Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Naplózás és elszámoltathatóság

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

4.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

4.1. A szervezet:

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

4.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó naplózásra és elszámoltathatóságra vonatkozó szabályzatot, amely

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

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

4.1.1.2. a naplózási és elszámoltathatósági eljárásrendet, amely a naplózásra és elszámoltathatóságra vonatkozó szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

4.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki a naplózásra és elszámoltathatóságra vonatkozó szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

4.1.3. Felülvizsgálja és frissíti az aktuális naplózásra és elszámoltathatóságra vonatkozó szabályzatot és a naplózási és elszámoltathatósági eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

MAGYARÁZAT

A naplózást és elszámoltathatóságot magában foglaló szabályzatnak és a kapcsolódó eljárásrend(ek)nek illeszkednie kell az érintett szervezet kockázatkezelési stratégiájához. A megfelelő minőségben és megfelelő szempontok mentén elkészített szabályzatok és eljárásrendek nagy mértékben járulnak hozzá a szervezet biztonságának megőrzéséhez. Az elkészült szabályzatoknak és eljárásrendeknek összhangban kell lenniük egymással és a szervezet információbiztonsági környezetével. A szervezeti szintű biztonsági szabályzatok és eljárásrendek használata általában előnyösebb, hiszen szükségtelenné teheti a különböző szervezeti célok vagy rendszerek szintjén kialakítandó szabályzatokat és eljárásrendeket. A

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

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

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

6. A szervezetnek felül kell vizsgálnia és szükség esetén frissítenie kell az aktuális naplózást és elszámoltathatóságot magában foglaló szabályzatot/szabályokat, illetve a kapcsolódó eljárásrendeket a szervezet által meghatározott gyakorisággal, valamint a szervezet által meghatározott események bekövetkezését követően.

KAPCSOLÓDÓ INTÉZKEDÉSEK

1.10. Kockázatkezelési stratégia

14.12. Fegyelmi intézkedések

18.67. Információ kezelése és megőrzése

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

3.3.12.1. Naplózási 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

AU-1

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

4.2. NAPLÓZHATÓ ESEMÉNYEK

4.2. A szervezet:

4.2.1. Meghatározza a naplózható és naplózandó eseményeket, és felkészíti erre az EIR-t.

4.2.2. Egyezteti a naplózási elvárásokat a naplózási információt igénylő szervezeti egységekkel, hogy iránymutatással és információkkal segítse a naplózandó események kiválasztását.

4.2.3. Meghatározza az EIR-en belül naplózandó eseménytípusokat, és az azokhoz kapcsolódó gyakoriságot vagy az azt szükségessé tevő eseményeket.

4.2.4. Indokolja, hogy a kiválasztott eseménytípusok, miért alkalmasak a biztonsági események utólagos kivizsgálásának támogatására;

4.2.5. Meghatározott gyakorisággal felülvizsgálja és frissíti a naplózásra kiválasztott eseménytípusokat.

MAGYARÁZAT

Azok az eseménytípusok igényelnek naplózást az EIR-ben, amelyek jelentősek és relevánsak az EIR biztonsága szempontjából. Az események naplózása támogatja a specifikus monitorozási és naplózási igényeket is. A naplózandó eseménytípusok közé tartoznak pl. a jelszóváltozások, a sikeres vagy sikertelen bejelentkezési kísérletek, a biztonsági funkciókhoz kapcsolódó sikertelen hozzáférések, a privilegizált jogosultságok használata, a hitelesítő adatok használata, az adatműveletek változásai, illetve a bizalmas adatokhoz kapcsolódó lekérdezések. Az események naplózásának követelményei, beleértve a specifikus eseménytípusok naplózásának szükségességét, számos más védelmi intézkedés kapcsán megjelennek. A naplóbejegyzések különböző szinteken generálhatók, beleértve a csomagszintet is, ahogy az információ áthalad a hálózaton. Az eseménynaplózás megfelelő szintjének kiválasztása fontos része a monitorozási és naplózási képességnek, és segíthet azonosítani a problémák gyökérokait. Az egyes naplózandó események a szervezet igényei alapján idővel változhatnak. Például a szervezet meghatározza, hogy az EIR-nek képesnek kell lennie naplózni minden sikeres és sikertelen fájlhozzáférést, azonban ezt a funkciót nem kapcsolja be a szervezet, mivel negatívan hatna az EIR teljesítményére. Ezért fontos, hogy a szervezet időről-időre felülvizsgálja és szükség esetén frissítse a naplózandó eseményeket annak érdekében, hogy azok továbbra is relevánsak legyenek és támogassák a szervezeti igények megvalósulását. A naplózandó és naplózható eseményekkel kapcsolatos biztonsági követelmények a "Fiókkezelés

– Automatikus naplózási műveletek", a "Hozzáférési szabályok érvényesítése – Hozzáférés-ellenőrző mechanizmusok ellenőrzött felülbírálata", a "Legkisebb jogosultság elve – Privilegizált funkciók használatának naplózása", a "Távoli hozzáférés – Felügyelet és irányítás", a "A konfigurációváltozások felügyelete (változáskezelés)", a "A változtatásokra vonatkozó hozzáférés korlátozások – Automatizált hozzáférés-érvényesítés és naplóbejegyzések", az "Eszközök azonosítása és hitelesítése – Dinamikus címkiosztás", a "Távoli karbantartás – Naplózás és felülvizsgálat", az "Adathordozók tárolása – Automatizált korlátozott hozzáférés", a "A fizikai belépés ellenőrzése", a "A határok védelme – Hálózati privilegizált hozzáférések", a "Kártékony kódok elleni védelem – Jogosulatlan parancsok észlelése", a "Az EIR monitorozása – Engedély nélküli hálózati szolgáltatások", a "Szoftver- és információsértetlenség – Naplózás és riasztás", a "Bemeneti információ ellenőrzés – Manuális felülírási képesség" kontrolloknál is kifejtésre kerültek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a naplózható és naplózandó eseményeket, és fel kell készítenie az EIR-t erre a feladatra.
2. A szervezetnek egyeztetnie kell a naplózási elvárásokat a naplózási információt igénylő szervezeti egységekkel, hogy minden szükséges információ rendelkezésre álljon a naplókban.
3. A szervezetnek meg kell határoznia az EIR-en belül naplózandó eseménytípusokat, és az azokhoz kapcsolódó gyakoriságot vagy az azt szükségessé tevő eseményeket.
4. A szervezetnek úgy kell meghatároznia a naplózandó eseményeket, hogy azok ne akadályozzák az EIR szervezeti célok eléréséhez szükséges teljesítményét.
5. A szervezetnek meghatározott gyakorisággal felül kell vizsgálnia és szükség esetén frissítenie kell a naplózásra kiválasztott eseménytípusokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

2.60. Legkisebb jogosultság elve

2.71. Sikertelen bejelentkezési kísérletek

2.75.1. A rendszerhasználat jelzése

2.89. Biztonsági tulajdonságok

2.100. Távoli hozzáférés

4.3. Naplóbejegyzések tartalma

4.5. Naplózás tárkapacitása

4.7. Naplózási hiba kezelése

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

3.3.12.2. Naplózható események

ISO/IEC 27001:2023 REFERENCIA

A.8.15

NIST SP 800-53 REV.5 REFERENCIA

AU-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

4.3. NAPLÓBEJEGYZÉSEK TARTALMA

4.3. A szervezet biztosítja, hogy a naplóbejegyzésekből az alábbi információk megállapíthatóak legyenek:

4.3.1. milyen típusú esemény történt;

4.3.2. mikor történt az esemény;

4.3.3. hol történt az esemény;

4.3.4. miből származott az esemény; és

4.3.5. mi volt az eseménynek a kimenetele, valamint

4.3.6. az eseményhez kapcsolódó személyek, alanyok, objektumok.

MAGYARÁZAT

A naplózás funkciót támogató tartalom magában foglalhatja az esemény leírását, az időbélyegeket, forrás és cél címeket, felhasználói vagy végrehajtó folyamat azonosítókat, a sikeres vagy sikertelen végrehajtásra vonatkozó információkat, és az érintett fájlneveket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy a naplóbejegyzések tartalmazzák az események leírását. Ez lehetővé teszi, hogy megállapíthassák, milyen típusú esemény történt.

2. A naplóbejegyzéseknek időbélyegeket is tartalmazniuk kell, amelyek segítségével meghatározható, mikor történt az esemény.

3. A szervezetnek biztosítania kell, hogy a naplóbejegyzések tartalmazzák a forrás- és célobjektumok címét. Ez lehetővé teszi, hogy megállapíthassák, az esemény forrását és célját.

4. A naplóbejegyzéseknek tartalmazniuk kell a felhasználói vagy a végrehajtói folyamat azonosítóját. Ez lehetővé teszi, annak a megállapítását, hogy az eseményt mely felhasználó vagy mely feldolgozó folyamat hajtotta végre.

5. A szervezetnek biztosítania kell, hogy a naplóbejegyzések tartalmazzák az események kimenetelét.

Kapcsolódó intézkedések

4.2. Naplózható események

4.24. Időbélyegek

4.40. Naplóbejegyzések létrehozása

4.48. Munkaszakasz-ellenőrzés

10.11. Távoli karbantartás

13.9. Központi kezelés

16.16. Biztonságtervezési elvek

18.42. Szoftver- és információsértetlenség

18.66. Hibakezelés

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

3.3.12.3. Naplóbejegyzések tartalma

ISO/IEC 27001:2023 referencia

A.5.28; A.8.15

NIST SP 800-53 rev.5 referencia

AU-3

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

4.4. NAPLÓBEJEGYZÉSEK TARTALMA – KIEGÉSZÍTŐ NAPLÓINFORMÁCIÓK

4.4. Az EIR a naplóbejegyzésekben további, a szervezet által meghatározott kiegészítő információkat is rögzít.

MAGYARÁZAT

Az EIR funkcionalitásától függ, hogy a naplóbejegyzések tartalmáta a szervezet képes-e konfigurálni és így lehetséges-e az, hogy a szervezet további információkkal lássa el a naplóbejegyzéseket. A szervezet fontolóra veheti további információk hozzáadását a naplóbejegyzésekhez, beleértve, de nem kizárólag, a hozzáférés-felügyeleti vagy áramlás ellenőrzési szabályokat, amelyek érvényesítésre kerültek, és a csoportfiókok felhasználóinak egyéni azonosítóit. Megfontolandó a kiegészítő információk korlátozása csak azokra az információkra, amelyekre kifejezetten szükség van a naplózási követelmények teljesítéséhez. A túlságosan sok kiegészítő információ megnehezítheti az érdeklődésre számot tartó információk megtalálását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az EIR-nek képesnek kell lennie a naplóbejegyzésekben a minimálisan elvárt információkon túl kiegészítő információk hozzáadására is. Ez az EIR naplózási funkciójának konfigurálhatóságától függ.
2. A szervezet megfontolhatja további információk hozzáadását a naplóbejegyzésekhez, beleértve, de nem kizárólag, az alkalmazott hozzáférés-felügyeleti szabályokat vagy az adatáramlási szabályokat, valamint a csoportfiókok felhasználóinak egyéni azonosítóit.
3. A szervezet megfontolhatja a kiegészítő naplóbejegyzési információ korlátozását csak azokra az információkra, amelyekre kifejezetten szükség van a naplózási követelmények teljesítéséhez. A naplóbejegyzésekben meglévő, szükségesnél több információ ronthatja a naplóelemzési tevékenység hatékonyságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.12.3. Naplóbejegyzések tartalma

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-3(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kiegészítő információ meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

4.5. NAPLÓZÁS TÁRKAPACITÁSA

4.5. A szervezet elegendő méretű tárkapacitást biztosít a naplózásra, figyelembe véve a naplózási funkciókat és a meghatározott megőrzési követelményeket.

MAGYARÁZAT

Az érintett szervezet figyelembe veszi a naplózási típusokat és a naplófeldolgozási követelményeket, amikor a naplók számára fenntartott tárhelykapacitást meghatározza. Elegendő tárkapacitás biztosítása a naplóbejegyzések számára csökkenti annak valószínűségét, hogy a nem megfelelő kapacitás a naplózási képesség elvesztését vagy csökkenését eredményezheti.

A szervezetnek biztosítania kell, hogy az EIR rendelkezzen elegendő tárhellyel a naplózáshoz, figyelembe véve az elvárt naplózási funkciókat és a meghatározott megőrzési követelményeket is. Ez azt jelenti, hogy az EIR-nek képesnek kell lennie arra, hogy kezelje és tárolja az összes naplóbejegyzést, amelyeket a szervezet naplózási szabályzata előír, és teljesíti a szabályozói előírásokat is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek elegendő tárkapacitást kell biztosítania a naplózásra, figyelembe véve a meghatározott naplózási típusokat, illetve funkciókat, valamint a meghatározott megőrzési- és naplófeldolgozási követelményeket.

2. A szervezetnek rendszeresen ellenőriznie kell a naplózásra fenntartott tárkapacitását, annak érdekében, hogy elősegítse a naplózás folyamatos működését. Az ellenőrzés során a szervezetnek meg kell bizonyosodnia arról, hogy a naplóbejegyzések által elfoglalt tárhely nem foglalja el a rendelkezésre álló tárhely adott százalékát.

3. A szervezetnek meg kell terveznie és végre kell hajtania egy naplókezelési stratégiát, amely magában foglalja a naplófájlok rendszeres archiválását és törlését, így biztosítva a tárkapacitás optimális kihasználását, ill. a megőrzési követelményeket is.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.2. Naplózható események

4.7. Naplózási hiba kezelése

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.22. Naplóbejegyzések csökkentése és jelentéskészítés

4.25. Naplóinformációk védelme

4.38. A naplóbejegyzések megőrzése

4.40. Naplóbejegyzések létrehozása

4.48. Munkaszakasz-ellenőrzés

18.13. Az EIR monitorozása

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

3.3.12.4. Napló tárkapacitás: Az érintett szervezet a naplózásra elegendő méretű tárkapacitást biztosít, a biztonsági osztályba sorolásból következő naplózási funkciók figyelembevételével.

ISO/IEC 27001:2023 REFERENCIA

A.8.6

NIST SP 800-53 REV.5 REFERENCIA

AU-4

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a naplók megőrzésére vonatkozó követelmények meghatározása

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

4.6. NAPLÓ TÁRKAPACITÁS – NAPLÓK ÁTVITELE ALTERNATÍV TÁROLÁSI HELYSZÍNRE

4.6. A szervezet meghatározott gyakorisággal továbbítja a naplóbejegyzéseket a forrásrendszerből vagy rendszerelemből egy különálló rendszerbe, rendszerelembe vagy tárolórendszerbe.

MAGYARÁZAT

A naplók átvitele, más néven a forrásrendszerből vagy rendszerelemből történő áthelyezés gyakori folyamat a korlátozott naplótárolási kapacitással rendelkező rendszerekben, amely így támogatja a naplófájlok hosszabb távú rendelkezésre állását. A kezdeti naplótárolót csak átmenetileg használják, amíg a rendszer nem tud kommunikálni a naplótárolásra kijelölt másodlagos vagy helyettesítő rendszerrel. Amikor ez megtörténik a naplók áthelyezésre kerülnek. A naplók alternatív tárolórendszerbe történő átvitele "A naplóinformációk védelme – Tárolás fizikailag különálló rendszereken vagy rendszerelemeken" védelmi intézkedés követelményeihez hasonlóan történik, mivel a naplókat egy másik helyre viszik át. "A naplóinformációk védelme – Tárolás fizikailag különálló rendszereken vagy rendszerelemeken" védelmi intézkedés alkalmazásának célja azonban a naplóbejegyzések bizalmasságának és sértetlenségének a védelme. A szervezetek választhatják a védelmi intézkedés mindkét megvalósítási módját. Tehát vagy a naplók tárolási kapacitását növelik meg, vagy a naplók és a naplóbejegyzések bizalmasságának, sértetlenségének és rendelkezésre állásának megőrzéséről gondoskodnak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a naplóbejegyzések továbbításának gyakoriságát. Ez a gyakoriság függhet a rendszer leterheltségétől, a naplózott események számától és a naplózás céljától.
2. A szervezetnek ki kell választania egy különálló rendszert, rendszerelemet vagy tárolórendszert, ahova a naplóbejegyzéseket továbbítja. Ez a rendszer lehet egy másik szerver, egy felhő alapú tároló vagy egy másik, a naplózást támogató infrastruktúra.

3. A szervezetnek be kell állítania a forrásrendszert vagy rendszerelemet, hogy a meghatározott gyakorisággal továbbítsa a naplóbejegyzéseket a kiválasztott rendszerbe, rendszerelembe vagy tárolórendszerbe. Ez magában foglalhatja a naplóbejegyzések automatikus továbbításának beállítását, vagy a naplóbejegyzések manuális továbbításának ütemezését.

4. A szervezetnek biztosítania kell, hogy a naplóbejegyzések továbbítása során a naplóbejegyzések bizalmassága, sértetlensége és rendelkezésre állása megmarad. Ez magában foglalhatja a naplóbejegyzések titkosítását a továbbítás során, és a naplóbejegyzések biztonságos tárolását a cél rendszerben, rendszerelemben vagy tárolórendszerben.

5. Végül, az érintett szervezetnek rendszeresen ellenőriznie kell a naplóbejegyzések továbbításának folyamatát, hogy biztosítsa a továbbítás hatékonyságát és a naplóbejegyzések biztonságát. Ez magában foglalhatja a továbbítás gyakoriságának felülvizsgálatát, a továbbítás során felmerülő hibák nyomon követését és a naplóbejegyzések biztonságának ellenőrzését a cél rendszerben, rendszerelemben vagy tárolórendszerben.

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

AU-4(1)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

4.7. NAPLÓZÁSI HIBA KEZELÉSE

4.7. A szervezet naplózási hiba esetén:

4.7.1. Riasztja a meghatározott személyeket vagy szerepköröket a szervezet által meghatározott időn belül.

4.7.2. További meghatározott intézkedéseket hajt végre.

MAGYARÁZAT

A naplózási hibák közé tartoznak a szoftver- és hardverhibák, a naplóbejegyzések rögzítési mechanizmusainak hibái, valamint a naplóbejegyzések tárolókapacitásának a kritikus küszöbértéket meghaladó kihasználása. Az érintett szervezet által meghatározott intézkedések közé tartozhat a legrégebbi naplóbejegyzések felülírása, az EIR leállítása és a naplóbejegyzések generálásának leállítása. A szervezet további intézkedéseket is meghatározhat a naplózási folyamat hibái esetén, a hiba típusa, helye, súlyossága vagy ezek kombinációja alapján.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell alakítania egy naplózási hibakezelő megoldást, amely képes azonosítani a naplózási tevékenységhez kapcsolódó szoftver- és hardverhibákat, vagy a naplóbejegyzések rögzítési mechanizmusának hibáit, valamint a napló tárolókapacitásra vonatkozó kritikus kihasználási szint elérését.
2. A szervezetnek meg kell határoznia a teendőket a naplózási folyamat hibái esetén. Ezek az intézkedések tartalmazhatják a legrégebbi naplóbejegyzések felülírását, az EIR leállítását, vagy a naplóbejegyzések generálásának leállítását.
3. A szervezetnek további intézkedések meghozatalára is szükség lehet a naplózási folyamat hibái esetén, figyelembe véve a hiba típusát, helyét, súlyosságát vagy ezek kombinációját.
4. A szervezetnek nyilvántartást kell vezetnie az összes riasztásról, hogy nyomon követhesse a hibaeseményeket és a válaszintézkedéseket. A nyilvántartás segíthet az érintett szervezetnek felismerni a mintázatokat, értékelni a riasztási rendszer hatékonyságát és továbbfejleszteni a biztonsági követelményeket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.2. Naplózható események

4.5. Naplózás tárkapacitása

4.22. Naplóbejegyzések csökkentése és jelentéskészítés

4.25. Naplóinformációk védelme

4.38. A naplóbejegyzések megőrzése

4.40. Naplóbejegyzések létrehozása

4.48. Munkaszakasz-ellenőrzés

18.13. Az EIR monitorozása

18.67. Információ kezelése és megőrzése

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

3.3.12.5. Naplózási hiba kezelése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-5

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

4.8. NAPLÓZÁSI HIBA KEZELÉSE – TÁRHELYKAPACITÁS FIGYELMEZTETÉS

4.8. Az EIR a szervezet által meghatározott időn belül figyelmezteti a meghatározott személyeket, szerepköröket és helyszíneket, ha a lefoglalt naplózási tárhely eléri a maximális naplózási tárhely szervezet által meghatározott százalékos értékét.

MAGYARÁZAT

A szervezet rendelkezhet több naplózásra fenntartott tárhellyel, melyeket több rendszerkomponens között oszt el. Az egyes tárhelyek különböző tárhelykapacitással rendelkezhetnek.

Amikor egy rendszerkomponens naplózási tárhelye eléri a maximális kapacitás egy bizonyos százalékát - amit a szervezet határoz meg - az EIR a szervezet által meghatározott időn belül értesíti a meghatározott személyeket, szerepköröket és/vagy helyszíneket. Ez annak biztosítására szolgál, hogy a szervezet értesüljön a naplózási tárhelykapacitás korlátjáról, és megtehesse a szükséges intézkedéseket annak megelőzésére, hogy az EIR naplózási funkciója tárhely hiánya miatt megszakadjon.

Az EIR maga is képes lehet a naplótárolás automatikus kezelésére, olyan stratégiák alkalmazásával, mint a naplórotáció és a naplóarchiválás, így biztosítva a naplózási funkció folyamatos működését.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a maximális naplózási tárhely százalékos értékét, ami azt a küszöböt jelenti, amikor a naplózási tárhely elér egy bizonyos szintet. Amennyiben ez megtörténik, az EIR-nek figyelmeztetést kell küldenie a meghatározott személyeknek, szerepköröknek és/vagy helyszíneknek.
2. A szervezetnek úgy kell beállítania az EIR-t, hogy folyamatosan figyelje a naplózási tárhely aktuális kihasználtságát.
3. A szervezetnek meg kell határoznia a figyelmeztetés küldésére vonatkozó szabályokat az EIR-ben. Ez magában foglalja a figyelmeztetés küldésének időpontját, illetve az értesítendő személyeket, szerepkört és/vagy helyszíneket.

4. A szervezetnek folyamatosan követnie kell az EIR figyelmeztetéseit, hogy biztosítsa a naplózási tárhely optimális kihasználtságát és a naplózás folyamatos működését.
5. A szervezetnek nyilvántartást kell vezetnie az összes riasztásról, hogy nyomon követhesse a hibaeseményeket és a válaszintézkedéseket. A nyilvántartás segíthet az érintett szervezetnek felismerni a mintázatokat, értékelni a riasztási rendszer hatékonyságát és továbbfejleszteni a biztonsági követelményeket.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

3.3.12.5. Naplózási hiba kezelése

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AU-5(1)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a személyek, szerepek és helyszínek illetve az idő intervallum meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	X

4.9. NAPLÓZÁSI HIBA KEZELÉSE – VALÓS IDEJŰ RIASZTÁSOK

4.9. Az EIR riasztást küld a meghatározott személyeknek vagy szerepköröknek, ha a meghatározott, valós idejű riasztást igénylő hibaesemények közül bármelyik bekövetkezik.

MAGYARÁZAT

A riasztások sürgős üzenetek a szervezet részére. A valós idejű riasztások az esemény detektálását követően néhány másodpercen belül vagy még annál is gyorsabban elküldik a riasztást tartalmazó üzenetet. Ezek a riasztások kritikus fontosságúak lehetnek a szervezet számára, mivel lehetővé teszik, hogy a szervezet gyorsan reagáljon a potenciálisan kártékony eseményekre, és ezáltal minimalizálni lehessen a lehetséges károkat. A valós idejű riasztások alapján a szervezet képes lehet azonosítani a gyakori hibaeseményeket, és megteheti a szükséges intézkedéseket a hasonló események megelőzésére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely hibaesemények igényelnek valós idejű riasztást. Ezek olyan események, melyek jelentős kockázatot jelentenek az EIR biztonságára vagy működésére nézve.
2. Miután a szervezet meghatározta a riasztást igénylő hibaeseményeket, a szervezetnek meg kell határoznia a riasztások címzettjeit. Ezek lehetnek konkrét személyek, például a szervezet elektronikus információs rendszer biztonságáért felelős munkavállalója, vagy szerepkörök, például a rendszergazdák.
3. Az szervezetnek úgy kell beállítania az EIR-t, hogy automatikusan küldjön valós idejú riasztásokat a meghatározott hibaesemények bekövetkezése esetén.
4. A szervezetnek nyilvántartást kell vezetnie az összes riasztásról, hogy nyomon követhesse a hibaeseményeket és a válaszintézkedéseket. A nyilvántartás segíthet az érintett szervezetnek felismerni a mintázatokat, értékelni a riasztási rendszer hatékonyságát és továbbfejleszteni a biztonsági követelményeket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.12.5. Naplózási hiba kezelése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-5(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a valós idejű periódus illetve a személyek, szerepek és helyszínek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

4.10. NAPLÓZÁSI HIBA KEZELÉSE – KONFIGURÁLHATÓ FORGALMI KÜSZÖBÉRTÉKEK

4.10. A szervezet olyan konfigurálható hálózati kommunikációs forgalmi küszöbértéket alkalmaz, amely megfelel a naplózás tárolási kapacitási korlátjainak és a küszöbérték feletti forgalmat visszautasítja vagy késlelteti.

MAGYARÁZAT

A szervezetnek megvan a képessége arra, hogy elutasítsa vagy késleltesse a hálózati kommunikációs forgalom feldolgozását, ha ez a forgalom meghaladja a naplózás tárolási kapacitásának korlátjait. Az elutasító vagy késleltetési reakciót a szervezet által meghatározott forgalmi mennyiségi küszöbértékek váltják ki, amelyek a naplózás tárolókapacitásának változása alapján módosíthatók.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a hálózati kommunikációs forgalmi küszöbértéket. Ez a küszöbérték a naplózás tárolási kapacitásának függvényében változhat.
2. A szervezetnek olyan konfigurálható hálózati kommunikációs forgalmi küszöbértéket kell alkalmaznia, amely képes visszautasítani vagy késleltetni a forgalmat, ha ez a forgalom meghaladja a naplózás tárolási kapacitásának korlátjait.
3. A szervezetnek rendszeresen ellenőriznie kell a naplózás tárolási kapacitását, és szükség esetén módosítania kell a hálózati kommunikációs forgalmi küszöbértéket.

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

AU-5(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.11. NAPLÓZÁSI HIBA KEZELÉSE – LEÁLLÍTÁS HIBA ESETÉN

4.11. A szervezet meghatározott naplózási hibák esetén kezdeményezi az EIR teljes vagy részleges leállítását, vagy korlátozza az elérhető ügymeneti és üzleti funkciókat, kivéve, ha a szervezet rendelkezik alternatív naplózási képességgel.

MAGYARÁZAT

A szervezet meghatározza a naplózási hibák azon típusait, amelyek automatikus rendszerleállást vagy korlátozott működést válthatnak ki. A szervezeti célok és az üzletmenet folytonosságának biztosításának fontossága miatt a szervezetek meghatározhatják, hogy a naplózási hiba jellege nem olyan súlyos, hogy az indokolná a szervezeti működési célokat és az alapvető üzleti funkciókat támogató EIR teljes leállítását. Ezekben az esetekben az EIR részleges leállítása vagy csökkentett üzemmódban történő működtetése lehet életszerű alternatíva.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a naplózási hibákat, amelyek az EIR automatikus leállítását vagy csökkentett üzemmódban történő működését váltják ki.
2. A szervezeti működési célok és az alapvető üzleti funkciók folyamatos biztosításának fontossága miatt a szervezet dönthet úgy, hogy a naplózási hiba természete nem olyan súlyos, hogy az indokolná azon EIR teljes leállítását, amely támogatja a szervezet alapvető ügymenetét és üzleti funkcióit. Ilyen esetekben az EIR részleges leállítása vagy a csökkentett üzemmódban történő működés lehetnek életszerű alternatívák.
3. A szervezetnek rendelkeznie kell alternatív naplózási képességgel, hogy a meghatározott naplózási hibák minél kevésbé befolyásolják az ügymenet és üzleti funkciók normál működését. Amennyiben a szervezet rendelkezik alternatív naplózási képességgel, előfordulhat, hogy naplózási hiba esetén nem kell kezdeményeznie az EIR teljes vagy részleges leállítását, illetve a csökkentett üzemmódra történő áttérést.

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

AU-5(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a naplózási hibák meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.12. NAPLÓZÁSI HIBA KEZELÉSE – ALTERNATÍV NAPLÓZÁSI KÉPESSÉG

4.12. Az EIR alternatív naplózási funkciót biztosít arra az esetre, ha az elsődleges naplózási funkció meghibásodik.

MAGYARÁZAT

Mivel az alternatív naplózási képesség rövid távú védelmi megoldás lehet, amelyet az elsődleges naplózási képesség hibájának kijavításáig alkalmaznak, a szervezet meghatározhatja, hogy az alternatív naplózási képességnek csak az elsődleges naplózási funkciónak a hiba által érintett részét kell ellátnia. Az alternatív naplózási funkció lényege, hogy biztosítja az EIR folyamatos működését és a naplók elérhetőségét, még akkor is, ha az elsődleges naplózási funkció meghibásodik. Ez kritikus fontosságú lehet, mivel a naplók fontos információkat tartalmaznak az EIR működéséről, beleértve a potenciális biztonsági eseményeket és a rendszerhasználati mintákat.

Az alternatív naplózási funkció használata azt is lehetővé teszi a szervezet számára, hogy gyorsan reagáljon a hibákra és minimalizálja a szolgáltatás kiesését. Az alternatív naplózási funkció használata segíthet továbbá a hibák diagnosztizálásában és a hibajavításban, mivel a naplók gyakran tartalmaznak részletes információkat a hiba jellegéről és időpontjáról.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR rendelkezzen egy alternatív naplózási funkcióval, amely akkor használatos, ha az elsődleges naplózási funkció meghibásodik.
2. A szervezetnek meg kell határoznia, hogy milyen esetekben tekinti hibásnak az elsődleges naplózási funkciót. Ez lehet például a naplózási funkció teljes leállása, vagy a naplózási funkció teljesítményének jelentős csökkenése.
3. A szervezetnek biztosítania kell, hogy az alternatív naplózási funkció képes legyen legalább a legfontosabb naplózási feladatok elvégzésére, amíg az elsődleges naplózási funkció hibáját ki nem javítják.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.25. Naplóinformációk védelme

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-5(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az alternatív naplózási funkció meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.13. A szervezet:

4.13.1. Meghatározott gyakorisággal felülvizsgálja és elemzi a rendszer naplóbejegyzéseit a nem megfelelő vagy szokatlan tevékenységre utaló jelek és az ilyen tevékenységek lehetséges hatásai szempontjából.

4.13.2. Jelenti ezeket a szervezet által meghatározott személyeknek vagy szerepköröknek.

4.13.3. Módosítja a naplóbejegyzések felülvizsgálatának, elemzésének és jelentésének szintjét, amennyiben hiteles információk és információforrások alapján a kockázat változik.

Magyarázat

A naplóbejegyzések felülvizsgálata, elemzése és jelentése magában foglalja az érintett szervezet által végzett információbiztonsági naplózást, beleértve a fiókok használatának, távoli hozzáférésnek, vezeték nélküli kapcsolatnak, mobil eszköz csatlakozásnak, konfigurációs beállításoknak, a rendszerkomponens leltárának, karbantartó eszközök használatának és nem helyi karbantartásnak, fizikai hozzáférésnek, hőmérsékletnek és páratartalomnak, berendezések szállításának és eltávolításának, az EIR interfészeinél történő kommunikációnak, valamint a mobil kód vagy az internetes hanghívás (VoIP) használatának monitorozásából eredő naplózást. Az eredményeket jelenthetik a szervezet olyan egységeinek, mint a biztonsági eseménykezelő csapat, a helpdesk, valamint a biztonsági szakterület. Ha a szervezetnek megtiltják a naplóbejegyzések felülvizsgálatát és elemzését, vagy képtelen ilyen tevékenységeket végrehajtani, a felülvizsgálatot vagy elemzést más, ilyen felhatalmazással rendelkező szervezet végezheti el. A naplóbejegyzések felülvizsgálatának, elemzésének és jelentésének gyakoriságát, hatókörét és/vagy mélységét a szervezet igényei szerint lehet módosítani az újonnan beérkezett információk alapján.

A követelmény alkalmazásának lépései

1. A szervezetnek először kell határoznia a naplóbejegyzések felülvizsgálatának és elemzésének gyakoriságát. Ez magában foglalja a szervezet által végzett információbiztonsági naplózást, beleértve a fiókok használatának, távoli hozzáférésnek, vezeték nélküli kapcsolatnak, mobil

eszköz csatlakozásnak, konfigurációs beállításoknak, a rendszerkomponens leltárának, karbantartó eszközök használatának és nem helyi karbantartásnak, fizikai hozzáférésnek, hőmérsékletnek és páratartalomnak, berendezések szállításának és eltávolításának, az EIR interfészeinél történő kommunikációnak, valamint a mobil kód vagy az internetes hanghívás (VoIP) használatának monitorozásából eredő naplózást.

2. A szervezetnek jelentenie kell a naplóbejegyzések felülvizsgálatának és elemzésének eredményeit a szervezet által meghatározott személyeknek vagy szerepköröknek. Ez magában foglalhatja a biztonsági eseménykezelő csapatot, a helpdesket, valamint a biztonsági szakterületet.

3. Ha a szervezet nem tudja elvégezni a naplóbejegyzések felülvizsgálatát és elemzését, akkor a felülvizsgálatot vagy elemzést más, ilyen felhatalmazással rendelkező szervezettel végeztetheti el.

4. A szervezetnek módosítania kell a naplóbejegyzések felülvizsgálatának, elemzésének és jelentésének gyakoriságát, hatókörét és/vagy mélységét, ha olyan információk birtokába jut, amelyek ezt indokolttá teszik.

5. A szervezetnek meg kell határoznia a naplóelemzés eredményei alapján szükséges cselekvéseket, és végre kell hajtania ezeket annak érdekében, hogy kezelje az azonosított kiberbiztonsági kockázatokat.

6. A szervezetnek dokumentálnia kell a naplófelülvizsgálati és elemzési folyamatot, beleértve a gyűjtött adatokat, az elemzési eredményeket és a végrehajtott cselekvéseket, hogy bizonyítékot szolgáltasson a kiberbiztonsági követelményeknek való megfelelésről.

Kapcsolódó intézkedések

2.2. Fiókkezelés

2.15. Hozzáférés-ellenőrzés érvényesítése

2.59. Felelősségek szétválasztása

2.60. Legkisebb jogosultság elve

2.71. Sikertelen bejelentkezési kísérletek

2.100. Távoli hozzáférés

4.22. Naplóbejegyzések csökkentése és jelentéskészítés

4.51. Szervezeten átívelő naplózás

5.2. Biztonsági értékelések

5.14. Folyamatos felügyelet

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

3.3.12.6. Naplóvizsgálat és jelentéskészítés

ISO/IEC 27001:2023 REFERENCIA

A.5.25; A.6.8; A.8.15

NIST SP 800-53 REV.5 REFERENCIA

AU-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

4.14. NAPLÓBEJEGYZÉSEK FELÜLVIZSGÁLATA, ELEMZÉSE ÉS JELENTÉSTÉTEL – AUTOMATIZÁLT FOLYAMATINTEGRÁCIÓ

4.14. A szervezet automatizált mechanizmusokat használ a naplóbejegyzések felülvizsgálatának, elemzésének és jelentési folyamatainak integrálására.

MAGYARÁZAT

A következő szervezeten belüli folyamatok számára lehet hasznos a naplóbejegyzések felülvizsgálatának, elemzésének és jelentési folyamatainak automatizálása: incidenskezelés, folyamatos felügyelet, üzletmenet-folytonosságra vonatkozó eljárásrend, gyanús tevékenységek kivizsgálása és az azokra adott válasz. Az automatikus mechanizmusok automatikusan összegyűjtik és elemzik a naplóbejegyzéseket, annak érdekében, hogy azonosítsák a potenciális biztonsági problémákat és fenyegetéseket. Az eredményeket jelentések formájában továbbítják a megfelelő személyeknek vagy szerepköröknek, lehetővé téve számukra, hogy gyorsan reagáljanak a problémákra és minimalizálják a kockázatokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

A szervezetnek a 4.13-as pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. A szervezetnek be kell vezetnie automatikus mechanizmusokat a naplóbejegyzések felülvizsgálatára, elemzésére és jelentési folyamataira. Ez magában foglalhatja a naplóelemzési eszközök, mint például a SIEM rendszerek használatát.
2. A szervezetnek integrálnia kell ezeket a mechanizmusokat a meglévő EIR környezetébe. Ez azt jelenti, hogy az automatikus naplóelemzési és jelentési folyamatoknak képesnek kell lenniük az EIR különböző komponenseivel történő kommunikációra és azokból származó adatok feldolgozására.

KAPCSOLÓDÓ INTÉZKEDÉSEK

1.7. Vállalati architektúra

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

3.3.12.6. Naplóvizsgálat és jelentéskészítés

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-6(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

4.15. NAPLÓBEJEGYZÉSEK FELÜLVIZSGÁLATA, ELEMZÉSE ÉS JELENTÉSTÉTEL – NAPLÓZÁSI TÁRHELYEK ÖSSZEKAPCSOLÁSA

4.15. A szervezet elemzi és összekapcsolja a különböző tárhelyeken található naplóbejegyzéseket a teljes szervezetre kiterjedő helyzetfelismerés érdekében.

MAGYARÁZAT

A teljes szervezetre kiterjedő helyzetfelismerés magában foglalja a felismerést a kockázatkezelés mindhárom szintjén (szervezeti szint, célkitűzés/üzleti folyamat szint, EIR szint) és támogatja az egész szervezetre kiterjedő felismerést. Az érintett szervezet elemzi és összekapcsolja a különböző tárhelyeken található naplóbejegyzéseket. Ez azt jelenti, hogy az érintett szervezet összegyűjti és összehasonlítja a különböző forrásokból származó naplóbejegyzéseket, annak érdekében, hogy átfogó képet kapjon a szervezet egészének biztonsági állapotáról. A naplózási tárhelyek összekapcsolása lehetővé teszi a szervezet számára, hogy azonosítsa a mintázatokat, a rendellenességeket és a potenciális biztonsági fenyegetéseket. Ez segíthet a szervezetnek a kockázatok kezelésében, a biztonsági események megelőzésében és a válaszidők csökkentésében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely naplózási tárhelyeket kívánja összekapcsolni és ezt követően össze kell gyűjtenie a különböző tárhelyeken található naplóbejegyzéseket. Ez magában foglalhatja az EIR által generált naplóbejegyzéseket, a hálózati forgalommal kapcsolatos naplóbejegyzéseket, az alkalmazások által generált naplóbejegyzéseket, valamint az egyes adatbázisok által generált naplóbejegyzéseket is.
2. A szervezetnek implementálnia kell egy naplóelemző eszközt vagy szolgáltatást (pl.: SIEM rendszer) amely képes összegyűjteni, elemezni és összekapcsolni a naplóbejegyzéseket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.40. Naplóbejegyzések létrehozása

9.9.1. Biztonsági események kezelése

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

3.3.12.6. Naplóvizsgálat és jelentéskészítés

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-6(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

4.16. NAPLÓBEJEGYZÉSEK FELÜLVIZSGÁLATA, ELEMZÉSE ÉS JELENTÉSTÉTEL – KÖZPONTI VIZSGÁLAT ÉS ELEMZÉS

4.16. Az EIR biztosítja a több rendszerelemből származó naplóbejegyzések központi felülvizsgálatát és elemzését.

MAGYARÁZAT

A központi felülvizsgálatok és elemzések automatizált rendszerei közé tartoznak a biztonsági információ- és eseménykezelő (SIEM) eszközök. A SIEM képes összegyűjteni és összehasonlítani a különböző EIR-ekből származó naplóbejegyzéseket, lehetővé téve az érintett szervezet számára, hogy átfogó képet kapjon az EIR-ek állapotáról és azok tevékenységéről. Ez a funkció különösen hasznos lehet a kiberbiztonsági események kezelésében, mivel lehetővé teszi a szervezet számára, hogy gyorsan azonosítsa és reagáljon a potenciális biztonsági fenyegetésekre. Például, ha egy adott EIR rendellenes tevékenységet mutat a naplóbejegyzések alapján, a SIEM központilag észlelheti ezt, és értesítheti az érintett személyeket vagy szerepköröket. Ezen kívül a SIEM által végzett központi naplóelemzés segíthet a szervezetnek megérteni, hogy mely EIR-ek működnek jól, és melyek igényelnek további figyelmet vagy javítást. Ez lehetővé teszi a szervezet számára, hogy hatékonyabban menedzselje az erőforrásait és ezáltal javítsa az EIR-ek teljesítményét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell szereznie egy olyan automatizált eszközt, amely képes a központi felülvizsgálatok és elemzések végrehajtására pl.: biztonsági információ- és eseménykezelő eszköz (SIEM).
2. A szervezetnek a gyakorlatban is alkalmaznia kell az eszközt, és úgy kell beállítani, hogy képes legyen összegyűjteni a több EIR-ből származó naplóbejegyzéseket.
3. A szervezetnek be kell állítania a naplóbejegyzések gyűjtésének paramétereit, beleértve a gyűjtendő adatok típusát, a gyűjtés gyakoriságát és időtartamát.
4. A szervezetnek rendszeresen elemeznie a naplóbejegyzéseket, hogy azonosítsa a potenciális biztonsági problémákat vagy biztonsági eseményeket. (A SIEM termékek automatikusan elvégzik a naplóbejegyzések elemzését.)

Kapcsolódó intézkedések

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

AU-6(4)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

4.17. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Felügyeleti képességek integrálása

4.17. A szervezet egyesíti a naplók elemzését a sérülékenységmenedzsment során keletkezett információkkal, a teljesítményadatokkal, a rendszerfelügyeleti információkkal vagy egyéb forrásokból begyűjtött információkkal a nem megfelelő vagy szokatlan tevékenységek azonosításának javítása érdekében.

Magyarázat

A felügyeleti képességek integrálása nem igényel sérülékenység-szkennelést, teljesítményadat generálást vagy rendszerfelügyeletet. Ehelyett a felügyeleti képességek integrálásához az szükséges, hogy a szkennelés, a felügyelet vagy más adatgyűjtési tevékenységek által generált információk elemzése egyesítésre kerüljön a naplók elemzésével. A biztonsági információ- és eseménykezelő (SIEM) eszközök segíthetnek a naplóbejegyzések több rendszerkomponensből történő összegyűjtésében vagy konszolidálásában, illetve a naplóbejegyzések korrelációjában és elemzésében. A szervezet által kifejlesztett szabványosított naplóelemzési szkriptek használata (szükség szerinti helyi szkriptmódosításokkal) költséghatékonyabb megközelítést biztosít a gyűjtött naplóbejegyzésekkel kapcsolatos információk elemzéséhez. A naplóbejegyzésekkel kapcsolatos információk összevetése a sérülékenység-szkennelési információkkal fontos az EIR-en lefolytatott sérülékenység-szkennelés valóságtartalmának megállapításában, illetve az észlelt támadási események szkennelési eredményekkel történő összevetésben. A teljesítményadatokkal történő korreláció feltárhatja a szolgáltatás-megtagadásos támadásokat vagy más típusú támadásokat, amelyek az erőforrások jogosulatlan használatához vezetnek. Az rendszerfelügyeleti információkkal történő összevetés segíthet a támadások felderítésében és a naplóinformációk működési helyzetekhez való jobb hozzárendelésében.

A követelmény alkalmazásának lépései

1. A szervezetnek be kell gyűjtenie a naplókat, a sérülékenységi szkennelési információkat, a teljesítmény adatokat és a rendszerfelügyeleti információkat.

2. A szervezetnek egyesítenie kell az összegyűjtött információk elemzését. Ez azt jelenti, hogy a naplók elemzését össze kell kapcsolni a sérülékenységi szkennelési információkkal, a teljesítményadatokkal és a rendszerfelügyeleti információkkal.

3. A szervezet használhat biztonsági információ- és eseménykezelő SIEM) eszközt, amelyek segíthet a több rendszerkomponensből származó naplóbejegyzések összegyűjtésében, konszolidálásában, korrelációjában és elemzésében.

4. A szervezetnek össze kell vetnie a naplóbejegyzésekkel kapcsolatos információkat a sérülékenység-szkennelési információkkal, hogy meghatározza a szkennelések valóságtartalmát, illetve abban is segíthet, hogy a szervezet összeveti az észlelt támadási eseményeket a szkennelési eredményekkel.

5. A szervezetnek össze kell kapcsolnia a naplóbejegyzésekkel kapcsolatos információkat teljesítményadatokkal, ami segíthet a szolgáltatásmegtagadási támadások vagy más típusú támadások felfedezésében.

6. A szervezetnek össze kell kapcsolnia a naplóbejegyzésekkel kapcsolatos információkat a rendszerfelügyeleti információkkal, ami segíthet a támadások felfedezésében és a naplóinformációk működési helyzetekhez való jobb hozzárendelésében.

Kapcsolódó intézkedések

4.40. Naplóbejegyzések létrehozása

9.9.1. Biztonsági események kezelése

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

3.3.12.6. Naplóvizsgálat és jelentéskészítés

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AU-6(5)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az egyéb forrásokból begyűjtött adatok/információk meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

4.18. NAPLÓBEJEGYZÉSEK FELÜLVIZSGÁLATA, ELEMZÉSE ÉS JELENTÉSTÉTEL – ÖSSZEVETÉS A FIZIKAI FELÜGYELETTEL

4.18. A szervezet összeveti a naplóbejegyzésekből származó információkat a fizikai hozzáférés felügyeletéből nyert adatokkal, a szokatlan, nem odaillő, gyanús vagy rosszindulatú tevékenységek azonosítására vonatkozó képességek fejlesztése érdekében.

MAGYARÁZAT

Az érintett szervezet összeveti a fizikai hozzáférési naplóbejegyzésekkel kapcsolatos információkat az EIR naplóbejegyzéseivel, mely segíthet a gyanús tevékenységek azonosításában, vagy az azt alátámasztó bizonyítékok feltárásában. Például, ha egy adott felhasználói fiókkal logikai hozzáférés történt az EIR-hez, de a fizikai biztonsági információk szerint a személy nem volt jelen az intézményben, amikor a logikai hozzáférés történt, akkor az visszaélésre utalhat. Az ilyen típusú összefüggések feltárása hozzájárulhat a szokatlan, nem odaillő, gyanús vagy rosszindulatú tevékenységek azonosítására vonatkozó képességek fejlesztéséhez.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek össze kell gyűjtenie a naplóbejegyzésekből származó információkat, valamint a fizikai hozzáférés felügyeletéből származó adatokat.
2. A szervezetnek össze kell vetnie a naplóbejegyzésekből és a fizikai hozzáférés felügyeletéből származó adatokat. Ez segíthet a gyanús tevékenységek azonosításában, vagy az azt alátámasztó bizonyítékok feltárásában. Például, ha egy adott felhasználói fiókkal logikai hozzáférés történt az EIR-hez, de a fizikai biztonsági információk szerint a személy nem volt jelen az intézményben, amikor a logikai hozzáférés történt, akkor az visszaélésre utalhat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.12.6. Naplóvizsgálat és jelentéskészítés

ISO/IEC 27001:2023 REFERENCIA

A.7.4

NIST SP 800-53 REV.5 REFERENCIA

AU-6(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

4.19. NAPLÓBEJEGYZÉSEK FELÜLVIZSGÁLATA, ELEMZÉSE ÉS JELENTÉSTÉTEL – ENGEDÉLYEZETT MŰVELETEK

4.19. A szervezet meghatározza az engedélyezett tevékenységeket minden olyan rendszerfolyamathoz, szerepkörhöz vagy felhasználóhoz, amely a naplóbejegyzések felülvizsgálatával, elemzésével és jelentésekkel kapcsolatos.

MAGYARÁZAT

A szervezetek a rendszerfiók-kezelési tevékenységeken keresztül határozzák meg a rendszerfolyamatok, szerepkörök és felhasználók számára engedélyezett műveleteket, amelyek a naplóbejegyzések felülvizsgálatával, elemzésével és jelentésével kapcsolatosak. A naplóbejegyzések információival kapcsolatos engedélyezett műveletek meghatározásakor a legkisebb jogosultság elvét kell érvényesíteni. Az engedélyezett műveleteket a rendszer kényszeríti ki, melyek közé az olvasás, az írás, a végrehajtás, a hozzáadás és a törlés tartozik.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az engedélyezett tevékenységeket minden olyan rendszerfolyamathoz, szerepkörhöz vagy felhasználóhoz, amely a naplóbejegyzések felülvizsgálatával, elemzésével és a jelentésekkel kapcsolatosak.
2. Az engedélyezett tevékenységek meghatározását a szervezetnek a rendszerfiók-kezelési tevékenységeken keresztül kell elvégeznie.
3. Az engedélyezett tevékenységek meghatározása során a szervezetnek a legkisebb jogosultság elvét kell érvényesítenie a naplóbejegyzésekkel kapcsolatos információkhoz való hozzáférés során.
4. Az engedélyezett tevékenységeket az EIR-nek kell kikényszerítenie.

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

AU-6(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.20. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel – Privilegizált parancsok teljes szöveges elemzése

4.20. A szervezet elvégzi a naplózott privilegizált parancsok teljes szöveges elemzését a rendszer egy fizikailag és funkcionálisan elkülönített elemében vagy alrendszerében, vagy más, kifejezetten erre az elemzésre szolgáló rendszerben.

Magyarázat

A privilegizált utasítások teljes szöveges elemzése külön környezetet igényel a privilegizált felhasználókkal kapcsolatos naplóbejegyzések elemzéséhez úgy, hogy az ilyen információk ne sérüljenek azon a rendszeren, ahol a felhasználóknak megemelt jogosultságaik vannak, beleértve a privilegizált parancsok végrehajtására való képességet is. A teljes szöveges elemzés a privilegizált parancsok teljes szövegét figyelembe vevő elemzést jelenti (pl.: parancsok és paraméterek), szemben a csak a parancs nevét figyelembe vevő elemzéssel. A teljes szöveges elemzés magában foglalja a mintaillesztés és a heurisztikus módszerek használatát.

A követelmény alkalmazásának lépései

1. A szervezetnek létre kell hoznia egy fizikailag és funkcionálisan elkülönített elemet vagy alrendszert, vagy egy másik, kifejezetten a privilegizált parancsok teljes szöveges elemzésére szolgáló rendszert.
2. Ezután a szervezetnek naplóznia kell minden privilegizált parancsot, amelyet a felhasználók a rendszerben végrehajtanak. Ez magában foglalja a parancsok és a paraméterek teljes szövegét.
3. A naplózott adatokat a szervezetnek át kell vinni a különálló elembe vagy alrendszerbe, vagy más, kifejezetten erre az elemzésre szolgáló rendszerbe. Fontos, hogy ez az átvitel biztonságos módon történjen, hogy ne veszélyeztesse a naplózott információk sértetlenségét.
4. A szervezetnek el kell végeznie a naplózott privilegizált parancsok teljes szöveges elemzését. Ez magában foglalja a mintaillesztés és a heurisztikus módszerek alkalmazását is.
5. Az elemzés eredményeit a szervezetnek fel kell használnia a kiberbiztonsággal kapcsolatos intézkedések további fejlesztésére, például a privilegizált felhasználók tevékenységének jobb nyomon követésére és a potenciális biztonsági rések azonosítására.

Kapcsolódó intézkedések

4.3. Naplóbejegyzések tartalma

4.25. Naplóinformációk védelme

4.38. A naplóbejegyzések megőrzése

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

AU-6(8)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

4.21. NAPLÓBEJEGYZÉSEK FELÜLVIZSGÁLATA, ELEMZÉSE ÉS JELENTÉSTÉTEL – ÖSSZEVETÉS A NEM TECHNOLÓGIAI FORRÁSOKBÓL SZÁRMAZÓ INFORMÁCIÓKKAL

4.21. A szervezet összeveti a naplóbejegyzésekből származó információkat a nem technológiai forrásokból származó információkkal, a teljes szervezetre kiterjedő helyzetfelismerés javítása érdekében.

MAGYARÁZAT

A nem technológiai források közé tartoznak azon szervezeti szabályozók megsértését dokumentáló feljegyzések, amelyek például az információs eszközök nem megfelelő használatával kapcsolatosak. Az ilyen információk segíthetnek a célzott elemzési tevékenységekben a potenciálisan rosszindulatú bennfentes tevékenység felderítése érdekében. A szervezet korlátozza a nem technológiai forrásokból származó információkhoz való hozzáférést azok bizalmas jellege miatt. A korlátozott hozzáférés minimalizálja a személyes adatokkal kapcsolatos információk véletlen kiszolgáltatásának lehetőségét olyan személyek esetében, akiknek nem szükséges ismerniük az említett információkat. A nem technológiai forrásokból származó információk és a naplóbejegyzések összevetése általában csak akkor történik meg, ha egyes személyeket azzal gyanúsítanak, hogy érintettek voltak egy biztonsági eseményben. A szervezetnek az ilyen intézkedések kezdeményezése előtt célszerű jogi tanácsot kérni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek össze kell gyűjtenie a naplóbejegyzésekből származó információkat. Ezek a bejegyzések tartalmazhatnak adatokat a rendszerhasználattal, a hálózati forgalommal, a felhasználói tevékenységekkel és egyéb eseményekkel kapcsolatban.
2. A szervezetnek össze kell gyűjtenie a nem technológiai forrásokból származó információkat. Ez lehet például a szervezeti szabályozók megsértését dokumentáló feljegyzések, amelyek az információs eszközök nem megfelelő használatával kapcsolatosak.
3. A szervezetnek korlátoznia kell a nem technológiai forrásokból származó információkhoz való hozzáférést, mivel ezek bizalmas adatokat tartalmazhatnak. A korlátozott hozzáférés

minimalizálja a személyes adatokkal kapcsolatos információk véletlen kiszolgáltatásának lehetőségét olyan személyek esetében, akiknek nem szükséges ismerniük az említett információkat.

4. A szervezetnek össze kell vetnie a naplóbejegyzésekből és a nem technológiai forrásokból származó információkat. Ez általában akkor történik meg, ha egyes személyeket azzal gyanúsítanak, hogy érintettek voltak egy biztonsági eseményben.

5. A szervezetnek célszerű jogi tanácsot kérnie, mielőtt ilyen összehasonlító tevékenységet kezdeményezne. Ez segít biztosítani, hogy az összehasonlítás során a szervezet szem előtt tartsa az érintettek jogait és a szervezet jogi kötelezettségeit.

Kapcsolódó intézkedések

1.13. Belső fenyegetés elleni program

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AU-6(9)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

4.22. NAPLÓBEJEGYZÉSEK CSÖKKENTÉSE ÉS JELENTÉSKÉSZÍTÉS

4.22. A szervezet lehetőséget biztosít naplóbejegyzések csökkentésre és jelentéskészítésre:

4.22.1. amely támogatja az igény esetén végzendő naplófelülvizsgálati, naplóelemzési és jelentéstételi követelményeket, valamint a biztonsági eseményeket követő tényfeltáró vizsgálatokat;

4.22.2. amely nem változtathatja meg a naplóbejegyzések eredeti tartalmát és időrendjét.

MAGYARÁZAT

A naplóbejegyzések csökkentése egy olyan folyamat, amely manipulálja a gyűjtött naplóinformációkat és egy összefoglaló formátumba szervezi azokat, így könnyebben értelmezhetők az elemzők számára. A naplóbejegyzések csökkentési és jelentéskészítési képességei nem mindig származnak ugyanabból az EIR-ből vagy ugyanattól az érintett szervezettől, amelyek a naplózási tevékenységeket végzik. A naplóbejegyzések csökkentési képessége magában foglalja a modern adatbányászati technikákat fejlett adatszűrőkkel, annak érdekében, hogy azonosítani lehessen a szokatlan tevékenységeket a naplóbejegyzésekben. A naplócsökkentési megoldás által nyújtott jelentéskészítési képességnek képesnek kell lennie testreszabható jelentések generálására. A naplóbejegyzések időrendi sorrendje problémát jelenthet, ha a bejegyzés időbélyegének részletessége nem elegendő, ezért a forrásrendszerekben gondoskodni kell arról, hogy kellően pontos időbélyeggel legyenek ellátva a naplóbejegyzések. A naplócsökkentő megoldás nem változtathatja meg a naplóbejegyzések eredeti tartalmát és időrendjét.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell egy naplócsökkentési megoldást, amely képes manipulálni a gyűjtött naplóinformációkat és egy összefoglaló formátumba szervezni azokat, melyek így könnyebben értelmezhetők az elemzők számára.

2. A szervezetnek figyelembe kell vennie, hogy a naplóbejegyzések időrendi sorrendje problémát jelenthet, ha a bejegyzés időbélyegének részletessége nem elegendő. Ezért a szervezetnek biztosítania kell, hogy a forrásrendszerek kellően pontos naplóbejegyzésket

állítsanak elő, a naplócsökkentési megoldás pedig ne változtathassa meg a naplóbejegyzések eredeti tartalmát és időrendjét.

3. A szervezetnek a naplócsökkentési megoldásának modern adatbányászati technikákat kell tartalmaznia speciális adatszűrőkkel, annak érdekében, hogy azonosítani lehessen a szokatlan tevékenységeket a naplóbejegyzésekben.

4. A szervezetnek biztosítania kell, hogy a naplócsökkentési megoldás képes legyen testreszabható jelentések generálására.

Kapcsolódó intézkedések

2.2. Fiókkezelés

4.2. Naplózható események

4.3. Naplóbejegyzések tartalma

4.5. Naplózás tárkapacitása

4.7. Naplózási hiba kezelése

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.40. Naplóbejegyzések létrehozása

4.51. Szervezeten átívelő naplózás

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

8.21. A hitelesítésre szolgáló eszközök kezelése

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

3.3.12.7. Naplócsökkentés és jelentéskészítés

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

AU-7

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

4.23. NAPLÓBEJEGYZÉSEK CSÖKKENTÉSE ÉS JELENTÉSKÉSZÍTÉS – AUTOMATIKUS FELDOLGOZÁS

4.23. A szervezet gondoskodik arról, hogy a naplóbejegyzések automatikusan feldolgozhatók, rendezhetők és kereshetők legyenek a meghatározott adatmezők tekintetében.

MAGYARÁZAT

A releváns események azonosíthatók a naplóbejegyzések tartalma alapján, beleértve az érintett rendszererőforrásokat, a hozzáférhető információs objektumokat, a felhasználók azonosítói, az események típusait, az események helyszíneit, az események dátumait és időpontjait, az érintett IP-címeket, illetve a sikeres vagy sikertelen eseményeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a naplóbejegyzésekben szereplő adatmezőket, amelyek alapján a naplóbejegyzések automatikusan feldolgozhatók, rendezhetők és kereshetők lesznek pl.: felhasználói azonosítók, esemény típusa, helyszíne, dátuma és időpontja, IP-cím stb.
2. A szervezetnek implementálnia kell egy olyan megoldást, amely képes automatikusan feldolgozni, rendezni és keresni a naplóbejegyzéseket a meghatározott adatmezők alapján.
3. A szervezetnek biztosítania kell, hogy a naplófeldolgozó megoldás rendszeresen frissüljön és karbantartásra kerüljön, hogy a naplóbejegyzések folyamatosan feldolgozhatók, rendezhetők és kereshetők legyenek.
4. A szervezetnek rendszeres ellenőrzéseket kell végeznie a naplófeldolgozó megoldáson, hogy biztosítsa a naplóbejegyzések megfelelő feldolgozását, rendezését és keresését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.12.7. Naplócsökkentés és jelentéskészítés

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-7(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az adatmezők meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

4.24. IDŐBÉLYEGEK

4.24. A szervezet:

4.24.1. Belső rendszerórákat használ a naplóbejegyzések időbélyegeinek előállításához.

4.24.2. Időbélyegeket rögzít a naplóbejegyzésekben, amelyek megfelelnek a szervezet által meghatározott pontosságra vonatkozó követelményeknek, a koordinált világidőt használják és magukba foglalják a helyi időeltolódást.

MAGYARÁZAT

Az EIR által generált időbélyegek tartalmazzák a dátumot és az időt. Az időt általában koordinált világidőben (UTC), ami a Greenwichi középidő (GMT) modern formája, vagy helyi időben, UTC-től történő eltérés feltüntetésével szokás megjeleníteni. Az időmérés pontossága a rendszerórák és a referenciaórák közötti szinkronizáció mértékére utal (pl. az órák több száz milliszekundumon vagy tíz milliszekundumon belüli szinkronizációja). A szervezet különböző rendszerelemek számára különböző időrészletességet határozhat meg. Az időszolgáltatás kritikus lehet más biztonsági képességek, például a hozzáférés-felügyelet, az azonosítás és a hitelesítés szempontjából, attól függően, hogy milyen mechanizmusokat használ a szervezet ezeknek a képességeknek a támogatására.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az általa használt belső rendszerórák pontosak és szinkronizáltak legyenek, mivel ezeket használják a naplóbejegyzések időbélyegeinek előállításához.

2. A szervezetnek időbélyegeket kell rögzítenie a naplóbejegyzésekben. Ezeknek az időbélyegeknek meg kell felelniük a szervezet által meghatározott pontosságra vonatkozó követelményeknek.

3. A szervezetnek javasolt az időbélyegeket a koordinált világidőt (UTC) felhasználva megjeleníteniük, amely a Greenwichi középidő (GMT) modern megfelelője, vagy a helyi időt a koordinált világidőtől (UTC) történő eltérés feltüntetésével.

Kapcsolódó intézkedések

4.3. Naplóbejegyzések tartalma

4.40. Naplóbejegyzések létrehozása

4.48. Munkaszakasz-ellenőrzés

17.123. Rendszeridő szinkronizálása

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

3.3.12.8. Időbélyegek

ISO/IEC 27001:2023 referencia

A.8.17

NIST SP 800-53 rev.5 referencia

AU-8

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

4.25. NAPLÓINFORMÁCIÓK VÉDELME

4.25. Az EIR:

4.25.1. Megvédi a naplóinformációt és a naplókezelő eszközöket a jogosulatlan hozzáféréssel, módosítással és törléssel szemben.

4.25.2. Jogosulatlan hozzáférés, módosítás vagy a naplóinformáció törlésének észlelésekor értesíti a meghatározott személyeket vagy szerepköröket.

MAGYARÁZAT

A naplóinformációk magukban foglalják az EIR-ben végrehajtott tevékenységek sikeres ellenőrzéséhez szükséges összes információt, például a naplóbejegyzéseket, a naplófájlok beállításait, a vizsgálati jelentéseket és a személyazonosításra alkalmas információkat. A naplókezelő eszközök azok a programok és eszközök, amelyeket az EIR naplózására és a naplózási tevékenységek elvégzésére használnak. Az naplóinformációk védelme a technikai védelemre összpontosít, és a naplókezelő eszközökhöz történő hozzáférést és azok futtatását az arra jogosult személyekre korlátozza. A naplóinformációk fizikai védelmét mind az adathordozók védelmének intézkedései, mind a fizikai és környezeti védelem intézkedései biztosítják. A naplóinformációkhoz történő jogosulatlan hozzáférés felügyelete kritikus fontosságú a kiberbiztonsági események gyors észleléséhez és kezeléséhez, valamint az érintett szervezet kiberbiztonsági állapotának folyamatos monitorozásához.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR-ben végrehajtott tevékenységek sikeres ellenőrzéséhez szükséges összes információ rendelkezésre álljon pl.: naplóbejegyzések, naplófájlok beállításai, a vizsgálati jelentéseket és a személyazonosításra alkalmas információk.

2. A szervezetnek kiemelt figyelmet kell fordítania a naplóinformációk technikai védelmére. Korlátoznia kell a naplózási eszközökhöz történő hozzáférést, annak érdekében, hogy megakadályozza a jogosulatlan hozzáférést, módosítást, illetve törlést.

4. A szervezetnek fizikailag is meg kell védenie kell a naplóinformációkat. A naplóinformációk fizikai védelmét a szervezet az adathordozók védelmére, illetve a fizikai és környezeti védelemre vonatkozó biztonsági követelmények betartásával tudja biztosítani.

5. A szervezetnek úgy kell beállítania az EIR-t, hogy amennyiben jogosulatlan hozzáférést, módosítást vagy a naplóinformációk törlését észleli, képes legyen értesítést küldeni a meghatározott személyeknek vagy szerepköröknek.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

2.60. Legkisebb jogosultság elve

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.38. A naplóbejegyzések megőrzése

4.48. Munkaszakasz-ellenőrzés

11.2. Hozzáférés az adathordozókhoz

11.4. Adathordozók tárolása

12.2. A fizikai belépési engedélyek

12.6. A fizikai belépés ellenőrzése

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

3.3.12.9. A naplóinformációk védelme

ISO/IEC 27001:2023 referencia

A.5.33; A.8.15

NIST SP 800-53 rev.5 referencia

AU-9

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
X	X	X

4.26. A NAPLÓINFORMÁCIÓK VÉDELME – EGYSZER ÍRHATÓ ADATHORDOZÓ

4.26. Az EIR a naplóbejegyzéseket egy hardveresen kikényszerített, egyszer írható adathordozóra rögzíti.

MAGYARÁZAT

A naplófájlok hardveresen kikényszerített, egyszer írható adathordozóra történő írása a naplófájlok kezdeti létrehozására és a naplófájlok biztonsági mentésére vonatkozik. A naplófájlok hardveresen kikényszerített, egyszer írható adathordozóra történő írása nem vonatkozik a naplófájlokba történő írást megelőzően a naplóadatok kezdeti generálására. Az egyszer írható, sokszor olvasható (WORM) adathordozók közé tartozik a CD (Compact Disc-Recordable (CD-R)), a Blu-Ray (Blu-Ray Disc Recordable (BD-R)) és a DVD (Digital Versatile Disc-Recordable (DVD-R)). Ezzel szemben a kapcsolható írásvédelemmel ellátott adathordozók, például a szalagos kazetták, az USB-meghajtók (Universal Serial Bus), az újraírható CD-k (Compact Disc Re-Writeable (CD-RW)) és az újraírható DVD (Digital Versatile Disc-Read Write (DVD-RW)) használata írásvédett, de nem egyszer írható adathordozónak minősül.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gondoskodnia arról, hogy a létrehozott naplóbejegyzéseket az EIR egy hardveresen kikényszerített, egyszer írható adathordozóra írja.
2. A szervezetnek kerülnie kell az olyan kapcsolható írásvédelemmel ellátott adathordozók használatát, mint a szalagos kazetták, az USB-meghajtók (Universal Serial Bus), az újraírható CD-k (Compact Disc Re-Writeable (CD-RW)) és az újraírható DVD (Digital Versatile Disc-Read Write (DVD-RW)).

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.5. Naplózás tárkapacitása

4.7. Naplózási hiba kezelése

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

AU-9(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.27. A NAPLÓINFORMÁCIÓK VÉDELME – TÁROLÁS FIZIKAILAG KÜLÖNÁLLÓ RENDSZEREKEN VAGY RENDSZERELEMEKEN

4.27. Az EIR a naplóbejegyzéseket meghatározott gyakorisággal eltárolja egy olyan tárhelyen, amely a keletkezési helyétől fizikailag elkülönült rendszer vagy rendszerelem része.

MAGYARÁZAT

Az EIR naplóbejegyzéseinek tárolása egy olyan tárhelyen, amely fizikailag elkülönült az EIR-től vagy a rendszerelemeitől, segít biztosítani, hogy az EIR kompromittálása ne eredményezze a naplóbejegyzések kompromittálását is. A naplóbejegyzések tárolása különálló fizikai rendszeren vagy rendszerelemen megőrzi a naplóbejegyzések bizalmasságát és sértetlenségét, és megkönnyíti a naplóbejegyzések kezelését szervezeti szinten. A naplóbejegyzések tárolása különálló rendszeren vagy rendszerelemen vonatkozik a naplóbejegyzések eredeti, legenerált verziójára, valamint a naplóbejegyzések biztonsági mentésére is.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR naplóbejegyzéseit egy olyan tárhelyen tárolja, amely fizikailag elkülönült az EIR-től vagy annak elemeitől. Ez segít megelőzni, hogy az EIR kompromittálása esetén a naplóbejegyzések is kompromittálódjanak. Emellett így megőrizhető a naplóbejegyzések bizalmassága és sértetlensége, illetve könnyebbé válik a naplóbejegyzések kezelése szervezeti szinten.
2. A szervezetnek a naplóbejegyzések eredeti, legenerált verzióját, valamint a naplóbejegyzések biztonsági mentését is egy olyan tárhelyen kell tárolnia, mely a naplóinformációk keletkezési helyétől fizikailag elkülönült rendszer vagy rendszerelem része.
3. A szervezetnek rendszeresen ellenőriznie kell a naplóbejegyzések tárolási követelményeit.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.5. Naplózás tárkapacitása

4.7. Naplózási hiba kezelése

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

3.3.12.9. A naplóinformációk védelme

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-9(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

4.28. A NAPLÓINFORMÁCIÓK VÉDELME – KRIPTOGRÁFIAI VÉDELEM

4.28. A szervezet kriptográfiai eszközöket alkalmaz a naplóinformációk és a naplókezelő eszköz sértetlenségének védelmére.

MAGYARÁZAT

Az érintett szervezet kriptográfiai eszközöket alkalmaz a naplóinformációk sértetlenségének védelmére, beleértve az aszimmetrikus kriptográfiát használó aláírt hash funkciókat. Ez lehetővé teszi a nyilvános kulcs terjesztését a hash információ ellenőrzéséhez, miközben megőrzi a hash generálásához használt titkos kulcs bizalmasságát.

Az EIR naplóinformációinak sértetlenségének védelme nem csak az adatok biztonságát növeli, hanem segít az érintett szervezetnek megfelelni a különböző biztonsági követelményeknek is. A kriptográfiai eszközök használata segíthet a szervezetnek bizonyítani, hogy megfelelő intézkedéseket tett a naplóinformációk és a naplókezelő eszközök védelmére.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy milyen kriptográfiai eszközöket kíván alkalmazni a naplóinformációk és a naplókezelő eszköz sértetlenségének védelmére.
2. A szervezetnek ki kell választania egy megfelelő kriptográfiai eszközt. Az eszköz által alkalmazott kriptográfiai algoritmusnak biztosítania kell a naplóinformációk sértetlenségét, és meg kell akadályoznia a nem engedélyezett módosításokat.
3. A szervezetnek implementálnia kell a kiválasztott kriptográfiai eszközt. Ez magában foglalhatja a kriptográfiai eszköz beállításait, a kulcskezelést és a kriptográfiai eszköz használatának szabályait.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.33. Letagadhatatlanság

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

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

3.3.12.9. A naplóinformációk védelme

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-9(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

4.29. A NAPLÓINFORMÁCIÓK VÉDELME – PRIVILEGIZÁLT FELHASZNÁLÓK HOZZÁFÉRÉSE

4.29. A szervezet a naplózási funkciók kezeléséhez csak egy meghatározott jogosultsági szinttel rendelkező felhasználói csoportnak vagy felhasználói szerepeknek ad hozzáférési jogosultságot.

MAGYARÁZAT

Azok a személyek vagy szerepkörök, akik privilegizált hozzáféréssel rendelkeznek egy rendszerhez, és akik egyben az adott rendszer által végzett naplózás tárgyát is képezik, befolyásolhatják az naplózási információk megbízhatóságát azáltal, hogy korlátozzák a naplózási tevékenységeket vagy módosítják a naplóbejegyzéseket. A privilegizált hozzáférésnek a naplózással kapcsolatos jogosultságok és az egyéb jogosultságok közötti további elkülönítése korlátozza a naplózással kapcsolatos jogosultságokkal rendelkező felhasználók vagy szerepkörök számát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia azokat a felhasználókat vagy szerepköröket, akiknek jogosultsága van az EIR naplózási funkcióinak kezelésére.
2. A szervezetnek be kell állítania a jogosultsági szinteket, amelyek meghatározzák, hogy mely felhasználók vagy szerepkörök rendelkeznek hozzáférési jogosultsággal az EIR naplózási funkcióihoz.
3. A szervezetnek rendszeresen ellenőriznie kell a jogosultsági szinteket, annak érdekében, hogy biztosítsa, hogy csak a megfelelő felhasználók vagy szerepkörök rendelkeznek hozzáférési jogosultsággal az EIR naplózási funkcióihoz. Amennyiben szükséges a szervezetnek módosítania kell a jogosultságokat.
4. A szervezetnek dokumentálnia kell a folyamatot, beleértve a privilegizált felhasználók vagy szerepkörök meghatározását, a hozzáférési jogosultságok beállítását és a rendszeres ellenőrzéseket is.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.59. Felelősségek szétválasztása

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

AU-9(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kiemelt jogosultsággal rendelkező felhasználók, valamint a kiemelt jogosultságok meghatározása EIR-rel.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

4.30. A NAPLÓINFORMÁCIÓK VÉDELME – KETTŐS JÓVÁHAGYÁS

4.30. A szervezet kikényszeríti a kettős jóváhagyást a szervezet által meghatározott naplóinformációk áthelyezéséhez vagy törléséhez.

MAGYARÁZAT

A szervezet a naplóinformációk különböző típusaihoz különböző beállítási lehetőségeket választhat. A kettős jóváhagyási mechanizmusok két jogosult személy jóváhagyását igénylik a felügyeleti funkciók végrehajtásához. Az összejátszás kockázatának csökkentése érdekében a szervezetek megfontolják a kettős jóváhagyási feladatok eltérő személyek közötti rotációját. Amennyiben a köz- és környezeti biztonság érdekében azonnali válaszlépésekre van szükség, a szervezet mellőzheti a kettős jóváhagyási mechanizmusok alkalmazását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely naplóinformációk áthelyezéséhez vagy törléséhez szükséges a kettős jóváhagyás.
2. A szervezetnek kettős jóváhagyási mechanizmust kell bevezetnie, amely két feljogosított személy jóváhagyását igényli a meghatározott naplóinformációk áthelyezéséhez vagy törléséhez.
3. Az összejátszás kockázatának csökkentése érdekében a szervezetnek rotálnia kell a kettős jóváhagyási feladatokat eltérő személyek között.
4. A szervezetnek nem szükséges kettős jóváhagyási mechanizmust alkalmaznia, amikor azonnali válaszokra van szükség a köz- és környezetbiztonság biztosítása érdekében.
5. A szervezetnek biztosítania kell, hogy az EIR-ben a kettős jóváhagyás alkalmazása megfelelően dokumentálva legyen.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-9(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a naplóinformációk meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.31. A NAPLÓINFORMÁCIÓK VÉDELME – HOZZÁFÉRÉS CSAK OLVASÁSRA

4.31. A szervezet csak olvasási hozzáférést biztosít a naplóinformációkhoz a privilegizált felhasználók vagy szerepkörök egy meghatározott részhalmazának.

MAGYARÁZAT

A privilegizált felhasználók vagy szerepkörök jogosultságainak csak olvasásra történő korlátozása segít mérsékelni a szervezeteknek okozott potenciális károkat, amelyeket az ilyen felhasználók vagy szerepkörök okozhatnak pl.: naplóbejegyzések törlése annak érdekében, hogy a rosszindulatú tevékenység elfedésre kerüljön.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, mely felhasználók vagy szerepkörök rendelkeznek privilegizált hozzáféréssel a naplóinformációkhoz.
2. A szervezetnek létre kell hoznia egy részhalmazt ezekből a privilegizált felhasználókból vagy szerepkörökből, akiknek a naplóinformációkhoz csak olvasási hozzáférést kíván biztosítani.
3. A szervezetnek be kell állítania a megfelelő hozzáférési jogosultságokat, annak érdekében, hogy ezek a kiválasztott felhasználók vagy szerepkörök csak olvasási hozzáféréssel rendelkezzenek a naplóinformációkhoz.
4. A szervezetnek rendszeresen ellenőriznie kell a jogosultsági szinteket, annak érdekében, hogy biztosítsa, hogy csak a megfelelő felhasználók vagy szerepkörök rendelkeznek hozzáférési jogosultsággal az EIR naplózási funkcióihoz. Amennyiben szükséges a szervezetnek módosítania kell a jogosultságokat.
5. A szervezetnek dokumentálnia kell a folyamatot, beleértve a privilegizált felhasználók vagy szerepkörök meghatározását, a hozzáférési jogosultságok beállítását és a rendszeres ellenőrzéseket is.

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

AU-9(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kiemelt jogosultsággal rendelkező felhasználók, valamint a kiemelt jogosultságok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.32. A NAPLÓINFORMÁCIÓK VÉDELME – TÁROLÁS ELTÉRŐ OPERÁCIÓS RENDSZERT FUTTATÓ RENDSZERELEMEN

4.32. Az EIR a naplóinformációkat egy olyan rendszerelemben tárolja, amely eltérő operációs rendszert futtat, mint a naplózott rendszer vagy rendszerelem.

MAGYARÁZAT

A naplózási információk tárolása egy másik operációs rendszert futtató rendszerelemen csökkenti annak kockázatát, hogy a rendszerre jellemző sérülékenység a naplóbejegyzések kompromittációját eredményezze.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell választania egy olyan rendszerelemet, amely eltérő operációs rendszert futtat, mint a naplózott rendszer vagy rendszerelem annak érdekében, hogy az EIR-el kapcsolatos naplóinformációkat az említett rendszerelemben tárolja.
2. A szervezetnek úgy kell beállítania a naplózással kapcsolatos konfigurációt a naplózott rendszerben vagy rendszerelemben, hogy a naplóinformációk továbbítódjanak az eltérő operációs rendszert futtató rendszerelembe.
3. A szervezetnek biztosítania kell, hogy a naplóinformációk biztonságos módon továbbítódnak és tárolódnak az új rendszerelemben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.5. Naplózás tárkapacitása

4.7. Naplózási hiba kezelése

4.38. A naplóbejegyzések megőrzése

17.85. A rendszerelemek esetében alkalmazott változatos információs technológiák

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

AU-9(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.33. Letagadhatatlanság

4.33. Az EIR megcáfolhatatlan bizonyítékot szolgáltat arra, hogy egy személy vagy a nevében futó feldolgozási folyamat végrehajtott egy a szervezet által meghatározott, a letagadhatatlanság követelménye alá eső tevékenységet.

Magyarázat

A letagadhatatlanság hatálya alá tartozó egyéni műveletek közé tartozik az információk létrehozása, az üzenetek küldése és fogadása, valamint az információk jóváhagyása. A letagadhatatlanság védelmet nyújt a szerzők azon állításai ellen, hogy bizonyos dokumentumokat nem ők írtak, emellett ha a küldő azt állítja, hogy nem ő küldött üzenetet, a címzett azt állítja, hogy nem ő kapott üzenetet, az aláíró pedig azt állítja, hogy nem ő írta alá a dokumentumokat. A letagadhatatlansági szolgáltatások felhasználhatók annak megállapítására, hogy az információ egy adott személytől származik-e, vagy hogy egy adott személy végzett-e bizonyos műveleteket. Az érintett szervezet különböző technikák vagy mechanizmusok, például digitális aláírások és digitális üzenetátvételi elismervények alkalmazásával valósítja meg a letagadhatatlanságot elősegítő szolgáltatásokat.

A követelmény alkalmazásának lépései

1. Az EIR-nek képesnek kell lennie arra, hogy megcáfolhatatlan bizonyítékot szolgáltasson arról, hogy egy személy vagy a nevében futó feldolgozási folyamat milyen tevékenységet hajtott végre.
2. A szervezetnek letagadhatatlanságot elősegítő szolgáltatásokat kell igénybe vennie, amelyeket különböző technikák vagy mechanizmusok alkalmazásával lehet elérni, beleértve a digitális aláírásokat és a digitális üzenetátvételi elismervényeket.

Kapcsolódó intézkedések

4.25. Naplóinformációk védelme

1.13. Belső fenyegetés elleni program

16.16. Biztonságtervezési elvek

17.40. Az adatátvitel bizalmassága és sértetlensége

17.49. Kriptográfiai kulcs előállítása és kezelése

17.53. Kriptográfiai védelem

17.58. Biztonsági tulajdonságok átvitele

17.62. Nyilvános kulcsú infrastruktúra tanúsítványok

17.73. Munkaszakasz hitelessége

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

3.3.12.10. Letagadhatatlanság: Az elektronikus információs rendszer védelmet biztosít az ellen, hogy egy adott személy az általa használt alkalmazás tekintetében letagadhassa, hogy elvégzett-e egy, a letagadhatatlanság követelménye alá sorolt tevékenységet.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-10

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a letagadhatatlanság követelménye alá eső tevékenység meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

4.34. Letagadhatatlanság – Személyazonosság társítása

4.34. Az EIR:

4.34.1. Az információ előállítójának személyazonosságát összekapcsolja az információval, a szervezet által meghatározott módon.

4.34.2. Biztosítja a jogosult személyek számára, hogy megállapíthassák az információ előállítójának személyazonosságát.

Magyarázat

A személyazonosság információkhoz társítása támogatja a naplózási követelményeket, amelyek segítségével a szervezeti személyzet számára lehetővé válik, hogy információátadás esetén azonosítani lehessen, hogy ki állított elő egy adott információt. A szervezet az információ előállítója és az információ közötti azonosító kapcsolat erősségét az információ biztonsági kategóriája és más releváns kockázati tényezők alapján határozzák meg és hagyják jóvá.

A követelmény alkalmazásának lépései

1. A szervezetnek a személyazonosságot információkhoz kell társítania, így a szervezeti személyzet számára lehetővé válik, hogy információátadás esetén azonosítani lehessen, hogy ki állított elő egy adott információt.

2. Az EIR-nek képesnek kell lennie az információ előállítójának személyazonosságát információhoz kapcsolni a szervezet által meghatározott módon.

3. Az EIR-nek biztosítania kell a jogosult személyek számára, hogy megállapíthassák az információ előállítójának személyazonosságát.

Kapcsolódó intézkedések

2.28. Információáramlási szabályok érvényesítése

2.89. Biztonsági tulajdonságok

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

AU-10(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.35. Letagadhatatlanság – Az információt előállító egyén személyazonossági kapcsolatának hitelesítése

4.35. A szervezet:

4.35.1. meghatározott gyakorisággal ellenőrzi az információt előállító egyén személyazonosságának és az előállított információnak az összekapcsolását; és

4.35.2. ellenőrzési hiba esetén végrehajtja az szervezet által meghatározott műveleteket.

Magyarázat

Az információt előállító személyazonosságának az előállított információhoz történő társításának ellenőrzése megakadályozza az információ módosítását az előállítás és a felülvizsgálat között. A kapcsolatok hitelesítését például kriptográfiai ellenőrző összegek (checksums) alkalmazásával lehet elérni. A szervezet meghatározza, hogy az ellenőrzések felhasználói kérésre történnek-e, vagy automatikusan generálódnak.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a személyazonosság és az előállított információ összekapcsolásának ellenőrzési gyakoriságát.
2. A szervezetnek implementálnia kell az EIR-ben egy olyan funkciót, amely képes az ellenőrzések végrehajtására. Ez a funkció lehet egy kriptográfiai ellenőrző összegeket (checksums) használó megoldás, amely képes validálni az összekapcsolásokat.
3. A szervezetnek döntenie kell arról, hogy az ellenőrzések a felhasználói kérések alapján vagy automatikusan generálódjanak.
4. Ha az EIR hibát észlel az ellenőrzés során, a szervezetnek a meghatározott műveleteket kell végrehajtania pl.: hibás tranzakciók visszavonása, a hibás adatok javítása, vagy a hibás műveletek ismételt végrehajtása.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

2.28. Információáramlási szabályok érvényesítése

2.89. Biztonsági tulajdonságok

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

AU-10(2)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

4.36. LETAGADHATATLANSÁG – FELÜGYELETI LÁNC

4.36. A szervezet fenntartja az információ kibocsátójához és felülvizsgálójához tartozó hitelesítő adatokat a létrehozott felügyeleti láncon belül.

MAGYARÁZAT

A felügyeleti lánc egy olyan folyamat, amely nyomon követi a bizonyítékok mozgását a gyűjtés, a megőrzés és az elemzés életciklusán keresztül, dokumentálva minden egyes személyt, aki a bizonyítékot kezelte, továbbá a bizonyíték gyűjtésének vagy átadásának dátumát és időpontját, valamint az átadás célját. Ha a felülvizsgálatot végző egy emberi személy, vagy ha a felülvizsgálati funkció automatizált, de elkülönül a kiadási vagy átadási funkciótól, akkor a rendszer a kiadandó információ felülvizsgálója személyazonosságát összekapcsolja az információval és az információ címkéjével. Emberi felülvizsgálat esetén a felülvizsgálók vagy kiadók hitelesítő adatainak megőrzése lehetővé teszi a szervezet számára annak azonosítását, hogy ki vizsgálta felül és adta ki az információt. Automatizált felülvizsgálatok esetében biztosítja, hogy csak jóváhagyott felülvizsgálati funkciókat használjanak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek létre kell hoznia egy felügyeleti láncot, amely nyomon követi az információ mozgását a gyűjtéstől, a biztonságos tároláson át, egészen az elemzésig.
2. Ha az információ felülvizsgálója egy személy, vagy ha a felülvizsgálati funkció automatizált, de külön áll a kiadási vagy átadási funkciótól, az EIR hozzárendeli az információ felülvizsgálójának azonosítóját az információhoz és az információ címkéjéhez.
3. A szervezetnek gondoskodnia kell a felülvizsgálók vagy kiadók hitelesítő adatainak megőrzéséről, ha azok személyek.
4. Ha az információ felülvizsgálata automatizált, a szervezetnek biztosítania kell, hogy csak jóváhagyott felülvizsgálati funkciókat használjanak.
5. A szervezetnek naplót kell vezetnie minden lépésről, amelyet az információ megszerzése, tárolása és elemzése során tett, beleértve az összes személy azonosítóját, aki hozzáfért az információhoz, az információ gyűjtésének vagy átadásának dátumát és idejét, valamint az átadás célját.

6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a felügyeleti láncot, hogy biztosítsa az adatok naprakészségét és pontosságát.

Kapcsolódó intézkedések

2.28. Információáramlási szabályok érvényesítése

2.89. Biztonsági tulajdonságok

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.5.28

NIST SP 800-53 rev.5 referencia

AU-10(3)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

4.37. Letagadhatatlanság – az információt ellenőrző egyén személyazonossági kapcsolatának hitelesítése

4.37. A szervezet:

4.37.1. ellenőrzi az információt felülvizsgáló egyén személyazonosságának és a felülvizsgált információnak az összekapcsolását az információ átadási vagy kiadási pontjainál, a kiadás vagy az átadás előtt a szervezet által meghatározott biztonsági tartományokban; és

4.37.2. ellenőrzési hiba esetén végrehajtja az szervezet által meghatározott műveleteket.

Magyarázat

Az információk ellenőrzése során a felülvizsgáló személyazonosságának az információhoz való kötése az átadási vagy közzétételi pontokon megakadályozza az információ jogosulatlan módosítását a felülvizsgálat és az átadás, vagy közzététel között. A kapcsolatok hitelesítését kriptográfiai ellenőrző összegek (checksums) alkalmazásával lehet elérni. A szervezet meghatározza, hogy az ellenőrzések felhasználói kérésre történnek-e, vagy automatikusan generálódnak.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia a biztonsági tartományokat, ahol az információ átadása vagy kiadása történik.
2. A szervezetnek be kell vezetnie egy megoldást, amely ellenőrzi az információt felülvizsgáló egyén személyazonosságának és a felülvizsgált információnak az összekapcsolását.
3. A szervezetnek biztosítania kell, hogy az ellenőrzési folyamatok mind a felhasználói kérések alapján, mind az automatikusan generált események esetén végrehajtásra kerüljenek.
4. A szervezetnek meg kell határoznia és implementálnia kell azokat a műveleteket, amelyeket ellenőrzési hiba esetén végrehajtanak. Ez magában foglalhatja például a hibás tranzakciók visszavonását, a rendszer állapotának visszaállítását a hiba előtti állapotra, vagy a hibás tranzakciók javítását.
5. A szervezetnek naplóznia kell minden ellenőrzési eseményt és annak hibát, hogy nyomon követhető legyen a rendszer állapota és a hibák kezelési folyamata.

Kapcsolódó intézkedések

2.28. Információáramlási szabályok érvényesítése

2.89. Biztonsági tulajdonságok

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

AU-10(4)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

4.38. A NAPLÓBEJEGYZÉSEK MEGŐRZÉSE

4.38. A szervezet a naplóbejegyzéseket a jogszabályi és a szervezeten belüli információmegőrzési követelmények szerint meghatározott időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

MAGYARÁZAT

A szervezet a naplóbejegyzéseket addig őrzi meg, amíg meg nem állapítja, hogy azokra már nincs szükség és nem használhatók fel adminisztratív, jogi, naplózási vagy egyéb működési célokra. A naplóbejegyzések megőrzését és elérhetőségét biztosítani kell a vonatkozó jogszabályok szerint arra az esetre is, ha egy illetékes hatóság (pl.: rendvédelmi szerv) megkeresést küld a szervezetnek. A szervezet standard kategóriákat dolgoz ki a naplóbejegyzések számára az ilyen típusú intézkedésekkel kapcsolatban, és standard válaszadási folyamatot dolgoz ki minden egyes intézkedéstípushoz.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a naplóbejegyzések megőrzésének időtartamát, figyelembe véve az adminisztratív, jogi, naplózási és egyéb működési szempontokat.
2. A szervezetnek biztosítania kell a naplóbejegyzések elérhetőségét az esetleges hatósági megkeresések esetére.
3. A szervezetnek standard kategóriákat kell kialakítania a naplóbejegyzések besorolására.
4. A szervezetnek standard válaszadási folyamatokat kell kidolgoznia a hatósági keresések kezelésére.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.2. Naplózható események
4.5. Naplózás tárkapacitása
4.7. Naplózási hiba kezelése
4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel
4.25. Naplóinformációk védelme
4.48. Munkaszakasz-ellenőrzés
11.8. Adathordozók törlése

15.10. Sérülékenységmonitorozás és szkennelés

18.67. Információ kezelése és megőrzése

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

3.3.12.11. A naplóbejegyzések megőrzése: Az érintett szervezet a naplóbejegyzéseket meghatározott - a jogszabályi és az érintett szervezeten belüli információ megőrzési követelményeknek megfelelő - időtartamig megőrzi a biztonsági események utólagos kivizsgálásának biztosítása érdekében.

ISO/IEC 27001:2023 REFERENCIA

A.5.28; A.8.15

NIST SP 800-53 REV.5 REFERENCIA

AU-11

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a követelmények szerint meghatározott időtartamig történő megőrzés meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

4.39. A NAPLÓBEJEGYZÉSEK MEGŐRZÉSE – HOSSZÚ TÁVÚ VISSZAKERESÉSI KÉPESSÉG

4.39. A szervezet olyan intézkedéseket alkalmaz, amelyek biztosítják a rendszer által generált naplóbejegyzések hosszú távú visszakereshetőségét.

MAGYARÁZAT

A szervezetnek hozzá kell férnie a hosszú távú tárolást igénylő naplóbejegyzésekhez és biztosítania kell azok olvashatóságát (évenkénti időrendben). A naplóbejegyzések visszakeresésének megkönnyítése érdekében alkalmazott intézkedések közé tartozik a naplóbejegyzések konvertálása újabb formátumba, a naplóbejegyzések olvasására alkalmas berendezések megtartása, valamint a szükséges dokumentáció megőrzése, annak érdekében, hogy a személyzet megértse, hogyan kell értelmezni a bejegyzéseket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell a rendszer által generált naplóbejegyzések hosszú távú visszakereshetőségét.
2. A szervezetnek olyan intézkedéseket kell alkalmaznia, melyek biztosítják a naplóbejegyzések visszakeresésének megkönnyítését. A visszakereshetőség megkönnyítése érdekében alkalmazott intézkedések közé pl.: a naplóbejegyzések konvertálása újabb formátumba.
3. A szervezetnek meg kell tartania azokat az eszközöket, amelyek képesek olvasni a naplóbejegyzéseket, annak érdekében, hogy biztosítsa azok hosszú távú hozzáférhetőségét.
4. A szervezetnek meg kell tartania a szükséges dokumentációt, amely segít a személyzetnek megérteni, hogyan kell értelmezni a naplóbejegyzéseket. Ez magában foglalhatja a naplóbejegyzések formátumának, struktúrájának és tartalmának leírását.
5. A szervezetnek rendszeresen ellenőriznie kell ezeket az intézkedéseket, hogy biztosítsa a naplóbejegyzések hosszú távú visszakereshetőségét.

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

AU-11(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az intézkedések meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.40. NAPLÓBEJEGYZÉSEK LÉTREHOZÁSA

4.40. Az EIR:

4.40.1. Biztosítja a naplóbejegyzés generálási képességet a "Naplózható események" pontban meghatározott naplózható eseményekre.

4.40.2. Lehetővé teszi meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, hogy mely naplózható események legyenek naplózva az EIR egyes elemei által.

4.40.3. Naplóbejegyzéseket állít elő a "Naplózható események" pont szerinti eseményekre az "Naplóbejegyzések tartalma" pontban meghatározott tartalommal.

MAGYARÁZAT

Az EIR különböző elemeiből naplóbejegyzések generálhatóak. Az események utólagos kivizsgálásában támogatást nyújtó eseménytípusok azok az eseménytípusok, amelyekre naplóbejegyzéseket kell generálni, és ezek csak egy részét képezik az összes eseménytípusnak, amelyekre az EIR képes naplóbejegyzéseket generálni. Az eseménytípusokra vonatkozó előírások a "Naplózható események" kontrollnál kerültek bővebben kifejtésre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. Az EIR-nek képesnek kell lennie naplóbejegyzések generálni a "Naplózható események" pontban meghatározott előírásoknak megfelelően.

2. Az EIR-nek lehetővé kell tennie meghatározott személyeknek vagy szerepköröknek, hogy kiválasszák, mely naplózható események legyenek naplózva az EIR egyes elemei által.

3. Az EIR-nek naplóbejegyzéseket kell előállítania a "Naplózható események" pont szerinti eseményekre az "Naplóbejegyzések tartalma" pontban meghatározott tartalommal.

4. Az érintett szervezetnek biztosítania kell, hogy az EIR működése megfeleljen a fenti követelményeknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.60. Legkisebb jogosultság elve

2.100. Távoli hozzáférés

4.2. Naplózható események

4.3. Naplóbejegyzések tartalma

4.5. Naplózás tárkapacitása

4.7. Naplózási hiba kezelése

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.22. Naplóbejegyzések csökkentése és jelentéskészítés

4.48. Munkaszakasz-ellenőrzés

6.18. A változtatásokra vonatkozó hozzáférés korlátozások

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

3.3.12.12. Naplógenerálás

ISO/IEC 27001:2023 REFERENCIA

A.8.15

NIST SP 800-53 REV.5 REFERENCIA

AU-12

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

4.41. NAPLÓBEJEGYZÉSEK LÉTREHOZÁSA – AZ EGÉSZ RENDSZERRE KITERJEDŐ ÉS IDŐBELI NAPLÓZÁSI NYOMVONAL.

4.41. Az EIR a szervezet által meghatározott rendszerelemekből származó naplóbejegyzésekből egy rendszerszintű naplót állít össze, amely a szervezet által meghatározott tűréshatáron belüli időbélyegek alapján kerül összekapcsolásra.

MAGYARÁZAT

Az EIR naplóbejegyzéseinek időbelisége megfelelő, ha az egyes naplóbejegyzések időbélyegei megbízhatóan összekapcsolhatók más naplóbejegyzések időbélyegeivel. Ezáltal a szervezet által meghatározott tűréshatáron belül időrendi sorrend kerül létrehozásra a naplóbejegyzések között.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a rendszerelemeket, amelyekből naplóbejegyzéseket szeretne gyűjteni.
2. A szervezetnek meg kell határoznia a tűréshatárt, amelyen belül az időbélyegek alapján összekapcsolja a naplóbejegyzéseket. Ez azt jelenti, hogy a szervezetnek el kell döntenie, mennyi időeltolódás fogadható el a naplóbejegyzések időbélyegei között anélkül, hogy azok relevanciája vagy megbízhatósága veszélybe kerülne.
3. A szervezetnek úgy kell beállítania az EIR-t úgy, hogy az összegyűjtse ezeket a (a különböző rendszerelemekből származó) naplóbejegyzéseket, és összeállítson belőlük egy EIR-szintű naplót.
4. A szervezetnek rendszeresen ellenőriznie kell az EIR-szintű naplót, hogy az az elvárásoknak megfelelően működik.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.24. Időbélyegek

17.123. Rendszeridő szinkronizálása

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

3.3.12.12. Naplógenerálás

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-12(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerelemek, illetve a rendszerelemekből származó naplóbejegyzések időbélyegei közötti kapcsolati tűréshatár meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

4.42. NAPLÓBEJEGYZÉSEK LÉTREHOZÁSA – SZABVÁNYOS FORMÁTUMOK

4.42. Az EIR az egész rendszerre kiterjedő szabványos formátumú naplóbejegyzésekből álló naplót állít össze.

MAGYARÁZAT

A szabványokat alkalmazó naplóbejegyzések elősegítik az eszközök és az EIR-ek közötti átjárhatóságot és információcserét. Az átjárhatóság és az információcsere elősegítése megkönnyíti az eseményekkel kapcsolatos információk előállítását, amelyek könnyen elemezhetőek és összefüggésbe hozhatóak. Ha a naplózási mechanizmusok nem felelnek meg a szabványosított formátumoknak, az EIR-ek az egész EIR-re kiterjedő naplóállományok összeállításakor az egyes naplóbejegyzéseket szabványosított formátumokba alakítják át.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR naplóbejegyzései megfelelnek a szabványoknak. Ez elősegíti az átjárhatóságot és az információcserét az eszközök és az EIR között.
2. Ha az EIR naplózó mechanizmusai nem felelnek meg a szabványosított formátumoknak, akkor a szervezetnek gondoskodnia kell arról, hogy az EIR az egyes naplóbejegyzéseit szabványos formátumokra konvertálja, amikor összeállítja az egész EIR-re kiterjedő naplókat.
3. A szervezetnek folyamatosan ellenőriznie kell az EIR naplózó mechanizmusait, hogy biztosítsa a szabványos formátumoknak való megfelelést.

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

AU-12(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.43. Naplóbejegyzések létrehozása – Felhatalmazott személyek változtatásai

4.43. Az EIR lehetőséget biztosít a meghatározott személyeknek vagy szerepköröknek, hogy megváltoztassák az egyes rendszerelemek naplózását a meghatározott eseménykritériumok alapján egy meghatározott időtartamon belül.

Magyarázat

Az EIR lehetőséget biztosít a meghatározott személyeknek vagy szerepköröknek, hogy megváltoztassák az egyes rendszerelemek naplózását, lehetővé téve az érintett szervezetek számára, hogy szükség szerint kiterjesszék vagy korlátozzák a naplózást. A rendszererőforrások megőrzése érdekében korlátozott naplózást ki lehet terjeszteni (ideiglenesen vagy tartósan) bizonyos veszélyhelyzetek kezelésére. Ezen kívül a naplózás korlátozható az eseménytípusok egy meghatározott csoportjára, ezzel könnyítve a naplócsökkentést, az elemzést és a jelentéstételt. A szervezet időkorlátokat állíthat be, amelyeken belül a naplózási műveletek megváltoznak (pl. közel valós időben, perceken vagy órákon belül).

A követelmény alkalmazásának lépései

1. A szervezetnek lehetővé kell tennie a meghatározott személyek vagy szerepkörök számára, hogy megváltoztassák az EIR naplózását. Ez lehetővé teszi a szervezet számára, hogy szükség esetén kiterjessze vagy korlátozza a naplózást, annak érdekében, hogy megfeleljen a szervezeti követelményeknek.
2. A szervezetnek az EIR erőforrásainak megőrzése érdekében korlátozott naplózást kell alkalmaznia, amit ki lehet terjeszteni bizonyos veszélyhelyzetek kezelésére.
3. A szervezet a naplózást korlátozhatja az eseménytípusok egy meghatározott csoportjára, hogy megkönnyítse a naplócsökkentést, az elemzést és a jelentéstételt.
4. A szervezet időkorlátokat állíthat be, amelyekben a naplózási műveletek megváltoznak (pl. közel valós időben, perceken vagy órákon belül).

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése

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

3.3.12.12. Naplógenerálás

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-12(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a személyek és szerepek, illetve a rendszerelemek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

4.44. INFORMÁCIÓK KISZIVÁRGÁSÁNAK FIGYELEMMEL KÍSÉRÉSE

4.44. A szervezet:

4.44.1. Rendszeresen figyelemmel kíséri a meghatározott nyílt forrású információkat vagy információs oldalakat a szervezeti információk jogosulatlan nyilvánosságra hozatalának bizonyítékaiért.

4.44.2. Ha fény derül az információ nyilvánosságra hozatalára:

4.44.2.1. értesíti a meghatározott személyeket vagy szerepköröket; és

4.44.2.2. további meghatározott intézkedéseket hajt végre.

MAGYARÁZAT

Az információk jogosulatlan közzététele az adatszivárgás egyik formája. A nyílt forrású információk közé tartoznak például a közösségi média oldalakon, a kódmegosztó platformokon, tárhelyeken, valamint a sötét web (dark web) felületein megtalálható információk. A szervezeti információk közé tartoznak például a szervezet birtokában lévő személyes adatok vagy a szervezet által létrehozott, bizalmas információk.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek rendszeresen figyelemmel kell kísérnie a meghatározott nyílt forrású információkat vagy információs oldalakat pl.: közösségi média oldalak, kódmegosztó platformok, tárhelyek, dark web. A szervezet ezt többféle módon is megteheti, például időszakos OSINT (nyílt információgyűjtés) vizsgálat elvégzésével és/vagy a sötét weben (dark web) fellelhető információk folyamatos monitorozásával.
2. Ha a szervezet felfedezi, hogy olyan információ került nyilvánosságra, amely nem publikus, azonnal értesítenie kell a meghatározott személyeket vagy szerepköröket pl.: szervezet vezetői, a kiberbiztonságért felelős szervezeti egység, az adatvédelmi tisztviselő és a releváns hatóságok.
3. A szervezetnek további meghatározott intézkedéseket kell végrehajtania az információ jogosulatlan közzétételének kezelésére pl.: stratégia kidolgozása a nyilvános kommunikációra, biztonsági esemény esetén a megfelelő hatóságok értesítése.

4. A szervezetnek dokumentálnia kell a szervezeti információk jogosulatlan nyilvánosságra hozatalát, illetve az ezzel kapcsolatban megtett szervezeti intézkedéseket.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.124. Nyilvánosan elérhető tartalom

12.6. A fizikai belépés ellenőrzése

1.13. Belső fenyegetés elleni program

15.10. Sérülékenységmonitorozás és szkennelés

17.17. A határok védelme

18.80. Adatszivárgás észlelésének támogatása

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

A.8.12; A.8.16

NIST SP 800-53 REV.5 REFERENCIA

AU-13

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.45. Információ kiszivárgásának figyelemmel kísérése – Automatizált eszközök használata

4.45. A szervezet meghatározott automatizált mechanizmusok segítségével figyelemmel kíséri a nyílt forrású információkat és információs oldalakat.

Magyarázat

Az automatizált mechanizmusok közé sorolhatók olyan kereskedelmi forgalomban elérhető szolgáltatások, amelyek értesítéseket és riasztásokat biztosítanak a szervezetek számára. Az automatizált szkriptek is ide sorolhatók, melyek figyelemmel kísérik a weboldalakon megjelenő új bejegyzéseket.

A követelmény alkalmazásának lépései

A szervezetnek a 4.44-es pontban meghatározott intézkedések mellett az alábbiakat kell megtennie:

1. A szervezetnek be kell szereznie vagy le kell fejlesztenie olyan automatizált mechanizmusokat, amelyek képesek figyelemmel kísérni a meghatározott nyílt forrású információkat vagy oldalakat. Az automatizált mechanizmusok közé sorolhatók olyan kereskedelmi forgalomban elérhető szolgáltatások, amelyek értesítéseket és riasztásokat biztosítanak a szervezetek számára. Az automatizált szkriptek is ide sorolhatók, melyek figyelemmel kísérik a weboldalakon megjelenő új bejegyzéseket.
2. A szervezetnek úgy kell beállítania az automatizált mechanizmusokat, hogy rendszeresen ellenőrizzék a kiválasztott információkat és oldalakat. Ennek során az automatizált mechanizmusok értesítéseket küldhetnek, amikor új információk vagy frissítések érkeznek.
3. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell az automatizált mechanizmusok által gyűjtött információkat. Szükség esetén módosítani kell az automatizált mechanizmusok beállításait, illetve amennyiben a begyűjtött információ alapján indokolt, meg kell tenni a szükséges 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

AU-13(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az automatizált mechanizmusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.46. Információ kiszivárgásának figyelemmel kísérése – Figyelemmel kísért webhelyek felülvizsgálata

4.46. A szervezet meghatározott gyakorisággal felülvizsgálja a figyelemmel kísért nyílt forrású információs oldalak listáját.

Magyarázat

A figyelemmel kísért nyílt forrású információs oldalak aktuális listájának rendszeres felülvizsgálata segít abban, hogy a kiválasztott oldalak továbbra is relevánsak maradjanak. A felülvizsgálat lehetőséget ad arra is, hogy új nyílt forrású információs oldalak kerüljenek felvételre, amelyek bizonyítékot szolgáltathatnak a szervezeti információk jogosulatlan közzétételére. A figyelemmel kísért weboldalak listáját a fenyegetések felderítésére szolgáló, más hiteles információforrásokból származó információk alapján lehet összeállítani.

A követelmény alkalmazásának lépései

1. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a figyelemmel kísért nyílt forrású információs oldalak listáját. Szükség esetén módosítani kell a figyelemmel kísért oldalak listáját, ami azt is jelentheti, hogy új nyílt forrású információs oldal kerül felvételre a már meglévő listába. Emellett amennyiben a begyűjtött információ alapján indokolt, meg kell tenni a szükséges intézkedéseket.
2. A szervezetnek gondoskodnia kell a felülvizsgálattal kapcsolatos felelősségi feladatok ellátásáról.
3. A szervezetnek dokumentálnia kell a felülvizsgálatokat és az ahhoz köthetően megtett 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

AU-13(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a gyakoriság meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.47. Információ kiszivárgásának figyelemmel kísérése – Információk jogosulatlan másolása

4.47. A szervezet felderítési technikákat, folyamatokat és eszközöket alkalmaz annak meghatározására, hogy külső entitások jogosulatlan módon másolják-e a szervezeti információkat.

Magyarázat

A szervezeti információk külső entitások általi jogosulatlan felhasználása vagy másolása káros hatással lehet a szervezeti működésre és az eszközökre, beleértve a szervezeti hírnév sérülését is. Ilyen tevékenység lehet például egy szervezeti weboldal másolása egy támadó által, aki megpróbálja magát a weboldalt üzemeltető szervezetnek kiadni. A szervezeti információk külső entitások általi jogosulatlan másolásának megállapítására használt felderítési eszközök, technikák és folyamatok közé tartozik az internet irányából elérhető weboldalak átvizsgálása, a közösségi média figyelemmel kísérése, valamint a munkatársak képzése a szervezeti információk jogosulatlan felhasználásának felismerésére.

A követelmény alkalmazásának lépései

1. A szervezetnek be kell szereznie a megfelelő felderítő eszközöket, technikákat és folyamatokat, amelyek segítségével képes lesz meghatározni, hogy külső entitások jogosulatlanul másolják-e a szervezeti információkat. Ilyen tevékenység lehet például egy szervezeti weboldal másolása egy támadó által, aki megpróbálja magát a weboldalt üzemeltető szervezetnek kiadni.
2. A szervezetnek rendszeresen ellenőriznie kell, hogy külső entitások jogosulatlanul másolják-e a szervezeti információkat. A szervezet ezt többféle módon is megteheti, például időszakos OSINT (nyílt információgyűjtés) vizsgálat elvégzésével és/vagy a sötét weben (dark web) fellelhető információk folyamatos monitorozásával.
3. A szervezetnek dokumentálnia kell az elvégzett ellenőrzés eredményét és szükség esetén meg kell tennie a megfelelő intézkedéseket.

4. A szervezetnek rendszeresen felül kell vizsgálnia és szükség esetén frissítenie kell a felderítési technikáit, folyamatait és eszközeit, hogy biztosítsa azok hatékonyságát és naprakészségét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

AU-13(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.48. MUNKASZAKASZ-ELLENŐRZÉS

4.48. A szervezet:

4.48.1. Gondoskodik arról, hogy bizonyos felhasználók vagy szerepkörök meghatározott körülmények között rögzíthessék, megtekinthessék, meghallgathassák vagy naplózhassák egy felhasználói munkaszakasz tartalmát.

4.48.2. A munkaszakasz ellenőrzési tevékenységeket a hatályos jogszabályokkal, szabályzatokkal, irányelvekkel összhangban dolgozza ki és valósítja meg.

MAGYARÁZAT

A munkaszakaszok naplózása magában foglalja a billentyűleütések nyomon követését, a meglátogatott webhelyek nyilvántartását, valamint az információ- vagy fájlátvitelek rögzítését. A munkaszakaszok naplózási képessége az eseménynaplózás mellett kerül bevezetésre, és magában foglalhatja speciális munkaszakasz-felvételi technológia alkalmazását. A szervezetek mérlegelik, hogy a munkaszakaszok naplózása hogyan tárhat fel olyan információkat az egyénekről, amelyek adatvédelmi kockázatot jelenthetnek, valamint azt, hogy hogyan lehet ezeket a kockázatokat csökkenteni. Mivel a munkaszakaszok naplózása hatással lehet a rendszer és a hálózat teljesítményére, a szervezetek jól meghatározott helyzetekben aktiválják a képességet. A szervezet konzultálhat jogi tanácsadókkal, az állampolgári jogokért felelős biztossal és az adatvédelmi tisztviselőkkel annak biztosítása érdekében, hogy minden jogi, adatvédelmi, állampolgári jogi vagy polgári jogi kérdéssel - beleértve a személyazonosításra alkalmas információk felhasználását is - megfelelően foglalkozzanak.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek gondoskodnia kell a felhasználói munkaszakaszok tartalmának rögzítésére, megtekintésére, meghallgatására vagy naplózására feljogosított felhasználói vagy szerepköri feladatok ellátásáról.

2. A szervezetnek meg kell valósítania a munkaszakaszok ellenőrzési tevékenységeit a hatályos jogszabályokkal, szabályzatokkal és irányelvekkel összhangban. Ez magában foglalhatja a specializált munkaszakasz-felvételi technológiák bevezetését.

3. A szervezetnek figyelembe kell vennie, hogy a munkaszakaszok ellenőrzése információkat tárhat fel az érintett személyekről, amelyek adatvédelmi kockázatot jelenthetnek, és ezeket a kockázatokat mérlegelnie kell.
4. Mivel a munkaszakaszok ellenőrzése befolyásolhatja az EIR és a hálózat teljesítményét, a szervezetnek jól meghatározott helyzetekben célszerű csak aktiválnia ezt a képességet.
5. A szervezetnek szükség esetén konzultálnia kell jogi tanácsadókkal, állampolgári jogokért felelős biztossal és adatvédelmi tisztségviselőkkel, hogy biztosítsa, hogy minden jogi, adatvédelmi, állampolgári jogi vagy polgári jogi kérdéssel - beleértve a személyazonosításra alkalmas információk felhasználását is - megfelelően foglalkozzanak.

Kapcsolódó intézkedések

2.15. Hozzáférés-ellenőrzés érvényesítése
2.75.1. A rendszerhasználat jelzése
4.2. Naplózható események
4.3. Naplóbejegyzések tartalma
4.5. Naplózás tárkapacitása
4.7. Naplózási hiba kezelése
4.24. Időbélyegek
4.25. Naplóinformációk védelme
4.38. A naplóbejegyzések megőrzése
4.40. Naplóbejegyzések létrehozása

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

A.8.15

NIST SP 800-53 rev.5 referencia

AU-14

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.49. Munkaszakasz ellenőrzés – Rendszerindítás

4.49. Az EIR automatikusan elindítja a munkaszakasz ellenőrzéshez szükséges folyamatokat a rendszerindításkor.

Magyarázat

A rendszerindításkor automatikusan elinduló, a munkaszakaszok ellenőrzéséhez szükséges folyamatok abban segítenek, hogy az egyes személyek vonatkozásában begyűjtött információk teljeskörűek legyenek és ne lehessen azokat manipulálni.

A követelmény alkalmazásának lépései

1. A szervezetnek biztosítania kell, hogy az EIR automatikusan elindítja a munkaszakasz ellenőrzéséhez szükséges folyamatokat a rendszerindítás során.
2. A szervezetnek meg kell bizonyosodnia róla, hogy az EIR megfelelően rögzíti az egyes személyek munkaszakaszával kapcsolatos információkat.
3. A szervezetnek biztosítania kell, hogy az EIR által, az egyes személyek munkaszakaszával kapcsolatosan begyűjtött információkat ne lehessen manipulálni.

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

AU-14(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.50. MUNKASZAKASZ ELLENŐRZÉSE – TÁVOLI MEGFIGYELÉS ÉS LEHALLGATÁS

4.50. A szervezet biztosítja és megvalósítja azt a képességet, hogy az arra feljogosított felhasználók valós időben távolról megtekinthessék és meghallgathassák a létrehozott felhasználói munkaszakaszhoz kapcsolódó tartalmat.

MAGYARÁZAT

Az EIR-nek képes arra és biztosítja, hogy valós időben, távolról, az arra feljogosított felhasználók megtekinthessék és meghallgathassák a létrehozott felhasználói munkaszakaszhoz kapcsolódó tartalmat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek biztosítania kell, hogy az EIR rendelkezzen a szükséges technológiai képességekkel a valós idejű, távoli hozzáféréshez. Ez magában foglalhatja a megfelelő szoftverek és hardverek beszerzését, valamint a megfelelő hálózati infrastruktúra kiépítését.
2. A szervezetnek meg kell határoznia és be kell állítania a felhasználói jogosultságokat az EIR-ben ahhoz, hogy az arra felhatalmazott felhasználók hozzáférjenek a valós idejű, távoli hozzáférést biztosító funkcióhoz.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.100. Távoli 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

AU-14(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

4.51. SZERVEZETEN ÁTÍVELŐ NAPLÓZÁS

4.51. A szervezet meghatározott módszereket alkalmaz a meghatározott naplóinformációk külső szervezetekkel történő egyeztetésére, amikor a naplóinformációt a szervezeti határokon túlra továbbítják.

MAGYARÁZAT

Ha a szervezet külső szervezetek rendszereit vagy szolgáltatásait használja, akkor a naplózási képesség összehangolt, szervezeten átívelő megközelítést tesz szükségessé. Például a konkrét szolgáltatásokat igénylő egyének személyazonosságának biztosítása a szervezeti határokon átnyúlóan gyakran nehézségekbe ütközhet. Ezért gyakran előfordul, hogy a szervezeten átívelő naplózás csupán az eredeti rendszerben rögzíti a kérést benyújtó személyek személyazonosságát, és a többi rendszer csak azt rögzíti, hogy a kérések egy arra jogosult személytől származnak. A szervezet fontolóra veheti, hogy az információcsere-megállapodásokba belefoglalják a naplózási információk védelmére vonatkozó folyamatokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a módszereket, melyeket a meghatározott naplóinformációk külső szervezetekkel történő egyeztetésére kíván alkalmazni, amikor a naplóinformációt a szervezeti határokon túlra továbbítják.
2. A szervezetnek ki kell dolgoznia és alkalmaznia kell a meghatározott módszereket a naplóinformációk külső szervezetekkel történő egyeztetésére. Ez magában foglalhatja a naplóinformációk továbbításának módját, a naplóinformációk védelmét, valamint a naplóinformációk egyeztetésének folyamatát.
3. A szervezetnek figyelembe kell vennie a személyek azonosításának nehézségeit, akik különböző szolgáltatásokat igényelnek a szervezeti határokon túl. Ez jelentős teljesítménybeli kockázatokkal is járhat.
4. A szervezetnek be kell építenie a naplóinformációk követelményeinek és védelmének koordinálására vonatkozó folyamatokat az információcserére vonatkozó megállapodásokban.
5. A szervezetnek gondoskodnia kell arról, hogy a naplóinformációk megfelelően védettek legyenek, amikor azokat a szervezeti határokon túlra továbbítják.

Kapcsolódó intézkedések

4.3. Naplóbejegyzések tartalma

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

4.22. Naplóbejegyzések csökkentése és jelentéskészítés

5.6. Információcsere

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

AU-16

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a módszerek, illetve a naplóinformációk meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

4.52. Szervezeten átívelő naplózás – Naplóinformációk megosztása

4.52. A szervezet biztosítja a meghatározott naplóinformációkat a meghatározott szervezetek számára az adott információmegosztási megállapodások alapján.

Magyarázat

A naplózási információk elosztott jellege miatt a naplózási információk szervezeteken átívelő megosztása alapvető fontosságú lehet az elvégzett naplózás hatékony elemzéséhez. Például előfordulhat, hogy egy szervezet naplóbejegyzései nem nyújtanak elegendő információt ahhoz, hogy meghatározzák, hogy a más szervezeteknél dolgozó személyek megfelelően használják-e a szervezeti információs erőforrásokat. Bizonyos esetekben csak az adott személyek saját szervezete rendelkezik megfelelő ismeretekkel ennek megállapításához, így a naplózási információk szervezetek közötti megosztására van szükség.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia, hogy milyen naplóinformációkat kell megosztania a meghatározott szervezetekkel. Ez magában foglalhatja a hálózati tevékenységeket, a rendszereszközök használatát, a felhasználói műveleteket és más, a kiberbiztonsággal kapcsolatos tevékenységeket.
2. A szervezetnek létre kell hoznia egy információmegosztási megállapodást a meghatározott szervezetekkel. Ez a megállapodás részletezi, milyen információkat osztanak meg, hogyan és mikor történik a megosztás, és milyen biztonsági intézkedések vannak érvényben az információ védelme érdekében.
3. A szervezetnek biztosítania kell, hogy a naplóinformációk biztonságosan kerüljenek átadásra a meghatározott szervezeteknek. Ez magában foglalhatja az adatok titkosítását, a biztonságos átviteli csatornák használatát és az adatok sértetlenségének ellenőrzését.
4. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az információmegosztási megállapodásokat, hogy biztosítsa azok relevanciáját és hatékonyságát. Ez magában foglalhatja a megosztott információk típusának, a megosztás gyakoriságának és az alkalmazott módszereknek, valamint a biztonsági intézkedéseknek a felülvizsgálatát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

9.9.1. Biztonsági események kezelése

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

AU-16(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a szervezetek, illetve a meghatározott szervezetek számára az adott információmegosztási megállapodások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024