. A szervezetnek meg kell határoznia a manuális felülbírálati lehetőség használatára jogosult személyeket.

3. A szervezetnek ellenőriznie kell a manuális felülbírálat lehetőségének használatát. Például naplót vezethet arról, hogy mely felhasználó, mikor és milyen adatokat bírált felül manuálisan.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

4.2. Naplózható események

4.40. Naplóbejegyzések létrehozása

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

SI-10(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.61. BEMENETI INFORMÁCIÓ ELLENŐRZÉS – HIBÁK FELÜLVIZSGÁLATA ÉS MEGOLDÁSA

18.61. A szervezet meghatározott időn belül felülvizsgálja és kezeli az adatbevitel érvényesítési hibáit.

MAGYARÁZAT

A beviteli érvényesítési hibák megoldása magában foglalja a hibák rendszerszintű okainak kijavítását és a tranzakciók újbóli benyújtását a javított adatokkal. Az érintett információs bemeneteket lásd az alap kontrollban: 18.59.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az adatbeviteli hibák ellenőrzésére kiszabott időkorlátot.
2. A szervezetnek ki kell dolgozni a stratégiát, amely alapján az adatbeviteli hibák ellenőrzésre kerülnek a meghatározott időn belül.
3. A szervezetnek alkalmaznia kell az adatbeviteli hibák meghatározott időn belüli javítására irányuló stratégiát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

SI-10(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az idő intervallum meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.62. BEMENETI INFORMÁCIÓ ELLENŐRZÉS – RENDSZER KISZÁMÍTHATÓ MŰKÖDÉSE

18.62. A szervezet ellenőrzi, hogy a rendszer előrelátható és dokumentált módon viselkedik-e, amikor érvénytelen bemenő adatot kap.

MAGYARÁZAT

A szervezeti rendszerelemek gyakori sebezhetősége a kiszámíthatatlan viselkedés, amikor érvénytelen bemenet érkezik. A rendszerelem kiszámíthatóságának ellenőrzése segít biztosítani, hogy a rendszerelem a várt módon viselkedjen, amikor érvénytelen bemenetek érkeznek. Ez olyan rendszerszintű válaszesemények megadásával történik, amelyek lehetővé teszik, hogy a rendszerelem káros, nem szándékolt mellékhatások nélkül lépjen át ismert állapotokba. Az érintett információs bemeneteket lásd az alap kontrollban: 18.59.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia azokat az információs bemeneteket, amelyek érvénytelenek a rendszerelem számára.
2. A szervezetnek meg kell határoznia és dokumentálnia kell a rendszerelem válaszait az érvénytelen bemenetekre.
3. A szervezetnek ellenőriznie kell, hogy a rendszerelem előre láthatóan és dokumentált módon viselkedik-e, amikor érvénytelen bemenetet kap.

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

SI-10(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.63. BEMENETI INFORMÁCIÓ ELLENŐRZÉS – IDŐZÍTÉSI INTERAKCIÓK

18.63. Az EIR az érvénytelen bemeneti adatokra adott megfelelő válaszok meghatározásakor, figyelembe veszi a rendszerelemek közötti időzítési interakciókat.

MAGYARÁZAT

A protokollinterfészeken keresztül érkező érvénytelen rendszerbemenetek kezelése során az időzítési kölcsönhatások relevánssá válnák, amikor az egyik protokollnak figyelembe kell vennie a hibaválasz hatását a protokollköteg más protokolljaira. Például a 802.11 szabványú vezeték nélküli hálózati protokollok nem működnek jól együtt a TCP protokollokkal, amikor csomagok kerülnek eldobásra (ami lehet érvénytelen csomagbemenet miatt). A TCP feltételezi, hogy a csomagvesztés torlódás miatt következik be, míg a 802.11-es kapcsolatokon keresztül elveszett csomagok jellemzően a zaj vagy a kapcsolaton belüli ütközések miatt esnek ki. Ha a TCP torlódási választ ad, akkor az ütközéses eseményre adott válaszként rosszul cselekszik. rosszindulatú támadók kedvezőtlen hatásokat érhetnek el úgy, hogy a protokollok elfogadhatónak tűnő egyedi viselkedéseit együttesen használják fel az érvénytelen bemenet megfelelő felépítésével.Az érintett információs bemeneteket lásd az alap kontrollban: 18.59.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek figyelembe kell vennie az EIR-ben használt protokollok közötti időzítési interakciókat.
2. A szervezetnek meg kell határoznia azokat az érvénytelen bemeneteket, amelyek kapcsolódnak az EIR által definiált információs bemenetekhez a protokollok közötti időzítési interakciók figyelembevételével.

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

SI-10(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.64. Bemeneti információ ellenőrzés – Bemeneteket megbízható forrásokra és jóváhagyott formátumokra korlátozása

18.64. A szervezet az információbevitelt a meghatározott, megbízható forrásokra és a meghatározott formátumokra korlátozza.

Magyarázat

A bemeneti adatok használatának megbízható forrásokra és formátumokra való korlátozása a jogosult vagy engedélyezett szoftver fogalmának alkalmazása az információs bemenetekre. Az információs bemenetek ismert, megbízható forrásainak és elfogadható formátumainak meghatározása csökkentheti a káros tevékenység valószínűségét. Az érintett információs bemeneteket lásd az alap kontrollban: 18.59.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a megbízható forrásokat, amelyekről információbevitel történhet.
2. A szervezetnek meg kell határoznia a megbízható formátumokat, amelyekben az információbevitel történhet.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

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

SI-10(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a megbízható források illetve a formátumok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.65. BEMENETI INFORMÁCIÓ ELLENŐRZÉS – AZ ADATOK INJEKTÁLÁSÁNAK MEGAKADÁLYOZÁSA

18.65. Az EIR megakadályozza az adatok injektálását.

MAGYARÁZAT

A nem megbízható adatok injektálása megakadályozható egy paraméterezett interfész vagy a kimeneti kódolás segítségével. A paraméterezett interfészek elválasztják az adatokat a kódtól, így a rosszindulatú vagy nem kívánt adatok bevitele nem tudja megváltoztatni a küldött parancsok szemantikáját. A kimeneti átalakítás (output escaping - a veszélyes vezélrő karakterek lecserélése) a meghatározott karakterek segítségével dönti el az EIR kódfeldolgozója, hogy az adatok megbízhatóak-e. Az érintett információs bemeneteket lásd az alap kontrollban: 18.59.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR-ben használt információ bemeneteket.
2. A szervezetnek paraméterezett interfészeket, vagy kimeneti átalakítást (output escaping, output encoding) kell alkalmaznia a meghatározott információ bemenetekre.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

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

SI-10(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.66. HIBAKEZELÉS

18.66. Az EIR:

18.66.1. olyan hibajelzéseket állít elő, amelyek a hibák kijavításához szükséges információkat szolgáltatnak anélkül, hogy kihasználható információkat tárnának fel; és

18.66.2. a hibaüzeneteket csak a meghatározott személyeknek vagy szerepköröknek teszi elérhetővé.

MAGYARÁZAT

Az érintett szervezetek gondosan mérlegelik a hibaüzenetek szerkezetét és tartalmát. A rendszerelem képességét, hogy kezelje a hibaállapotokat, a szervezet irányelvei és működési követelményei szabják meg.

A kihasználható információk közé tartoznak a verem-nyomkövetés (stack traces) és implementációs részletek;

hibás bejelentkezési kísérletek, amikor a jelszót tévedésből a felhasználónév helyére írják;

a küldetési vagy üzleti információ, amelyet a naplózott információból lehet levezetni, ha azt nem közvetlenül jelzik;

és a személyesen azonosítható információk, mint például a számlaszámok, a szociális biztonsági számok és a hitelkártya-számok.

A hibaüzenetek továbbá rejtett csatornát is biztosíthatnak az információk továbbításához, mely információ szivárgáshoz vezethet.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a hibaüzenetek struktúráját és tartalmát.

2. A szervezetnek biztosítania kell, hogy a rendszerelem ne szolgáltasson kihasználható információkat a hibaüzenetekben, ugyanakkor a hibák kijavításához szükséges információkat tartalmazza.

3. A szervezetnek meg kell határoznia, hogy mely személyek vagy szerepkörök férhetnek hozzá a hibaüzenetekhez.

4. A szervezetnek biztosítania kell, hogy a hibaüzenetek csak a meghatározott személyek vagy szerepkörök számára legyenek elérhetőek.

Kapcsolódó intézkedések

4.2. Naplózható események

4.3. Naplóbejegyzések tartalma

17.92. Rejtett csatornák elemzése

18.2. Hibajavítás

18.77. A kimeneti információ kezelése és megőrzése

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

3.3.11.11. Hibakezelés

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SI-11

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

18.67. INFORMÁCIÓ KEZELÉSE ÉS MEGŐRZÉSE

18.67. A szervezet az EIR-ben lévő és az onnan kikerülő információk kezelése és megőrzése során a szervezetre vonatkozó, hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások és működési követelmények szerint jár el.

MAGYARÁZAT

Az információkezelési és megőrzési követelmények az információ teljes életciklusát lefedik, néhány esetben a rendszer megsemmisítésén túl is. A megőrzendő információk közé tartozhatnak az irányelvek, eljárások, tervek, jelentések, a követelménymegvalósításból származó adatkimenetek és egyéb adminisztratív információk. Ha a szervezetnek van iratkezelési részlege, érdemes lehet együttműködni az iratkezelési személyzettel.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia a rendszerben lévő és onnan kikerülő információk kezelésének és megőrzésének szabályzatát, eljárásait és terveit a hatályos jogszabályok, irányelvek, szabályozások, szabványok és ajánlások, valamint a működési követelmények szerint.
2. A szervezetnek alkalmaznia kell a meghatározott szabályzatokat és eljárásokat a rendszerből kikerülő információk kezelésének és megőrzésének során.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.89. Biztonsági tulajdonságok
4.7. Naplózási hiba kezelése
4.38. A naplóbejegyzések megőrzése
5.2. Biztonsági értékelések
5.6. Információcsere
5.9. Az intézkedési terv és mérföldkövei
5.11. Engedélyezés
5.14. Folyamatos felügyelet
5.24. Belső rendszerkapcsolatok
6.18. A változtatásokra vonatkozó hozzáférés korlátozások

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

SI-12

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

18.68. ELŐRELÁTHATÓ MEGHIBÁSODÁS MEGELŐZÉSE

18.68. A szervezet:

18.68.1. meghatározza a meghibásodásig eltelt átlagos időt (MTTF) a meghatározott rendszerelemekre a meghatározott működési környezetekben; és

18.68.2. helyettesítő rendszerelemeket biztosít, valamint az aktív és készenléti rendszerelemek cseréjének módját a meghatározott helyettesítési kritériumoknak megfelelően végzi.

MAGYARÁZAT

Bár a meghibásodásig eltelt átlagos idő (mean time to failure (MTTF)) elsősorban megbízhatósági kérdés, a kiszámítható meghibásodás megelőzése a biztonsági képességeket biztosító rendszerelemek lehetséges meghibásodásait hivatott kezelni. A meghibásodási arányok inkább az alkalmazásspecifikus állapotokat tükrözik, mintsem az iparági átlagot. A szervezetek az MTTF-érték alapján határozzák meg az rendszerelemek cseréjének feltételet, figyelembe véve az alkatrészhibákból eredő potenciális károkat. Az aktív és a készenléti elemek közötti felelősségátadás nem veszélyeztetheti a biztonságot, az üzemi készenlétet vagy a biztonsági képességeket. A rendszerállapot-változók megőrzése szintén kritikus fontosságú a sikeres átadási folyamat biztosításához. A készenléti elemek a karbantartási problémák vagy a folyamatban lévő helyreállítási hibák kivételével mindig rendelkezésre állnak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet meghatározza a meghibásodásig eltelt átlagos időt (mean time to failure (MTTF)), valamint a helyettesítési kritériumoknak a meghatározott rendszerelemekre a meghatározott működési környezetekben.

2. A szervezet biztosítja helyettesítő rendszerelemeket.

3. A szervezet az aktív és készenléti rendszerelemek cseréjét a meghatározott helyettesítési kritériumoknak megfelelően végzi.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.2. Üzletmenet-folytonossági terv

7.43. Az elektronikus információs rendszer helyreállítása és újraindítása

7.49. Alternatív biztonsági mechanizmusok alkalmazása

10.2. Szabályozott karbantartás

10.21. Kellő időben történő karbantartás

16.16. Biztonságtervezési elvek

17.16. Erőforrások rendelkezésre állása

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

SI-13

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.69. Előrelátható meghibásodás megelőzése - Helyettesítő rendszerelemek használata

18.69. A szervezet a rendszerelemeket úgy helyezi üzemen kívül, hogy a rendszerelemek feladatai a helyettesítő rendszerelemekre helyeződnek át, legkésőbb a meghibásodásig eltelt átlagos idő (MTTF) szervezet által meghatározott hányadának vagy százalékának leteltét követően.

Magyarázat

Az elsődleges rendszerelemek feladatainak más helyettesítő rendszerelemekre történő átruházása az elsődleges rendszerelem meghibásodása előtt fontos a meghatározott célok és üzleti funkciók romlásának vagy gyengülésének kockázatának csökkentése érdekében. Az ilyen átadásoknak a meghibásodásig eltelt átlagos idő százalékos aránya alapján történő végrehajtása lehetővé teszi a szervezetek számára, hogy kockázattűrő képességüknek megfelelően proaktívan járjanak el. Az EIR-elemek idő előtti cseréje azonban a rendszerüzemeltetés megnövekedett költségeit eredményezheti.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a rendszerelemek átlagos meghibásodási idejét.
2. A szervezetnek meg kell határoznia a meghibásodásig eltelt átlagos idő (mean time to failure (MTTF)) százalékos arányát, amely után a rendszerelemeket üzemen kívül helyezi.
3. A szervezetnek rendelkeznie kell helyettesítő rendszerelemekkel, amelyek átveszik a kivont rendszerelemek feladatait.
4. A szervezetnek be kell ütemeznie a rendszerelemek kivonását és a helyettesítő rendszerelemek bevezetését, hogy a folyamat minimalizálja a működési zavarokat.

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

SI-13(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az hányad vagy százalék meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.70. Előre látható meghibásodás megelőzése – Manuális átvitel rendszerelemek között

18.70. A szervezet manuálisan kezdeményezi az aktív és készenléti rendszerelemek közötti átállást, amikor az aktív rendszerelem használati ideje eléri a meghibásodásig eltelt átlagos idő (MTTF) szervezet által meghatározott hányadát vagy százalékát.

Magyarázat

Például, ha egy rendszerelem meghibásodásáig eltelt átlagos idő 100 nap, és az érintett szervezet által meghatározott MTTF százalék 90 százalék, akkor a manuális átállás 90 nap után történik.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia az aktív rendszerelemek meghibásodásáig eltelt átlagos időt.
2. A szervezetnek meg kell határoznia azt a százalékos értéket, amely alapján a manuális átállást kezdeményezik.
3. Ha egy aktív rendszerelem használati ideje eléri az MTTF érték meghatározott százalékát, akkor a szervezetnek manuálisan át kell állnia a készenléti rendszerelemre.

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

SI-13(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a százalékos arány meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.71. Előre látható meghibásodás megelőzése – Készenléti tartalék rendszerelemek telepítése és értesítés

18.71. A szervezet a rendszerelemek hibáinak észlelésekor:

18.71.1. gondoskodik arról, hogy a készenléti rendszerelemek sikeresen és átlátható módon telepítésre kerüljenek a szervezet által meghatározott időablakon belül, és

18.71.2. aktiválja a meghatározott riasztást, valamint automatikusan leállítja az EIR-t és egyéb meghatározott műveleteket hajt végre.

Magyarázat

A készenléti rendszerelemek automatikus, vagy manuális módon történő aktív módba kapcsolása akkor történik meg, ha egy aktív rendszerelem meghibásodását észlelik.

A követelmény alkalmazásának lépései

1. A szervezetnek rendelkeznie kell egy olyan rendszerrel, amely képes észlelni különböző rendszerelemek hibáit.

2. A szervezetnek meg kell határoznia azon intézkedéseket és körülményeket, melyek alapján egy meghibásodott rendszerelem cseréje sikeresen és átlátható módon megtörténhet. Ebbe beletartozhat a időablak, amelyen belül a készenléti rendszerelemek telepítése megtörténik, valamint további intézkedések, mint a riasztás, amelyet ki kell küldeni hiba észlelésekor, valamint a rendszer automatikusan leállítása.

3. Amikor egy hiba észlelhető egy rendszerelemben, a szervezetnek gondoskodnia kell arról, hogy a meghatározott intézkedések végre legyenek hajtva a meghatározott körülmények között.

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

SI-13(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.72. ELŐRE LÁTHATÓ MEGHIBÁSODÁS MEGELŐZÉSE – BIZTONSÁGI MENTŐKAPACITÁS

18.72. A szervezet valós idejű vagy közel valós idejű átállási képességet biztosít az EIR számára, a szervezet által meghatározott módon.

MAGYARÁZAT

Az átállás az elsődleges rendszer hibájának esetén egy alternatív rendszerre történő automatikus átváltást jelenti. Az átállási képesség magában foglalja a rendszerműveletek tükrözött lefolytatását alternatív feldolgozási helyszíneken vagy az adatok periodikus tükrözését az érintett szervezet által meghatározott helyreállítási időszakokban.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a rendszer átállási képességének (Failover Capability) szükségességét és módját. Ez magában foglalhatja a rendszerműveletek tükrözött lefolytatását alternatív feldolgozási helyeken, vagy az adatok tükrözését a szervezet által meghatározott időközönként.
2. A szervezetnek biztosítania kell, hogy a rendszer közel valós idejű átállást tudjon biztosítani a meghatározott módon.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.19. Biztonsági tárolási helyszín

7.23. Alternatív feldolgozási helyszín

7.35. Az elektronikus információs rendszer mentései

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

SI-13(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági mentőkapacitás meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.73. NEM ÁLLANDÓ RENDSZERELEMEK ÉS SZOLGÁLTATÁSOK

18.73. A szervezet olyan nem állandó rendszerelemeket és szolgáltatásokat alkalmaz, amelyeket ismert állapotban indít el, és a munkaszakasz végén vagy meghatározott gyakorisággal leállít.

MAGYARÁZAT

A nem állandó rendszerelemek és szolgáltatások alkalmazása csökkenti a fejlett, tartós fenyegetések (APT) kockázatát, mivel csökkenti a támadók célzó képességét (azaz a lehetőségeket és az elérhető támadási felületet) a támadások elindításához és befejezéséhez. A nem állandó jellegű koncepció alkalmazásával a szervezetek bizonyos rendszerelemekre megbízható, ismert állapotú számítási erőforrást tudnak biztosítani, amely nem ad elegendő időt a támadóknak a szervezet EIR-jében vagy működési környezetében lévő sebezhetőségek kihasználására. Mivel a fejlett, tartós fenyegetések (APT) képességei és szándékai, valamint a célpontjai tekintetében egy magas szintű, kifinomult fenyegetés, a szervezetek feltételezik, hogy hosszabb időn keresztül a támadások egy bizonyos százaléka sikeres lesz. A nem állandó rendszerelemek és szolgáltatások szükség szerint aktiválódnak a védett információk felhasználásával, és meghatározott gyakorisággal vagy a munkamenetek végén leállnak. Az időszakos működés növeli a szervezeti EIR-eket kompromittálni vagy feltörni próbáló támadók munkaerő-faktorait.

A nem állandóság elérhető a rendszerelemek frissítésével, az elemek rendszeres újrapéldányosításával lemezképfájlból, vagy számos általános virtualizációs technika alkalmazásával. A nem állandó szolgáltatásokat virtualizációs technikák alkalmazásával lehet megvalósítani, mint a virtuális gépek része, vagy új folyamatpéldányokként fizikai gépeken (akár állandó, akár nem állandó). Az rendszerelemek és szolgáltatások rendszeres frissítésének előnye, hogy nem igényli a szervezetektől, hogy megállapítsák, vajon megtörtént-e az elemek vagy szolgáltatások kompromittálása (amit gyakran nehéz lehet megállapítani). A kiválasztott rendszerelemek és szolgáltatások frissítése kellő gyakorisággal történik ahhoz, hogy megakadályozza a támadások terjedését vagy tervezett hatását, de nem olyan gyakorisággal, hogy az instabillá tegye az EIR-t. A kritikus elemek és szolgáltatások frissítése meghatározott

gyakorisággal történhet, hogy a támadók ne tudják kihasználni a sebezhetőségek optimális időablakát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek olyan nem állandó (non-persistent) rendszerelemeket és szolgáltatásokat kell alkalmaznia, amelyeket ismert állapotban indít el. Ezeket az elemeket és szolgáltatásokat a munkaszakasz végén vagy meghatározott gyakorisággal le kell állítani.
2. A szervezetnek meg kell valósítania a nem állandó jellegű koncepcióját a kiválasztott rendszerelemek számára. Ezáltal biztosítható, hogy a szervezet egy megbízható, ismert állapotú számítási erőforrást biztosítson egy adott időszakra, amely nem ad elegendő időt a támadóknak a szervezet EIR-jének vagy működési környezetének kihasználására.
3. A szervezetnek a nem állandó rendszerelemeket és szolgáltatásokat védett információk felhasználásával kell aktiválnia, és rendszeresen vagy a munkamenetek végén le kell állítania.
4. A nem állandóság elérhető a rendszerelemek frissítésével, rendszeres újratelepítéssel lemezképfájlból, vagy számos általános virtualizációs technika alkalmazásával.
5. A rendszerelemek és szolgáltatások időszakos frissítésének előnye, hogy a szervezetnek nem kell először megállapítania, hogy az elemek vagy szolgáltatások kompromittálódtak-e (amit gyakran nehéz és időigényes lehet megállapítani). A rendszerelemek és szolgáltatások frissítése elegendő gyakorisággal történik ahhoz, hogy megakadályozza a támadások terjedését vagy szándékos hatását, de nem olyan gyakran, hogy instabillá tenné az EIR-t.
6. A kritikus elemek és szolgáltatások frissítése időszakosan történhet, hogy megakadályozza a támadók általi sebezhetőségek kihasználását.
7. A szervezetnek dokumentálnia kell a nem állandó rendszerelemek és szolgáltatások aktiválását és leállítását/megszüntetését, valamint az elemek és szolgáltatások frissítését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.87. Elfedés és megtévesztés

17.98. Végrehajtható, de nem módosítható programok

18.81. Információfrissítés

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

SI-14

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az rendszerelemek és szolgáltatások illetve a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.74. NEM ÁLLANDÓ RENDSZERELEMEK ÉS SZOLGÁLTATÁSOK – MEGBÍZHATÓ FORRÁSOKBÓL TÖRTÉNŐ FRISSÍTÉS

18.74. A szervezet a rendszerelemek és szolgáltatások frissítése során felhasznált szoftvereket és adatokat a szervezet által meghatározott megbízható forrásokból szerzi be.

MAGYARÁZAT

A megbízható források közé tartoznak az egyszer írható, csak olvasható adathordozókról vagy kiválasztott, biztonságos offline tárolóhelyekről származó szoftverek és adatok.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és dokumentálnia azokat a megbízható forrásokat, ahonnan a szoftvereket és adatokat beszerzi. Ez magában foglalhatja a szoftvergyártók hivatalos weboldalait, hitelesített szoftverkönyvtárakat, vagy akár offline, biztonságos tárolóhelyeket.
2. A szervezetnek biztosítania kell, hogy az EIR frissítése során csak ezekből a megbízható forrásokból származó szoftvereket és adatokat használják. Ez magában foglalhatja a szoftverek letöltését és telepítését, valamint az adatok importálását és exportálását.
3. A szervezetnek rendszeresen ellenőriznie kell, hogy az EIR frissítései megfelelnek-e a megbízható forrásokból származó szoftverek és adatok használatával támasztott követelményének. Ez magában foglalhatja a naplók áttekintését, a szoftverek és adatok eredetének ellenőrzését, és a megbízható források listájának frissítését.
4. A szervezetnek biztosítania kell, hogy az EIR frissítéseinek folyamatai és eljárásai megfelelnek a szervezet belső szabályainak és eljárásainak, valamint a vonatkozó jogszabályi és szabványos követelményeknek.
5. A szervezetnek rendszeresen képeznie kell a munkatársait az EIR frissítéseinek folyamatairól és eljárásairól, valamint a megbízható forrásokból származó szoftverek és adatok használatának fontosságáról.

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

SI-14(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a megbízható források meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.75. NEM ÁLLANDÓ INFORMÁCIÓK KEZELÉSE

18.75. A szervezet:

18.75.1. meghatározott gyakorisággal frissíti a meghatározott információkat, igény szerint létrehozza a meghatározott információkat; és

18.75.2. törli az információkat, amennyiben már nincs rájuk szükség.

MAGYARÁZAT

Az információknak a szükségesnél hosszabb ideig történő megőrzése potenciális célponttá teszi az információkat a fejlett támadók számára, akik értékes információkat keresnek, amelyeket jogosulatlan nyilvánosságra hozatal, jogosulatlan módosítás vagy kiszivárogtatás útján veszélyeztethetnek. Az EIR-rel kapcsolatos információk esetében a szükségtelen megőrzés olyan információkat biztosít a fejlett támadók számára, amelyek segíthetik felderítésüket és az EIR-en keresztüli mozgást.

A szervezetnek meg kell határoznia a frissítések gyakoriságát a meghatározott információkra vonatkozóan, hogy biztosítsa azok naprakészségét és relevanciáját.

A szervezetnek továbbá törölnie kell azokat az információkat, amelyekre már nincs szüksége. A felesleges vagy tartós használaton kívüli adatok törlése csökkenti az adatok jogosulatlan hozzáférésének kockázatát, és segít megőrizni az EIR integritását és biztonságát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, milyen információkat kell rendszeresen frissítenie. Ez magában foglalhatja a különböző adatokat, dokumentumokat, jelentéseket stb.

2. A szervezetnek be kell állítania egy rendszert, amely automatikusan frissíti ezeket az információkat a meghatározott gyakorisággal. Ez lehet naponta, hetente, havi vagy évente, attól függően, hogy milyen gyakran van szükség a frissítésekre.

3. A szervezetnek meg kell határoznia, milyen információkat kell igény szerint létrehoznia. Ez magában foglalhatja a különböző adatokat, dokumentumokat, jelentéseket stb.

4. A szervezetnek be kell állítania egy EIR-t, amely képes automatikusan létrehozni ezeket az információkat, amikor szükség van rájuk.

5. A szervezetnek rendszeresen ellenőriznie kell az EIR-ben tárolt információkat, hogy meghatározza, melyek azok, amelyekre már nincs szükség.

6. A szervezetnek be kell állítania egy EIR-t, amely képes automatikusan törölni azokat az információkat, amelyekre már nincs szükség.
7. A szervezetnek naplót kell vezetnie minden frissítésről, létrehozásról és törlésről, hogy nyomon követhető legyen az EIR használata és a kiberbiztonsági követelményeknek való megfelelés.

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

SI-14(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

18.76. NEM ÁLLANDÓ KAPCSOLATOK LÉTREHOZÁSA

18.76. A szervezet igény szerint rendszerkapcsolatokat hoz létre és megszakítja a kapcsolatokat, ha egy kérést teljesíteni kell, vagy ha adott ideig nem használták a kapcsolatokat.

MAGYARÁZAT

Az állandó kapcsolatok az EIR-ekkel lehetőséget adnak a fejlett ellenfeleknek arra, hogy laterálisan mozogjanak az EIR-eken keresztül és potenciálisan közelebb kerüljenek az értékes információkhoz vagy elemekhez. Az ilyen kapcsolatok folyamatos rendelkezésre állásának korlátozása akadályozza a támadó azon képességét, hogy szabadon mozogjon a szervezeti EIR-eken keresztül.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az EIR-k közötti kapcsolatokat, amelyeket igény szerint létrehozhat vagy megszakíthat. Ez magában foglalja a kapcsolatok típusának, céljának és időtartamának meghatározását.
2. A szervezetnek implementálnia kell egy rendszert, amely képes kezelni a kapcsolatok létrehozását és megszakítását. Ez magában foglalhatja a kapcsolatok automatikus létrehozását és megszakítását bizonyos feltételek alapján, például, ha egy kérés teljesítésre kerül, vagy ha a kapcsolatot egy adott időn keresztül nem használták.
3. A szervezetnek biztosítania kell, hogy a kapcsolatok létrehozása és megszakítása megfelelően naplózásra kerüljön. Ez lehetővé teszi a szervezet számára, hogy nyomon követhesse a kapcsolatok használatát, és szükség esetén reagálhasson a rendellenességekre.
4. A szervezetnek rendszeresen felül kell vizsgálnia a kapcsolatok használatát, hogy biztosítsa azok megfelelő kezelését. Ez magában foglalhatja a nem használt kapcsolatok megszakítását, valamint a szükségtelenül hosszú ideig tartó kapcsolatok megszakítását.
5. A szervezetnek folyamatosan frissítenie és finomítania kell a kapcsolatkezelési eljárásait, hogy megfeleljen a változó körülményeknek és fenyegetéseknek. Ez magában foglalhatja az új kapcsolatok létrehozás szabályainak bevezetését, valamint a meglévő szabályok felülvizsgálatát.

Kapcsolódó intézkedések

17.46. A hálózati kapcsolat megszakítása

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

SI-14(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

18.77. A KIMENETI INFORMÁCIÓ KEZELÉSE ÉS MEGŐRZÉSE

18.77. A szervezet bizonyos szoftverek és alkalmazások esetén ellenőrzi a kimeneti információkat annak biztosítása érdekében, hogy azok összhangban legyenek az elvárt tartalommal.

MAGYARÁZAT

A számítógépes támadások bizonyos típusai, beleértve az SQL-injekciókat is, olyan kimeneti eredményeket hoznak létre, amelyek váratlanok vagy nem felelnek meg a szoftvertől vagy alkalmazástól elvárt kimeneti eredményeknek. Ez az intézkedés kiegészítés, az információk kimeneti szűrése az idegen tartalom észlelésére összpontosít, megakadályozva az ilyen idegen tartalmak megjelenítését, és figyelmezteti a felügyeleti eszközöket a felfedezett rendellenes viselkedésről.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely szoftverek és alkalmazások esetében szükséges az információk kimeneti ellenőrzése. Ez magában foglalhatja a kritikus üzleti alkalmazásokat, a hálózati eszközöket és más EIR-eket, amelyek érzékeny adatokat kezelnek vagy tárolnak.
2. A szervezetnek alkalmaznia kell egy kimeneti szűrőrendszert, amely képes azonosítani és blokkolni az elvárttól eltérő tartalmat. Ez magában foglalhatja a szokatlan karaktereket, a nem várt adatformátumokat és a potenciálisan káros kódokat.
3. Az EIR-nek képesnek kell lennie arra, hogy riasztásokat küldjön a felügyeleti eszközöknek, amikor anomália észlelhető. Ez lehetővé teszi a szervezet számára, hogy gyorsan reagáljon a potenciális biztonsági eseményekre.
4. A szervezetnek naplózni kell az összes kimeneti ellenőrzés eredményét. Ez lehetővé teszi a szervezet számára, hogy nyomon kövesse a rendszer viselkedését, és azonosítsa a visszaéléseket vagy a rendellenes működést.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kimeneti szűrőrendszerét, hogy biztosítsa annak hatékonyságát és relevanciáját. Ez magában foglalhatja a szűrési szabályok frissítését, a riasztási küszöbök módosítását és a monitoring eszközök konfigurációjának finomítását.

6. Végül, de nem utolsósorban, a szervezetnek képzést kell biztosítania a munkatársak számára a kimeneti információk ellenőrzésének fontosságáról és a szűrőrendszer használatáról. Ez segít abban, hogy a munkatársak megértsék a rendszer működését, és képesek legyenek hatékonyan reagálni a riasztásokra.

Kapcsolódó intézkedések

18.8. Kártékony kódok elleni védelem

18.13. Az EIR monitorozása

18.66. Hibakezelés

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

3.3.11.12. A kimeneti információ kezelése és megőrzése: Az érintett szervezet az elektronikus információs rendszer kimeneti információit a jogszabályokkal, szabályzatokkal és az üzemeltetési követelményekkel összhangban kezeli és őrzi meg.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SI-15

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a szoftver programok és alkalmazások meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

18.78. MEMÓRIAVÉDELEM

18.78. A szervezet meghatározott védelmi intézkedéseket alkalmaz annak érdekében, hogy megvédje a rendszermemóriát a jogosulatlan kódok végrehajtásától.

MAGYARÁZAT

Egyes támadók olyan módon indíthatnak támadásokat, amelyek célja kód futtatása a memória nem erre kijelölt területein, vagy tiltott memóriahelyeken. A memória védelme érdekében alkalmazott biztonsági biztosítékok közé tartozik például a DEP (Data Execution Prevention) és az ASLR (Address Space Layout Randomization). A DEP-et végrehajtó intézkedések lehetnek hardveresen vagy szoftveresen kikényszerítettek, a hardveres kikényszerítés a mechanizmus nagyobb erősségét biztosítja.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a védelmi intézkedéseket, amelyeket alkalmazni kíván a jogosulatlan kódok végrehajtásának megakadályozása érdekében az EIR memóriájában.
2. A szervezetnek olyan ellenőrző mechanizmusokat kell bevezetnie, mint a Data Execution Prevention (DEP) és az Address Space Layout Randomization (ASLR). A DEP megakadályozza a kódok végrehajtását a nem végrehajtható memóriaterületeken, míg az ASLR véletlenszerűen rendezi el a memóriaterületeket, ami megnehezíti a támadók számára a kártékony kódok végrehajtását.
3. A DEP ellenőrző mechanizmus lehet hardver-alapú vagy szoftver-alapú. A szervezetnek a hardver-alapú DEP-et javasolt alkalmaznia, mivel ez erősebb védelmet nyújt.
4. A szervezetnek rendszeresen naplót kell vezetnie az EIR memóriájának használatáról, hogy nyomon követhesse a jogosulatlan kódok végrehajtásának kísérleteit.
5. A szervezetnek továbbá biztosítania kell, hogy a védelmi intézkedések frissítve legyenek a legújabb fenyegetések elleni védekezés érdekében.
6. A szervezetnek rendszeres időközönként felül kell vizsgálnia és értékelnie kell a védelmi intézkedéseket, hogy biztosítsa azok hatékonyságát.

Kapcsolódó intézkedések

2.129. Referenciának való megfelelőség vizsgálata

17.4. Biztonsági funkciók elkülönítése

18.42. Szoftver- és információsértetlenség

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

3.3.11.13. Memóriavédelem: Az elektronikus információs rendszerben biztonsági beállításokat kell alkalmazni azért, hogy védje a memóriát a jogosulatlan kódok végrehajtásától.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

SI-16

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági követelmények meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

18.79. HIBA ESETÉN ALKALMAZANDÓ BIZTONSÁGI ELJÁRÁSOK

18.79. A szervezet meghatározott meghibásodások bekövetkezésekor a szervezet által meghatározott hibaelhárító eljárásokat hajt végre.

MAGYARÁZAT

A meghibásodási körülmények közé tartozik a kritikus rendszerelemek közötti vagy a rendszerelemek és az üzemeltetési létesítmények közötti kommunikáció elvesztése. A hibaelhárító eljárások közé tartozik az üzemeltető személyzet riasztása és a további lépésekre vonatkozó konkrét utasítások megadása. A további lépések közé tartozhat a semmittevés, a rendszerbeállítások helyreállítása, a folyamatok leállítása, a rendszer újraindítása vagy a kijelölt szervezeti személyzettel való kapcsolatfelvétel.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell a kritikus rendszerelemeket és azok kommunikációját az üzemeltetési létesítményekkel.
2. A szervezetnek meg kell határoznia a potenciális meghibásodásokat, amelyek befolyásolhatják az EIR működését.
3. Ki kell dolgozni a hibaelhárító eljárásokat, amelyeket a meghibásodások esetén alkalmazni kell. Ezeknek az eljárásoknak tartalmazniuk kell az üzemeltető személyzet értesítését és konkrét utasításokat a következő lépésekről.
4. A hibaelhárító eljárások további lépései a következők lehetnek: az, hogy semmit nem teszünk, visszaállítjuk a rendszerbeállításokat, leállítjuk a folyamatokat, újraindítjuk a rendszert, vagy kapcsolatba lépünk a szervezet által kijelölt személyzettel.
5. A szervezetnek a hibaelhárító eljárásokat dokumentálnia kell és rendszeresen felül kell vizsgálnia, hogy biztosítsák azok hatékonyságát és relevanciáját.

KAPCSOLÓDÓ INTÉZKEDÉSEK

7.48. Átállás biztonságosüzemmódra

7.49. Alternatív biztonsági mechanizmusok alkalmazása

17.77. Ismert állapot való meghibásodás

18.68. Előrelátható meghibásodás megelőzése

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

SI-17

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a meghibásodási feltételek és a hozzájuk tartozó hibaelhárító eljárásokra vonatkozó lista meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.80. ADATSZIVÁRGÁS ÉSZLELÉSÉNEK TÁMOGATÁSA

18.80. A szervezet adatokat vagy funkciókat ágyaz be a meghatározott EIR-ekbe vagy rendszerelemekbe, annak megállapítására, hogy a szervezeti adatokat kiszivárogtatták-e vagy jogosulatlanul eltávolították-e azokat a szervezetből.

MAGYARÁZAT

Számos kibertámadás a szervezeti információkat vagy a szervezet által más szervezetek nevében tárolt információkat (pl. személyes adatokat) veszi célba, és ezeket az adatokat kiszivárogtatja. Ezenkívül a belső támadások és a hibás felhasználói eljárások olyan információkat is eltávolíthatnak, kiszivárogtathatnak az EIR-ből, amelyek sértik a szervezeti irányelveket. A beszennyezési megközelítések a passzívtól az aktívig terjedhetnek. Egy passzív szennyezési módszer akár annyiból is állhat, hogy fiktív, erre a célra létrehozott e-mail címeket adunk hozzá egy belső adatbázishoz. Ha a szervezet a hamis e-mail címek valamelyikére e-mailt kap, akkor tudja, hogy az adatbázis védelme sérült. A szervezet továbbá tudja, hogy az e-mailt egy illetéktelen szervezet küldte, így az abban szereplő csomagok potenciálisan rosszindulatú kódot tartalmaznak, és hogy az illetéktelen szervezet potenciálisan megszerezhette az adatbázis másolatát. Egy másik szennyezési módszer lehet hamis adatok vagy steganográfiai adatok beágyazása a fájlokban, hogy az adatok nyílt forráskódú elemzéssel megtalálhatók legyenek. Végül, az aktív szennyezési módszer magában foglalhatja az adatokba olyan szoftver beágyazását, amely képes hazatelefonálni, és ezáltal figyelmeztetni a szervezetet az adatok megszerzésére, és esetleg a helyére, valamint arra az útra, amelyen keresztül az adatokat kiszivárogtatták vagy eltávolították.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, mely EIR-ekbe vagy rendszerelemekbe szeretné beágyazni a "szennyezett" adatokat vagy funkciókat (data tainting).
2. Ezután a szervezetnek ki kell dolgoznia egy "szennyezési" stratégiát, amely lehet passzív vagy aktív. A passzív szennyezési megközelítés lehet egyszerű, mint fiktív, erre a célra létrehozott e-mail címek és nevek hozzáadása egy belső adatbázishoz. Ha a szervezet e-mailt kap egyik hamis e-mail címén, tudja, hogy az adatbázist kompromittálták.

3. A szervezetnek további szennyezési megközelítéseket is be kell vezetnie, mint például hamis adatok vagy szteganográfiai adatok beágyazása a fájlokba, hogy az adatokat nyílt forrású elemzéssel kereshetőek legyenek.
4. Végül, az aktív szennyezési megközelítés magában foglalhatja olyan szoftver beágyazását az adatokba, amely képes "haza telefonálni", így értesítve a szervezetet az adatszivárgásról, és esetleg annak helyéről, valamint az útról, amelyen keresztül az adatokat kiszivárogtatták vagy eltávolították.
5. A szervezetnek naplót kell vezetnie minden ilyen tevékenységről, hogy nyomon követhesse a potenciális adatszivárgásokat és jogosulatlan eltávolításokat.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a szennyezési stratégiáit, hogy biztosítsa azok hatékonyságát és relevanciáját a változó kiberbiztonsági fenyegetésekkel szemben.

Kapcsolódó intézkedések

4.44. Információk kiszivárgásának figyelemmel kísérése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.8.12

NIST SP 800-53 rev.5 referencia

SI-20

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a rendszerek vagy rendszerelemek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

18.81. INFORMÁCIÓFRISSÍTÉS

18.81. A szervezet adott gyakorisággal frissíti a meghatározott információkat vagy előállítja a szükséges információkat és eltávolítja azokat, amennyiben már nincs rájuk szükség.

MAGYARÁZAT

Az információknak a szükségesnél hosszabb ideig történő megőrzése egyre értékesebb és vonzóbb célponttá teszi azokat a támadók számára. Ha az információkat a szervezeti ügymeneti vagy üzleti funkciók támogatásához szükséges minimális ideig tesszük elérhetővé, az csökkenti a támadók lehetőségét az információk kompromittálására, megszerzésére és kiszivárogtatására.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, mely információkra van szüksége, és milyen gyakran kell ezeket frissíteni. Ez magában foglalhatja a különböző adatok, dokumentumok, jelentések és egyéb információk azonosítását, amelyeket az EIR kezel.
2. A szervezetnek be kell állítania egy rendszert vagy folyamatot, amely lehetővé teszi az információk rendszeres frissítését. Ez magában foglalhatja a frissítések ütemezését, a frissítési folyamatok meghatározását, és a felelős személyek vagy csapatok kijelölését.
3. A szervezetnek biztosítania kell, hogy az információk frissítése során az EIR megfelelően működik, és a frissítések pontosak és időben történnek.
4. A szervezetnek rendszeresen ellenőriznie kell az EIR-t, hogy biztosítsa az információk pontosságát és relevanciáját. Ez magában foglalhatja a naplók ellenőrzését, a hibák vagy eltérések azonosítását, és a szükséges javítások elvégzését.
5. A szervezetnek el kell távolítania azokat az információkat az EIR-ből, amelyek már nem szükségesek. Ez magában foglalhatja az elavult vagy felesleges információk azonosítását, és a megfelelő törlési folyamatok végrehajtását.
6. A szervezetnek biztosítania kell, hogy ezek a folyamatok megfelelően dokumentálva vannak, és rendszeresen felülvizsgálják őket a hatékonyság és a megfelelőség érdekében.

KAPCSOLÓDÓ INTÉZKEDÉSEK

18.73. Nem állandó rendszerelemek és szolgáltatások

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.10

NIST SP 800-53 REV.5 REFERENCIA

SI-21

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az információ illetve a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.82. INFORMÁCIÓ DIVERZITÁS

18.82. A szervezet:

18.82.1. meghatározza és azonosítja az alternatív információforrásokat a szervezet működése szempontjából kritikus funkciók és szolgáltatások számára; és

18.82.2. egy alternatív információforrást használ a szervezet működése szempontjából kritikus funkciók vagy szolgáltatások végrehajtásához a meghatározott EIR-ek vagy rendszerelemek esetén, amikor az elsődleges információforrás sérült vagy nem elérhető.

MAGYARÁZAT

A rendszerszolgáltatások vagy funkciók által végrehajtott tevékenységek gyakran az általuk kapott információk alapján működnek. Az információ sérülése, hamisítása, módosítása vagy törlése befolyásolhatja a szolgáltatás vagy funkció képességét a szándékolt tevékenységek megfelelő végrehajtásában. Több információforrás használatával a szolgáltatás vagy funkció folytathatja a működést, ha egyik információforrás megrongálódik vagy már nem elérhető. Lehetséges, hogy az alternatív információforrások kevésbé pontosak vagy kevésbé megbízhatóak, mint az elsődleges információforrás, azonban a kevésbé optimális információforrások is elégséges minőséget biztosíthatnak ahhoz, hogy az alapvető szolgáltatás vagy funkció - akár csökkentett vagy gyengített módon - végrehajtható legyen.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet meghatározza a szervezet működése szempontjából kritikus funkciókat és szolgáltatásokat.

2. A szervezet meghatározza az alternatív információforrásokat a szervezet működése szempontjából kritikus funkciók és szolgáltatások számára.

3. Amennyiben szükséges, a szervezet az alternatív információforrásokat használja a szervezet működése szempontjából kritikus funkciókat és szolgáltatásokat biztosító rendszerek, vagy rendszerelemek elsődleges információforrásának sérülése esetén.

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

SI-22

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

18.83. FRAGMENTÁLT INFORMÁCIÓ

18.83. A szervezet meghatározott körülmények esetén:

18.83.1. a meghatározott információt fragmentálja; és

18.83.2. a fragmentált információt szétosztja a meghatározott EIR-ek és rendszerelemek között.

MAGYARÁZAT

Az APT (advanced persistent threat) csoportok egyik célja az értékes információ kiszivárogtatása. Miután ez megtörtént, az érintett szervezet általában nem képes visszaszerezni az elveszett információt. Ezért a szervezetek fontolóra vehetik az információ különböző elemekre bontását és ezeknek az elemeknek a szétosztását több rendszeren és rendszerelemen, valamint helyszínek között. Az ilyen lépések növelik az ellenfél munkamennyiségét a kívánt információ megszerzéséhez és kiszivárogtatásához, és ezzel növelik a felismerésük valószínűségét. Az információ fragmentálása ugyanakkor befolyásolja a szervezet képességét arra, hogy időben hozzáférjen az információhoz. A fragmentálás mértékét az információ értéke vagy besorolási szintje, a kapott fenyegetési hírszerzési információk, az adatok szándékos "szennyezettsége" (data tainting) határozza meg. (azaz az adatok szennyezéséből származó információk az egyes információk kiszivárogtatásáról eredményezhetik a maradék információ fragmentálását).

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a fragmentálásra szoruló információt.

2. A szervezet meghatározza, hogy milyen rendszerek és rendszerelemek és helyszínek között ossza szét a fragmentált információt.

3. A szervezet meghatározza, hogy mely körülmények esetén szükséges az információ fragmentálás és szétosztása.

4. A szervezet alkalmazza a meghatározott intézkedéseket a meghatározott elemekre és a meghatározott körülmények esetén.

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

SI-23

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a körülmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024