Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója

Azonosítás és hitelesítés

Verzió 1.0

NEMZETI KIBERVÉDELMI INTÉZET

2024

Tartalomjegyzék

8.1. SZABÁLYZAT ÉS ELJÁRÁSRENDEK

8.1. A szervezet:

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

8.1.1.1. a szervezeti-, folyamat és rendszerszintű követelményeket tartalmazó azonosítási és hitelesítési szabályzatot, amely

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

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

8.1.1.2. Az azonosítási és hitelesítési eljárásrendet, amely az azonosítási és hitelesítési szabályzat és az ahhoz kapcsolódó ellenőrzések megvalósítását segíti elő.

8.1.2. Kijelöl egy, a szervezet által meghatározott személyt, aki az azonosítási és hitelesítési szabályzat és eljárások kidolgozásának, dokumentálásának, kiadásának és megismertetésének irányításáért felel.

8.1.3. Felülvizsgálja és frissíti az aktuális azonosítási és hitelesítési szabályzatot és az azonosítási és hitelesítési eljárásokat és eljárásrendet a szervezet által meghatározott gyakorisággal és a szervezet által meghatározott események bekövetkezését követően.

MAGYARÁZAT

Az azonosítási és hitelesítési szabályzatnak és a kapcsolódó eljárásrend(ek)nek illeszkednie kell az érintett szervezet kockázatkezelési stratégiájához. A megfelelő minőségben és megfelelő szempontok mentén elkészített szabályzatok és eljárásrendek nagy mértékben járulnak hozzá a szervezet biztonságának megőrzéséhez. Az elkészült szabályzatoknak és eljárásrendeknek összhangban kell lenniük egymással és a szervezet információbiztonsági környezetével. A szervezeti szintű biztonsági szabályzatok és eljárásrendek használata általában előnyösebb, hiszen szükségtelenné teheti a különböző szervezeti célok vagy rendszerek szintjén kialakítandó szabályzatokat és eljárásrendeket. A szervezet azonban dönthet úgy (amennyiben a szervezet felépítése ezt indokolja), hogy a szabályzati szinten megjelenő követelményeket

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

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

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

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

KAPCSOLÓDÓ INTÉZKEDÉSEK

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

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

3.3.9.1. Azonosítási és hitelesítési 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

IA-1

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

8.2. AZONOSÍTÁS ÉS HITELESÍTÉS

8.2. A szervezet egyedileg azonosítja és hitelesíti a felhasználókat, és egyedi azonosítóhoz kapcsolja a felhasználók által végzett tevékenységeket.

MAGYARÁZAT

A szervezeti felhasználók közé tartoznak a munkavállalók vagy azok a személyek, akiket az érintett szervezet munkavállalókkal egyenértékű státuszúnak tekint. A felhasználók egyedi azonosítása és hitelesítése minden hozzáférésre vonatkozik, kivéve azokat, amelyeket az "azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek" követelmény kapcsán azonosítanak. Az érintett szervezet megkövetelheti az egyének egyedi azonosítását a csoportfiókokban az egyéni tevékenység részletes elszámoltathatósága érdekében.

A szervezet jelszavakat, fizikai hitelesítőket vagy biometriai adatokat használ a felhasználói azonosság hitelesítésére, vagy többtényezős hitelesítés esetén ezeknek valamilyen kombinációját. A szervezet EIR-jeihez való hozzáférés helyi hozzáférésnek vagy hálózati hozzáférésnek minősül. A helyi hozzáférés bármilyen hozzáférés az érintett szervezet EIR-jeihez a felhasználók vagy a felhasználók nevében cselekvő folyamatok által, ahol a hozzáférést közvetlen kapcsolatokon keresztül, hálózatok használata nélkül lehet elérni. A hálózati hozzáférés a szervezet EIR-jeihez való hozzáférés a felhasználók (vagy a felhasználók nevében eljáró folyamatok) által, ahol a hozzáférés hálózati kapcsolatokon keresztül lehetséges (azaz nem lokális). A távoli hozzáférés egy olyan hálózati hozzáférés típus, amely külső hálózatokon keresztüli kommunikációt foglal magában. A belső hálózatok magukban foglalhatják a helyi hálózatokat (LAN) és a széles körű hálózatokat (WAN).

A titkosított virtuális magánhálózatok (VPN) használata a hálózati kapcsolatokhoz a szervezet által ellenőrzött végpontok és nem szervezet által ellenőrzött végpontok között kezelhető belső hálózatokként a hálózaton áthaladó információk bizalmasságának és sértetlenségének védelme szempontjából.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a felhasználói körét, beleértve az munkavállalókat és azokat a személyeket, akiket a szervezet alkalmazottakkal egyenértékű státuszúnak tekint.

2. A szervezetnek egyedileg kell azonosítania és hitelesítenie a felhasználókat, kivéve a meghatározott eseteket.
3. A szervezetnek jelszavakat, fizikai hitelesítőket vagy biometrikus adatokat kell alkalmaznia a felhasználói azonosságok hitelesítésére, vagy többtényezős hitelesítés esetén ezek kombinációját.
4. A szervezetnek meg kell határoznia az EIR-hez való hozzáférés típusát (helyi, helyi hálózati, belső stb.).
5. A szervezetnek naplóznia kell, hogy nyomon követhesse a felhasználók által végzett tevékenységeket és azokat egyedi azonosítóhoz kapcsolhassa.
6. A szervezetnek meg kell határoznia azonosítási és hitelesítési követelményeket a nem szervezeti felhasználók számára, amelyeket az "Azonosítás és hitelesítés (szervezeten kívüli felhasználók)" követelménypontban került meghatározásra.

Kapcsolódó intézkedések

2.2. Fiókkezelés
2.15. Hozzáférés-ellenőrzés érvényesítése
2.28. Információáramlási szabályok érvényesítése
2.88. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek
2.100. Távoli hozzáférés
2.108. Vezeték nélküli hozzáférés
4.1. Szabályzat és eljárásrendek
4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel
8.14. Azonosító kezelés
8.21. A hitelesítésre szolgáló eszközök kezelése

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

3.3.9.2. Azonosítás és hitelesítés

ISO/IEC 27001:2023 referencia

A.5.16

NIST SP 800-53 REV.5 REFERENCIA

IA-2

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

8.3. AZONOSÍTÁS ÉS HITELESÍTÉS (FELHASZNÁLÓK) – PRIVILEGIZÁLT FIÓKOK TÖBBTÉNYEZŐS HITELESÍTÉSE

8.3. A szervezet többtényezős hitelesítést alkalmaz a privilegizált fiókokhoz való hozzáféréshez.

MAGYARÁZAT

A többtényezős hitelesítés megköveteli, hogy két vagy több különböző tényező kerüljön használatra a hitelesítés elvégzéséhez. A hitelesítési tényezőket a következőképpen határozzuk meg: valami, amit a személy tud (pl. jelszó), valami, amit birtokol (pl. fizikai hitelesítő, mint a kriptográfiai privát kulcs), vagy a személy valamilyen tulajdonsága (pl. biometrikus adat). A fizikai hitelesítőket tartalmazó többtényezős hitelesítési megoldások közé tartoznak a hardver hitelesítők, amelyek időalapú vagy hívás-válasz alapú megoldásokat biztosítanak. A szervezet a felhasználók hitelesítését az EIR szintjén (azaz bejelentkezéskor) végezhetik el, és saját belátásuk szerint alkalmazhatnak hitelesítési mechanizmusokat alkalmazások szintjén is a megnövelt biztonság érdekében. Függetlenül a hozzáférés típusától (azaz helyi, hálózati, távoli), a privilegizált fiókokat a kockázatnak megfelelő többtényezős hitelesítési megoldásokkal hitelesítik. A szervezet további biztonsági intézkedéseket is hozzáadhat, például további vagy szigorúbb hitelesítési mechanizmusokat bizonyos hozzáférési típusokhoz. A szervezet dokumentálja hitelesítési folyamatait és eljárásait, annak érdekében, hogy minden bejelentkezés nyomon követhető legyen.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely fiókokat tekinti privilegizáltnak. Ezek általában olyan fiókok, amelyeknek széleskörű jogosultságuk van az EIR-hez és/vagy érzékeny adatokhoz.
2. A szervezetnek ki kell választania egy többtényezős hitelesítési megoldást.
3. A szervezetnek be kell vezetnie a kiválasztott többtényezős hitelesítési megoldást az EIR-ben. Ez magában foglalja a szoftver telepítését, a hardver beállítását, és a felhasználók képzését.
4. A szervezetnek be kell állítania a többtényezős hitelesítést a privilegizált fiókokhoz.

5. A szervezetnek dokumentálnia kell a bevezetett megoldást, a hitelesítési folyamatot és eljárást.
6. A szervezet EIR-jének naplóznia kell a bejelentkezéseket. Ez magában foglalja a sikeres és sikertelen hitelesítési kísérletek rögzítését.
7. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a többtényezős hitelesítési szabályzatát és gyakorlatát, hogy biztosítsa a kiberbiztonsági követelményeknek való megfelelést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.59. Felelősségek szétválasztása
2.60. Legkisebb jogosultság elve

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

3.3.9.2. Azonosítás és hitelesítés

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IA-2(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

8.4. AZONOSÍTÁS ÉS HITELESÍTÉS (FELHASZNÁLÓK) – NEM-PRIVILEGIZÁLT FIÓKOK TÖBBTÉNYEZŐS HITELESÍTÉSE

8.4. A szervezet többtényezős hitelesítést alkalmaz a nem privilegizált fiókokhoz való hozzáféréshez.

MAGYARÁZAT

A többtényezős hitelesítés megköveteli, hogy két vagy több különböző tényező kerüljön használatra a hitelesítés elvégzéséhez. A hitelesítési tényezőket a következőképpen határozzuk meg: valami, amit a személy tud (pl. jelszó), valami, amit birtokol (pl. fizikai hitelesítő, mint a kriptográfiai privát kulcs), vagy a személy valamilyen tulajdonsága (pl. biometrikus adat). A fizikai hitelesítőket tartalmazó többtényezős hitelesítési megoldások közé tartoznak a hardver hitelesítők, amelyek időalapú vagy hívás-válasz alapú megoldásokat biztosítanak. A szervezet a felhasználók hitelesítését az EIR szintjén (azaz bejelentkezéskor) végezhetik el, és saját belátásuk szerint alkalmazhatnak hitelesítési mechanizmusokat alkalmazások szintjén is a megnövelt biztonság érdekében. Függetlenül a hozzáférés típusától (azaz helyi, hálózati, távoli), a privilegizált fiókokat a kockázatnak megfelelő többtényezős hitelesítési megoldásokkal hitelesítik. A szervezet további biztonsági intézkedéseket is hozzáadhat, például további vagy szigorúbb hitelesítési mechanizmusokat bizonyos hozzáférési típusokhoz. A szervezet dokumentálja hitelesítési folyamatait és eljárásait, annak érdekében, hogy minden bejelentkezés nyomon követhető legyen.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely fiókokat tekinti privilegizáltnak. Ezek általában olyan fiókok, amelyeknek széleskörű jogosultságuk van az EIR-hez és/vagy érzékeny adatokhoz.
2. A szervezetnek ki kell választania egy többtényezős hitelesítési megoldást.
3. A szervezetnek be kell vezetnie a kiválasztott többtényezős hitelesítési megoldást az EIR-ben. Ez magában foglalja a szoftver telepítését, a hardver beállítását és a felhasználók képzését.
4. A szervezetnek be kell állítania a többtényezős hitelesítést a privilegizált fiókokhoz.

5. A szervezetnek dokumentálnia kell a bevezetett megoldást, a hitelesítési folyamatot és eljárást.
6. A szervezet EIR-jének naplóznia kell a bejelentkezéseket. Ez magában foglalja a sikeres és sikertelen hitelesítési kísérletek rögzítését.
7. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a többtényezős hitelesítési szabályzatát és gyakorlatát, hogy biztosítsa a kiberbiztonsági követelményeknek való megfelelést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.59. Felelősségek szétválasztása

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

3.3.9.2. Azonosítás és hitelesítés

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IA-2(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

8.5. AZONOSÍTÁS ÉS HITELESÍTÉS (FELHASZNÁLÓK) – EGYÉNI AZONOSÍTÁS CSOPORTOS HITELESÍTÉSSEL

8.5. Amikor a szervezet közös használatú fiókokat vagy hitelesítő eszközöket alkalmaz, akkor a felhasználókat egyénileg azonosítja, mielőtt hozzáférést biztosítana a közös használatú fiókokhoz vagy erőforrásokhoz.

MAGYARÁZAT

A szervezetek gyakran használnak közös használatú fiókokat vagy hitelesítő eszközöket, hogy megkönnyítsék a felhasználók számára a hozzáférést az EIR-hez, azonban ezek a módszerek kockázatot jelentenek, mivel a felhasználók tevékenységei nehezen követhetők, és a hozzáférési jogosultságokat nehéz kezelni.

Ezért fontos, hogy az érintett szervezetek egyénileg azonosítsák a felhasználókat, mielőtt hozzáférést biztosítanának a közös használatú fiókokhoz vagy erőforrásokhoz. Ez azt jelenti, hogy minden felhasználónak saját egyedi hitelesítő adatai vannak, amelyeket az EIR ellenőriz, mielőtt hozzáférést biztosítana a közös használatú fiókokhoz vagy erőforrásokhoz.

Ez a folyamat segít a szervezetnek abban, hogy nyomon kövesse a felhasználók tevékenységeit, és biztosítsa, hogy csak a megfelelő jogosultságokkal rendelkező személyek férjenek hozzá az EIR-hez.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell vezetnie egy olyan hitelesítési rendszert, amely lehetővé teszi a felhasználók egyedi azonosítását. Ez magában foglalhatja a felhasználónevek és jelszavak, biometrikus adatok vagy más egyedi azonosítók használatát.
2. A szervezetnek biztosítania kell, hogy minden felhasználó, aki hozzáfér az EIR-hez, rendelkezik egy egyedi azonosítóval. Ez azt jelenti, hogy minden felhasználónak saját felhasználóneve és jelszava van, amelyet csak ő használhat.
3. A szervezetnek létre kell hoznia egy szabályzatot, amely előírja, hogy a felhasználóknak minden esetben saját, egyedi azonosítójukkal kell bejelentkezniük, mielőtt hozzáférhetnek a közös használatú fiókokhoz vagy erőforrásokhoz.

4. A szervezetnek naplózni kell minden egyes hozzáférési kísérletet az EIR-hez. Ez magában foglalja a sikeres és sikertelen bejelentkezést, valamint a hozzáférési kísérleteket a közös használatú fiókokhoz és erőforrásokhoz. A naplózás segít azonosítani a szabálytalan vagy gyanús tevékenységeket.
5. A szervezetnek rendszeresen felül kell vizsgálnia a naplókat, hogy azonosítsa a szabálytalan vagy gyanús tevékenységeket. Ha ilyen tevékenységet észlelnek, az érintett szervezetnek azonnal cselekednie kell, hogy megvédje az EIR-t.
6. A szervezet felhasználói számára képzést kell biztosítani a biztonságos hitelesítési gyakorlatokról, beleértve a közös használatú fiókok és erőforrások biztonságos használatát.

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

IA-2(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

8.6. AZONOSÍTÁS ÉS HITELESÍTÉS (FELHASZNÁLÓK) – HOZZÁFÉRÉS A FIÓKOKHOZ – KÜLÖNÁLLÓ ESZKÖZ

8.6. A szervezet többtényezős hitelesítést vezet be a privilegizált vagy nem privilegizált fiókokhoz való helyi, hálózati vagy távoli hozzáféréshez úgy, hogy:

8.6.1. az egyik tényezőt egy a rendszertől különálló eszköz biztosítja;

8.6.2. az eszköz megfelel a szervezet által meghatározott erősségű védelmi követelményeknek.

MAGYARÁZAT

A többtényezős hitelesítés során a cél, hogy az egyik tényezőhöz olyan eszközre van szükség, amely elkülönül attól a rendszertől, amelyhez a felhasználó hozzáférést kíván szerezni. Erre azért van szükség, hogy csökkentse a rendszerben tárolt azonosítási vagy hitelesítő adatok veszélyeztetésének valószínűségét. A támadók képesek lehetnek az ilyen azonosítási vagy hitelesítő adatok kompromittálására, és ezt követően jogosultsággal rendelkező felhasználóknak adhatják ki magukat. A tényezők egyikének külön eszközön történő megvalósítása erősebb mechanizmust és nagyobb szintű biztonságot nyújt a hitelesítési folyamatban.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a többtényezős hitelesítési rendszert, amelyet bevezet.
2. A szervezetnek biztosítania kell, hogy az egyik tényezőt egy, az EIR-től különálló eszköz biztosítja.
3. A szervezetnek meg kell határoznia a védelmi követelményeket, amelyeknek a kiválasztott hitelesítőeszköznek meg kell felelnie. Ezek a követelmények tartalmazhatják például az eszköz fizikai védelmét, a generált azonosítók erősségét, vagy az eszköz kommunikációjának biztonságát.
4. A szervezetnek implementálnia kell a többtényezős hitelesítést az EIR-ben. Ez magában foglalja a hitelesítési rendszer beállítását, a felhasználói fiókok konfigurálását, a hitelesítési tényezők bevezetését, valamint a felhasználók képzését a helyes használatra.

5. A szervezetnek naplózni kell minden egyes hozzáférési kísérletet az EIR-hez. Ez magában foglalja a sikeres és sikertelen bejelentkezést. A naplózás segít azonosítani a szabálytalan vagy gyanús tevékenységeket.
6. A szervezetnek rendszeresen felül kell vizsgálnia a többtényezős hitelesítési rendszert, hogy biztosítsa annak megfelelő működését és a védelmi követelményeknek való megfelelést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.60. Legkisebb jogosultság elve

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IA-2(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.7. AZONOSÍTÁS ÉS HITELESÍTÉS (FELHASZNÁLÓK) – HOZZÁFÉRÉS A FIÓKOKHOZ – VISSZAJÁTSZÁS ELLENI VÉDELEM

8.7. A szervezet visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat alkalmaz a privilegizált és a nem privilegizált fiókokhoz való hozzáféréshez.

MAGYARÁZAT

A szervezetnek biztosítania kell, hogy a hitelesítési mechanizmusokat alkalmazzák mind a privilegizált, mind a nem privilegizált fiókokhoz való hozzáféréshez. A privilegizált fiókok olyan fiókok, amelyeknek kiterjedt jogosultságaik vannak az EIR-hez, és képesek változtatni az EIR működését vagy beállításait. A nem privilegizált fiókok korlátozottabb hozzáféréssel rendelkeznek az EIR-hez.

A visszajátszás elleni védelem biztosítása érdekében az érintett szervezetnek naplózásra és monitorozásra is szüksége van. A naplózás segít azonosítani a visszajátszásos támadásokat, míg a monitorozás lehetővé teszi az érintett szervezet számára, hogy észlelje a visszajátszásos támadásokat és azonnal reagáljon rájuk.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy mely fiókokat tekinti privilegizáltnak és melyeket nem.
2. A szervezetnek implementálnia kell a visszajátszás elleni védelmet biztosító hitelesítési mechanizmusokat. Ez magában foglalhatja a protokollokat, amelyek ún. kihívásokat használnak, mint például időszinkron vagy kriptográfiai hitelesítők.
3. A szervezetnek biztosítania kell, hogy ezek a hitelesítési mechanizmusok mind a privilegizált, mind a nem privilegizált fiókokhoz való hozzáféréshez alkalmazva legyenek.
4. A szervezetnek tesztelnie kell a hitelesítési mechanizmusokat, hogy biztosítsa, hogy azok hatékonyan működnek a visszajátszás elleni védelem érdekében.
5. A szervezetnek naplóznia kell a hitelesítési folyamatokat, hogy nyomon követhesse a hitelesítési kísérleteket és azonosíthassa a visszajátszásra utaló jeleket.

6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hitelesítési mechanizmusokat, hogy biztosítsa, hogy azok naprakészek és hatékonyak maradnak a visszajátszás elleni védekezésben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.9.2. Azonosítás és hitelesítés

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IA-2(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

8.8. AZONOSÍTÁS ÉS HITELESÍTÉS (FELHASZNÁLÓK) – EGYSZERI BEJELENTKEZÉS (SSO)

8.8. A szervezet biztosítja, hogy az egyszeri bejelentkezési képesség (SSO) rendelkezésre álljon a meghatározott rendszerfiókok és szolgáltatások számára.

MAGYARÁZAT

Az egyszeri bejelentkezési képesség (SSO) lehetővé teszi a felhasználók számára, hogy egyszeri bejelentkezéssel hozzáférjenek több EIR erőforráshoz. A szervezet mérlegeli az egyszeri bejelentkezési képesség által nyújtott hatékonyságot azzal a kockázattal, amelyet az egyetlen hitelesítési esemény révén több EIR-hez való hozzáférés engedélyezése jelent. Az egyszeri bejelentkezés lehetőséget teremthet az EIR biztonságának javítására, például azzal, hogy képes hozzáadni a többtényezős hitelesítést azokhoz az alkalmazásokhoz és EIR-ekhez (létező és új), amelyek esetleg nem képesek natívan támogatni a többtényezős hitelesítést.

A szervezet biztosítja, hogy az egyszeri bejelentkezési képesség rendelkezésre álljon a meghatározott EIR fiókok és szolgáltatások számára. Ez azt jelenti, hogy a felhasználóknak csak egyszer kell bejelentkezniük, és hozzáférhetnek az összes szükséges EIR-hez anélkül, hogy minden egyes EIR-hez külön-külön kellene bejelentkezniük. Ez nemcsak a felhasználói élményt javítja, hanem csökkenti a hitelesítési hibák számát is, amelyek gyakran biztonsági eseményekhez vezetnek.

Az egyszeri bejelentkezési képesség (SSO) használatakor azonban fontos, hogy a szervezet naplózza és rendszeresen ellenőrizze a hitelesítési eseményeket. Ez segít azonosítani a rendellenes vagy gyanús tevékenységeket, és lehetővé teszi a gyors reagálást a potenciális biztonsági eseményekre.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell választania és be kell vezetnie egy megfelelő SSO megoldást, amely kompatibilis az EIR-jével és a használt szolgáltatásokkal.
2. A szervezetnek be kell állítania az SSO-t az összes meghatározott EIR fiók és szolgáltatás számára. Ez magában foglalja a felhasználói hitelesítési adatok összekapcsolását az SSO rendszerrel.

3. Az szervezetnek tesztelnie kell az SSO működését, hogy biztosítsa a hibamentes bejelentkezést és a szolgáltatásokhoz való hozzáférést.
4. A szervezetnek be kell vezetnie a többtényezős hitelesítést, hogy növelje az EIR biztonságát. Ez különösen fontos, mivel az SSO lehetővé teszi a felhasználók számára, hogy egyetlen bejelentkezéssel hozzáférjenek több szolgáltatáshoz.
5. A szervezetnek naplóznia és monitoroznia kell a sikeres és sikertelen bejelentkezési kísérleteket, hogy nyomon követhesse a felhasználói tevékenységeket és azonosíthassa a potenciális biztonsági problémákat. A naplózás segíthet a rendellenes tevékenységek azonosításában és a rendszer biztonságának javításában.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az SSO beállításait, hogy biztosítsa a rendszer biztonságát és hatékonyságát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IA-2(10)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerfiókok és szolgáltatások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.9. AZONOSÍTÁS ÉS HITELESÍTÉS (FELHASZNÁLÓK) – MÁSODLAGOS HITELESÍTÉSI CSATORNA

8.9. A szervezet másodlagos hitelesítési csatornát alkalmaz, az általa meghatározott feltételek fennállása esetén, a kért művelet vagy hitelesítés ellenőrzése érdekében.

MAGYARÁZAT

A másodlagos hitelesítési csatorna azt jelenti, hogy az érintett szervezet két különálló kommunikációs csatornát használ felhasználók vagy eszközök azonosítására és hitelesítésére az EIR-ben. Az első csatorna a felhasználók vagy eszközök azonosítására és hitelesítésére szolgál, és általában ez az, amelyen keresztül az információ áramlik. A másodlagos csatorna függetlenül ellenőrzi a hitelesítést és/vagy a kért műveleteket. Például egy felhasználó hitelesít egy notebook számítógépen egy távoli szerverhez, amelyhez hozzáférést szeretne, és kezdeményezi a szerver valamilyen műveletének végrehajtását ezen a kommunikációs csatornán keresztül. Ezt követően a szerver a felhasználó mobiltelefonján keresztül lép kapcsolatba a felhasználóval, hogy ellenőrizze, hogy a kért művelet valóban a felhasználótól származik-e. A felhasználó megerősítheti a szándékolt műveletet egy telefonon keresztül, vagy hitelesítő kódot adhat meg telefonon keresztül. A másodlagos hitelesítési csatornát a "man-in-the-middle" támadások enyhítésére lehet használni.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia a két kommunikációs csatornát, amelyeket az EIR felhasználóinak vagy eszközeinek azonosítására és hitelesítésére használnak. Az első útvonal az azonosításra és hitelesítésre szolgál, míg a második útvonal (azaz az out-of-band útvonal) függetlenül ellenőrzi a hitelesítést és/vagy a kért műveletet.
2. A szervezetnek be kell állítania az EIR-t úgy, hogy a felhasználók vagy eszközök hitelesítése után a rendszer külön kommunikációs csatornán keresztül ellenőrizze a kért műveletet.
3. A szervezetnek meg kell határoznia a másodlagos hitelesítési csatorna aktiválásának feltételeit vagy kritériumait. Ezek a feltételek magukban foglalhatják a gyanús tevékenységeket, az új fenyegetés jeleit, a fenyegetettség megnövekedését, vagy a kért tranzakciókban szereplő információk hatását vagy besorolási szintjét.

4. A szervezetnek naplóznia kell az összes hitelesítési és ellenőrzési műveletet, hogy nyomon követhető legyen a rendszerben történő tevékenység, és hogy az érintett szervezet képes legyen azonosítani és kezelni az esetleges biztonsági eseményeket.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a másodlagos hitelesítési csatorna használatának szabályzatait és eljárásait, hogy biztosítsa az EIR biztonságát és hatékonyságát.

Kapcsolódó intézkedések

8.42. Helyzetfüggő hitelesítés
8.43. Újrahitelesítés
17.105. Sávon kívüli csatornák

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

IA-2(13)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a feltételek illetve a másodlagos hitelesítési csatorna meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

8.10. ESZKÖZÖK AZONOSÍTÁSA ÉS HITELESÍTÉSE

8.10. A szervezet egyedileg azonosítja és hitelesíti a meghatározott eszközöket, vagy eszköztípusokat, mielőtt helyi, távoli, hálózati vagy egyéb kapcsolatot létesítene velük.

MAGYARÁZAT

Az érintett szervezet által egyedileg azonosítandó és hitelesítendő eszközök típusonként, eszközönként, vagy ezek kombinációjában kerülhetnek meghatározásra. Az érintett szervezet által meghatározott eszköztípusok tartalmazzák azokat az eszközöket is, amelyek nem az érintett szervezet tulajdonában vannak. Az EIR ismert, megosztott információkat használ az eszközök azonosítására, vagy szervezeti hitelesítési megoldásokat (pl. IEEE 802.1x és EAP, RADIUS szerver EAP-TLS hitelesítéssel, Kerberos, stb.) az eszközök azonosítására és hitelesítésére a helyi vagy távoli hálózatokon. Az érintett szervezetek meghatározhatják a hitelesítési mechanizmusok szükséges erősségét az EIR biztonsági osztálya és az alapfeladatok vagy üzleti követelmények alapján.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet először határozza meg azokat az eszközöket vagy eszköztípusokat, amelyek egyedi azonosítást és hitelesítést igényelnek. Ez magában foglalhatja azokat az eszközöket is, amelyek nem az érintett szervezet tulajdonában vannak.
2. A szervezet meghatározza a hitelesítési mechanizmusok szükséges erősségét az EIR biztonsági osztálya és az alapfeladatok vagy üzleti követelmények alapján. Mivel az eszközhitelesítés átfogó bevezetése kihívásokkal jár, az érintett szervezet korlátozhatja a szabályozás alkalmazását egy meghatározott számú/típusú eszközre.
3. A szervezet naplózza és nyomon követi az eszközök azonosításának és hitelesítésének folyamatát, hogy biztosítsa a kiberbiztonsági követelményeknek való megfelelést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.100. Távoli hozzáférés
2.108. Vezeték nélküli hozzáférés
2.113. Mobil eszközök hozzáférés-ellenőrzése

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

5.6. Információcsere

5.24. Belső rendszerkapcsolatok

8.14. Azonosító kezelés

8.21. A hitelesítésre szolgáló eszközök kezelése

8.41. Szolgáltatás azonosítása és hitelesítése

8.43. Újrahitelesítés

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

3.3.9.3. Eszközök azonosítása és hitelesítése: Az elektronikus információs rendszer egyedileg azonosítja és hitelesíti a meghatározott eszközöket, vagy eszköz típusokat mielőtt helyi vagy távoli hálózati kapcsolatot létesítene velük.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IA-3

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az eszközök és eszköztípusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

8.11. Eszközök azonosítása és hitelesítése – Kétirányú kriptográfiai hitelesítés

8.11. A szervezet hitelesíti a szervezet által meghatározott eszközöket vagy eszköztípusokat, mielőtt kétirányú kriptográfiai hitelesítéssel helyi vagy távoli hálózati, vagy egyéb kapcsolatot létesítene velük.

Magyarázat

A kétirányú kriptográfiai hitelesítés erősebb védelmet nyújt az eszközök kilétének igazolásához nagyobb kockázatú kapcsolatok esetén.
Az érintett szervezetnek biztosítania kell, hogy az EIR-jéhez csatlakozó eszközök megfelelnek a szervezet által meghatározott biztonsági követelményeknek. Ez magában foglalja a naplózást és a rendszeres ellenőrzéseket is, hogy biztosítsák az eszközök megfelelő működését és a hitelesítési folyamatok betartását.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia és hitelesítenie azokat az eszközöket vagy eszköztípusokat, amelyekkel kétirányú kriptográfiai hitelesítést tervez létrehozni. Ez magában foglalja az eszközök specifikációinak, biztonsági jellemzőinek és egyéb releváns információinak összegyűjtését és ellenőrzését.
2. Miután az eszközöket azonosították, a szervezetnek implementálnia kell a kétirányú kriptográfiai hitelesítést. Ez azt jelenti, hogy mind az EIR, mind az eszközöknek képesnek kell lenniük azonosítani és hitelesíteni egymást, mielőtt adatokat cserélnek.
3. A szervezetnek biztosítania kell, hogy az EIR és az eszközök közötti kapcsolat biztonságos, és hogy a kriptográfiai hitelesítés megfelelően működik. Ez magában foglalhatja a kapcsolat tesztelését és a hitelesítési folyamat ellenőrzését.
4. A szervezetnek naplót kell vezetnie az eszközök hitelesítéséről és a kétirányú kriptográfiai hitelesítésről. Ez magában foglalja az eszközök hitelesítésének dátumát, időpontját és eredményét, valamint a kriptográfiai hitelesítési folyamat minden lépését.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hitelesítési folyamatot és a kétirányú kriptográfiai hitelesítést, hogy biztosítsa azok hatékonyságát és biztonságát. Ez

magában foglalhatja a hitelesítési folyamatok és a kriptográfiai hitelesítési technikák felülvizsgálatát és frissítését, valamint az eszközök újrahitelesítését, ha szükséges.

KAPCSOLÓDÓ INTÉZKEDÉSEK

17.40. Az adatátvitel bizalmassága és sértetlensége
17.49. Kriptográfiai kulcs előállítása és kezelése
17.53. Kriptográfiai védelem

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IA-3(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az eszközök és eszköztípusok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.12. Eszközök azonosítása és hitelesítése – Dinamikus címkiosztás

8.12. A szervezet:

8.12.1. dinamikus címkiosztás esetén standardizálja a meghatározott címkiosztással kapcsolatos információk tárolását és a bérleti időtartamot; valamint

8.12.2. ellenőrzi a címkiosztással kapcsolatos információkat a címek kiosztásakor.

Magyarázat

Az érintett szervezetnek a dinamikus címkiosztás (DHCP) esetén szükséges egységesítenie a meghatározott címkiosztással kapcsolatos információk tárolását és a bérleti időtartamot (DHCP lease time). Ez azt jelenti, hogy az érintett szervezetnek egyértelműen meg kell határoznia és követnie kell a címkiosztási eljárásokat.

A bérleti időtartam a címek kiosztásának ideje, amelyet az EIR határoz meg. Ez az időszak lehet rövid, például néhány óra, vagy hosszú, akár több hét is. Az érintett szervezetnek gondoskodnia kell arról, hogy a bérleti időtartam megfelelő legyen a címek kiosztásának szükségleteihez.

Az érintett szervezetnek ellenőriznie kell a címkiosztással kapcsolatos információkat a címek kiosztásakor. Ez azt jelenti, hogy az EIR-nek naplóznia kell a címkiosztási tevékenységeket, beleértve a kiosztott címeket, a bérleti időtartamot és a címek használatának időpontjait. Az ellenőrzés segít az érintett szervezetnek abban, hogy nyomon kövesse a címek kiosztását, és biztosítsa a címkiosztási eljárások betartását.

A követelmény alkalmazásának lépései

1. A szervezetnek be kell vezetnie a dinamikus címkiosztást, például a DHCP használatával, amely lehetővé teszi a kliensek számára, hogy dinamikusan kapjanak hálózati címet.
2. A szervezetnek standardizálnia kell a meghatározott címkiosztással kapcsolatos információk tárolását az EIR-ben. Ez azt jelenti, hogy az összes címkiosztási információt egységes formátumban kell tárolni, hogy könnyen hozzáférhető és érthető legyen.
3. A szervezetnek be kell állítania a bérleti időtartamot a dinamikus címkiosztás esetén.

4. A szervezetnek ellenőriznie kell a címkiosztással kapcsolatos információkat a címek kiosztásakor. Ez azt jelenti, hogy az EIR-nek naplóznia kell a címkiosztási eseményeket, beleértve a kiosztott címeket, a kiosztás időpontját és a bérleti időtartamot.
5. A szervezetnek rendszeresen felül kell vizsgálnia és ellenőriznie kell a címkiosztási naplókat, hogy biztosítsa a kiberbiztonsági követelményeknek való megfelelést. Amennyiben bármilyen rendellenességet észlelnek, az érintett szervezetnek azonnal cselekednie kell a probléma megoldása érdekében.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.2. Naplózható események

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

IA-3(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.13. ESZKÖZÖK AZONOSÍTÁSA ÉS HITELESÍTÉSE – ESZKÖZTANÚSÍTVÁNYOK

8.13. A szervezet az általa meghatározott konfigurációkezelési folyamatok mentén kezeli az eszközök azonosításához és hitelesítéséhez használt tanúsítványokat

MAGYARÁZAT

Az eszköz tanúsítása a leggyakoribb esetben egy kriptográfiai hash segítségével történik. Ha az eszköz tanúsítása az azonosítás és hitelesítés eszköze, akkor fontos, hogy az eszközön végrehajtott javításokat és frissítéseket egy konfigurációkezelési folyamat mentén kezeljék, hogy a javítások és frissítések biztonságosan történjenek meg, és ne zavarják meg az azonosítást és hitelesítést más eszközökkel szemben.

Az érintett szervezetnek tehát gondoskodnia kell arról, hogy az EIR konfigurációkezelési folyamatai megfelelően kezeljék az eszközök tanúsítványait. Ez magában foglalja a tanúsítványok létrehozását, kezelését, tárolását és törlését, valamint a tanúsítványokkal kapcsolatos naplózást és biztonsági intézkedéseket.

A konfigurációkezelési folyamatoknak biztosítaniuk kell, hogy az eszközök tanúsítványai mindig naprakészek és biztonságosak legyenek. Ez magában foglalja a tanúsítványok rendszeres frissítését, a tanúsítványokkal kapcsolatos biztonsági események kezelését, és a tanúsítványok érvényességének ellenőrzését.

Az érintett szervezetnek továbbá biztosítania kell, hogy a konfigurációkezelési folyamatok összhangban vannak a szervezet biztonsági szabályaival és eljárásaival, és hogy a folyamatokat rendszeresen felülvizsgálják és frissítik a biztonsági környezet változásainak megfelelően.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a konfigurációkezelési folyamatokat, amelyek mentén kezeli az eszközök azonosításához és hitelesítéséhez használt tanúsítványokat.
2. A szervezetnek be kell vezetnie egy eszköz-igazolási rendszert, amely az eszközök konfigurációján és ismert működési állapotán alapul.

3. A szervezetnek biztosítania kell, hogy az EIR frissítései és javításai a konfigurációkezelési folyamatok mentén történjenek, hogy a frissítések és javítások biztonságosak legyenek, és ne zavarják az azonosítást és hitelesítést más eszközökkel szemben.
4. A szervezetnek rendszeresen ellenőriznie kell az EIR konfigurációját, hogy biztosítsa a tanúsítványok érvényességét és a hitelesítési folyamatok megfelelőségét.
5. A szervezetnek naplót kell vezetnie az összes konfigurációkezelési tevékenységről, beleértve az eszközök azonosítását és hitelesítését, valamint a frissítéseket és javításokat. Ez a napló segíthet az esetleges problémák azonosításában és a jövőbeni hitelesítési folyamatok javításában.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a konfigurációkezelési folyamatokat, hogy biztosítsa azok hatékonyságát és megfelelőségét a változó kiberbiztonsági követelményeknek.

Kapcsolódó intézkedések

6.2. Alapkonfiguráció
6.7. A konfigurációváltozások felügyelete (változáskezelés)
6.23. Konfigurációs beállítások

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

IA-3(4)

A követelményhez meghatározandó paraméterek

A követelménypontho kapcsolódó szervezeti feladat a konfigurációkezelési folyamat meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.14. AZONOSÍTÓ KEZELÉS

8.14. A szervezet:

8.14.1. Az egyéni, csoport, szerepkör vagy eszköz azonosítók kiosztását a szervezet által meghatározott személyek vagy szerepkörök engedélyéhez köti.

8.14.2. Kiválaszt egy azonosítót, amely azonosítja az egyént, csoportot, szerepkört, szolgáltatást vagy eszközt.

8.14.3. Hozzárendeli az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz, szolgáltatáshoz vagy eszközhöz.

8.14.4. Meghatározott ideig megakadályozza az azonosítók újbóli felhasználását.

MAGYARÁZAT

A gyakran használt eszközazonosítók közé tartoznak például a MAC vagy az IP címek vagy az eszközök egyedi azonosítói. Megosztott, nem nevesített azonosítók nem alkalmazhatók egyéni azonosítóként. Az egyedi azonosítók általában azon felhasználónevek, melyek adott személyhez lettek rendelve. Ez a biztonsági követelmény azon egyedi azonosítókra is kiterjed, melyek nem feltétlen kapcsolódnak az EIR fiókokhoz. Az azonosítók újbóli felhasználásának megakadályozása azt jelenti, hogy a korábban használt egyén, csoport, szerepkör vagy eszköz azonosítók újbóli hozzárendelése nem megengedett különböző egyénekhez, csoportokhoz, szerepekhez vagy eszközökhöz. Ez azért fontos, mert az azonosító korábbi tulajdonosa, ismerője így nem tud visszaélni az információval, nem keletkezik elszámoltathatósági probléma.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a személyeket vagy szerepköröket, akik jogosultak az egyéni, csoport, szerepkör vagy eszköz azonosítók kiosztására. Ez magában foglalhatja a kiberbiztonsági csapatot, az IT menedzsmentet vagy más releváns szerepköröket.
2. A szervezetnek ki kell választania egy azonosítót, amely azonosítja az egyént, csoportot, szerepkört, szolgáltatást vagy eszközt. Ez lehet például MAC cím, IP cím, vagy eszköz-specifikus token.

3. A szervezetnek hozzá kell rendelnie az azonosítót a kívánt egyénhez, csoporthoz, szerepkörhöz, szolgáltatáshoz vagy eszközhöz. Ez általában az EIR felhasználói fiókok felhasználóneveinek hozzárendelését jelenti az adott személyekhez.
4. A szervezetnek meg kell akadályoznia az azonosítók újbóli felhasználását egy meghatározott időszakon belül. Ez azt jelenti, hogy meg kell akadályoznia, hogy a korábban használt egyéni, csoport, szerepkör, szolgáltatás, vagy eszköz azonosítókat más személyekhez, csoportokhoz, szerepkörökhöz, szolgáltatásokhoz vagy eszközökhöz rendeljék.
5. A szervezetnek dokumentálnia kell az azonosítók kiosztását és használatát, hogy nyomon követhető legyen az azonosítók használata és a hozzájuk rendelt személyek, csoportok, szerepkörök, szolgáltatások és eszközök.

Kapcsolódó intézkedések

2.59. Felelősségek szétválasztása
8.2. Azonosítás és hitelesítés
8.10. Eszközök azonosítása és hitelesítése
8.21. A hitelesítésre szolgáló eszközök kezelése
8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)
8.41. Szolgáltatás azonosítása és hitelesítése
8.44. Személyazonosság igazolása
10.11. Távoli karbantartás
12.2. A fizikai belépési engedélyek
12.6. A fizikai belépés ellenőrzése

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

3.3.9.4. Azonosító kezelés

ISO/IEC 27001:2023 referencia

A.5.16

NIST SP 800-53 rev.5 referencia

IA-4

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

8.15. AZONOSÍTÓ KEZELÉS – FIÓKAZONOSÍTÓK NYILVÁNOS AZONOSÍTÓKÉNT VALÓ HASZNÁLATÁNAK TILTÁSA

8.15. A szervezet megtiltja, hogy fiókok azonosítói megegyezzenek az egyéni fiókok nyilvánosan hozzáférhető azonosítóival.

MAGYARÁZAT

A fiókok nyilvános azonosítóként való használatának tilalma kiterjed minden nyilvánosan közzétett fiók azonosítóra, amelyeket kommunikációra, például elektronikus levelezésre és azonnali üzenetküldésre használnak. Az olyan rendszerfiók-azonosítók használatának tiltása szükséges, amelyek megegyeznek valamely nyilvános azonosítóval, például az elektronikus levelezési cím egyéni azonosító részével. Ez megnehezíti a támadók számára a felhasználói azonosítók kitalálását. A fiókazonosítók nyilvános azonosítóként való tiltása más támogató intézkedések végrehajtása nélkül csak megnehezíti az azonosítók kitalálását. A fiók védelméhez további védelemre van szükség az azonosító és a hitelesítő adatok esetében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia és azonosítania kell az összes olyan fiókot, amelynek azonosítói nyilvánosan hozzáférhetőek.
2. A szervezetnek meg kell tiltania, hogy az EIR fiókazonosítói megegyezzenek a nyilvánosan hozzáférhető azonosítókkal. Ez azt jelenti, hogy az egyéni azonosítók, például az elektronikus levelezési címek, nem lehetnek azonosak az EIR fiókazonosítókkal.
3. A szervezetnek további védelmi intézkedéseket kell bevezetnie az azonosítók kitalálásának megnehezítése érdekében. Ez magában foglalhatja a hitelesítő adatok és a hozzáférési jogosultságok szigorúbb kezelését.
4. A szervezetnek dokumentálnia kell a fiókazonosítókat, hogy nyomon követhesse a fiókok használatát és az esetleges biztonsági eseményeket. A dokumentálás segíthet azonosítani a rendszerben lévő biztonsági réseket és megakadályozhatja a jövőbeni biztonsági eseményeket.
5. A szervezetnek folyamatosan felül kell vizsgálnia és frissítenie kell a biztonsági szabályait, hogy megfeleljen a változó kiberbiztonsági környezetnek és fenyegetéseknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

3.2. Biztonságtudatossági képzés

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IA-4(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.16. AZONOSÍTÓ KEZELÉS – FELHASZNÁLÓI STÁTUSZ AZONOSÍTÁSA

8.16. A szervezet a felhasználói azonosítókhoz státuszjelölést rendel.

MAGYARÁZAT

Az érintett szervezet a felhasználói azonosítókhoz státuszjelölést rendel. A státuszjelölések olyan jellemzőket tartalmaznak, amelyek az egyének státuszát azonosítják, mint például szerződéses munkavállalók, külföldi állampolgárok és a szervezeten kívüli felhasználók. Az egyének státuszának azonosítása ezekkel a jellemzőkkel további információkat nyújt azokról az emberekről, akikkel az érintett szervezet munkatársai kommunikálnak. Például hasznos lehet egy alkalmazott számára tudni, hogy az e-mail üzenet egyik címzettje szerződéses munkavállaló.

Az EIR ezt a státuszjelölést használja a felhasználói azonosítókhoz, hogy segítse az érintett szervezet munkatársait a kommunikációban és a napló tevékenységekben. A státuszjelölések segítségével az EIR képes nyomon követni és naplózni a felhasználói tevékenységeket, valamint biztosítani, hogy a megfelelő személyek férjenek hozzá az érintett szervezet információihoz.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a felhasználói azonosítókhoz rendelhető státuszjelöléseket.
2. Az szervezetnek a felhasználói azonosítókhoz rendelt státuszjelölések alapján további információkat kell gyűjtenie a felhasználókról.
3. A szervezetnek be kell építenie a státuszjelölések rendszerét az EIR-be. Ez magában foglalja a státuszjelölések létrehozását, módosítását és törlését, valamint a státuszjelölésekkel kapcsolatos bármilyen rendellenességet.
5. A szervezetnek rendszeresen felül kell vizsgálnia és felül kell vizsgálnia a státuszjelölések használatát az EIR-ben. Ez magában foglalja a státuszjelölésekkel kapcsolatos naplók áttekintését és az esetleges rendellenességek kivizsgálását.

6. A szervezetnek biztosítania kell, hogy a státuszjelölések használata megfelel az összes releváns jogszabálynak és szabályozásnak. Ez magában foglalja a személyes adatok védelmével és a kiberbiztonsággal kapcsolatos előírások betartását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

Nincs kapcsolódó követelménypont!

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

3.3.9.5. A hitelesítésre szolgáló eszközök kezelése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IA-4(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a felhasználói azonosítókhoz tartozó státuszjelölés meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

8.17. AZONOSÍTÓ KEZELÉS – DINAMIKUS KEZELÉS

8.17. A szervezet dinamikusan kezeli az egyéni azonosítókat a meghatározott dinamikus azonosítókezelési szabályoknak megfelelően.

MAGYARÁZAT

Az hagyományos azonosítási megközelítésekkel ellentétben, amelyek statikus fiókokat feltételeznek előre regisztrált felhasználók számára, számos elosztott rendszer üzemelés közben hoz létre azonosítókat olyan entitások (pl. felhasználók vagy kliensek) számára, amelyek korábban ismeretlenek voltak. Amennyiben az azonosítókat üzemelés közben hozzák létre korábban ismeretlen entitások számára, az érintett szervezetek előre láthatják és előkészíthetik az azonosítók dinamikus létrehozását.

Az EIR-nek képesnek kell lennie az azonosítók létrehozására, módosítására és törlésére a szükséges időben, a felhasználói igények és a biztonsági követelmények alapján. Az EIR-nek továbbá képesnek kell lennie a naplózásra, hogy nyomon követhető legyen az azonosítók használata és a változások.

Az érintett szervezetnek biztosítania kell, hogy az EIR megfelelően kezeli az azonosítókat, és hogy a dinamikus azonosítókezelési szabályokat betartják. Ez magában foglalja a megfelelő biztonsági intézkedések megtételét, mint például a hitelesítési adatok védelme, az azonosítók érvényesítése és a naplózás. Az érintett szervezetnek továbbá biztosítania kell, hogy az EIR képes legyen reagálni a változó körülményekre és igényekre, és hogy képes legyen alkalmazkodni a dinamikus azonosítókezelési szabályokhoz.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a dinamikus azonosítókezelési szabályokat, amelyek meghatározzák, hogyan kezelik az egyéni azonosítókat.
2. A szervezetnek be kell vezetnie egy rendszert, amely lehetővé teszi az azonosítók dinamikus létrehozását.
3. A szervezetnek be kell vezetnie egy rendszert, amely képes kezelni a dinamikus azonosítókat. Ez a rendszer lehetővé teszi az azonosítók dinamikus létrehozását és kezelését.

4. A szervezetnek naplóznia kell minden dinamikus azonosító létrehozást és kezelést. Ez a napló segít az érintett szervezetnek nyomon követni és ellenőrizni az azonosítók használatát, és biztosítja, hogy megfeleljenek a dinamikus azonosítókezelési szabályoknak.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a dinamikus azonosítókezelési szabályokat és az EIR-t, hogy biztosítsa a kiberbiztonsági követelményeknek való megfelelést.

KAPCSOLÓDÓ INTÉZKEDÉSEK

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

IA-4(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a dinamikus azonosító szabályzat meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.18. AZONOSÍTÓ KEZELÉS – SZERVEZETEK KÖZÖTTI KEZELÉS

8.18. A szervezet koordinálja a szervezetközi azonosítók használatát a meghatározott külső szervezetek esetében.

MAGYARÁZAT

Az érintett szervezet képes azonosítani az egyéneket, csoportokat, szerepeket vagy eszközöket, amikor szervezetközi tevékenységeket végez, amelyek az információ feldolgozását, tárolását vagy továbbítását érintik.

Az EIR itt kulcsszerepet játszik, mivel az azonosítók kezelését és koordinációját végzi. Az EIR segítségével az érintett szervezet képes nyomon követni és ellenőrizni az azonosítók használatát, biztosítva, hogy azokat megfelelően használják, és hogy az információ biztonságosan kerüljön feldolgozásra, tárolásra és továbbításra.

Az EIR továbbá lehetővé teszi az érintett szervezet számára, hogy naplózza az azonosítók használatát, ami segíthet a potenciális biztonsági problémák azonosításában és megelőzésében. A naplózás segítségével az érintett szervezet képes lehet azonosítani a szabálytalan vagy gyanús tevékenységeket, és megteheti a szükséges lépéseket a biztonsági események megelőzése érdekében.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely külső szervezetekkel fog együttműködni, és milyen azonosítókat fog használni a szervezetközi tevékenységek során.
2. A szervezetnek létre kell hoznia egy központi rendszert, amely képes kezelni az azonosítókat. Ez a rendszer tartalmazza az összes szükséges információt az azonosítókról, beleértve a hozzájuk kapcsolódó személyeket, csoportokat, szerepeket vagy eszközöket.
3. A szervezetnek biztosítania kell, hogy a rendszerben tárolt azonosítók biztonságosak legyenek. Ez magában foglalja az azonosítók védelmét a jogosulatlan hozzáféréstől, módosítástól és törléstől.
4. A szervezetnek rendszeresen naplót kell vezetnie az EIR használatáról. Ez magában foglalja az azonosítók létrehozását, módosítását, törlését és használatát.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR-t, hogy biztosítsa az azonosítók relevanciáját és pontosságát.
6. A szervezetnek biztosítania kell, hogy a külső szervezetek is megfelelően kezelik az azonosítókat. Ez magában foglalja a külső szervezetekkel való együttműködést az azonosítók használatának szabályainak kidolgozásában és betartásában.

Kapcsolódó intézkedések

4.51. Szervezeten átívelő naplózás
8.2. Azonosítás és hitelesítés
8.21. A hitelesítésre szolgáló eszközök 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

IA-4(6)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a külső szervezetek meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

8.19. AZONOSÍTÓ KEZELÉS – ÁLNEVESÍTETT AZONOSÍTÓK

8.19. A szervezet álnevesített (pszeudonim), nem újra felhasználható azonosítókat alkalmaz.

MAGYARÁZAT

Páros egyedi álneves azonosítók létrehozása, amelyek nem tartalmaznak a felhasználóra vonatkozó azonosító információkat, hátráltatja a felhasználói tevékenység nyomon követését és profilozását, túlmutatva az érintett szervezet által meghatározott működési követelményeken.

Az EIR ebben az esetben az azonosító szolgáltatót és a megbízó felet is magában foglalja. Az EIR-nek biztosítania kell, hogy az álneves azonosítók egyediek és nem újra felhasználhatók, hogy megakadályozza a felhasználói tevékenység nyomon követését és profilozását. Az EIR-nek naplózásra is szüksége van, hogy nyomon követhesse az azonosítók használatát és biztosítsa azok biztonságát. Az érintett szervezetnek pedig gondoskodnia kell arról, hogy az EIR megfelelően működjön és betartsa a kiberbiztonsági követelményeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia egy személyazonosság-szolgáltatót (Identity Provider), amely a továbbiakban generálni fogja az álnevesített, nem újrafelhasználható azonosítókat.
2. A szervezetnek biztosítania kell, hogy az álnevesített azonosítók egyediek legyenek minden egyes felhasználó számára, kivéve azokat az eseteket, amikor egy felhasználó valamely körülménye indokolja a korreláció operatív szükségességét, vagy minden fél beleegyezik a korrelációba.
3. A szervezetnek biztosítania kell, hogy az álnevesített azonosítók generálása során ne kerüljön felhasználásra semmilyen azonosító információ a felhasználóról. Ez segít megakadályozni a felhasználói tevékenységek nyomon követését és profilozását az érintett szervezet által meghatározott operatív követelményeken túl.
4. A szervezetnek dokumentálnia kell az álnevesített azonosítók generálását és használatát. Ez segít az érintett szervezetnek nyomon követni és ellenőrizni az azonosítók használatát, és biztosítja, hogy azokat megfelelően használják.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az EIR-t, hogy biztosítsa az álnevesített azonosítók biztonságát és hatékonyságát. Ez magában foglalja az azonosítók generálásának és használatának naplóinak ellenőrzését, valamint az EIR frissítését a legújabb biztonsági intézkedésekkel.

KAPCSOLÓDÓ INTÉZKEDÉSEK

8.21. A hitelesítésre szolgáló eszközök 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

IA-4(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.20. AZONOSÍTÓ KEZELÉS – ATTRIBÚTUMKARBANTARTÁS ÉS -VÉDELEM

8.20. A szervezet megőrzi az egyedileg azonosított személyek, eszközök vagy szolgáltatások attribútumait egy meghatározott, védett központi tárhelyen.

MAGYARÁZAT

Fontos, hogy az érintett szervezet folyamatosan megőrizze az hitelesített entitások attribútumait egy központi tárhelyen. Az attribútumok olyan adatok, amelyek egyedileg azonosítják a személyeket, eszközöket vagy szolgáltatásokat. Ezek az adatok lehetnek például felhasználói nevek, jelszavak, eszközazonosítók vagy szolgáltatás-specifikus információk.
Az EIR-ben tárolt attribútumok naplózása kiemelten fontos. A naplózás segít az érintett szervezetnek nyomon követni az attribútumok változásait, és lehetővé teszi a szervezet számára, hogy gyorsan reagáljon a potenciális biztonsági problémákra. A naplózás segíthet azonosítani a rendellenes viselkedést, és segíthet a szervezetnek megelőzni a biztonsági eseményeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat az egyedileg azonosított személyeket, eszközöket és szolgáltatásokat, amelyek attribútumait meg kell őriznie. Ez magában foglalhatja a felhasználói fiókokat, hálózati eszközöket, szoftvereket, szervereket és egyéb EIR-elemeket.
2. A szervezetnek létre kell hoznia egy központi tárhelyet, ahol ezeket az attribútumokat tárolja. Ennek a tárhelynek védettnek kell lennie, hogy megakadályozza a jogosulatlan hozzáférést és módosítást.
3. A szervezetnek úgy kell konfigurálnia az EIR-t, hogy az automatikusan gyűjtse és tárolja az attribútumokat a központi tárhelyen. Ez magában foglalhatja a felhasználói műveleteket, a hálózati forgalmat, a rendszereseményeket és más releváns adatokat.
4. A szervezetnek rendszeresen ellenőriznie kell a központi tárhelyet, hogy biztosítsa az adatok sértetlenségét és pontosságát. Ez magában foglalhatja a napló elemzését és az adatok összehasonlítását a meglévő attribútumokkal.

5. A szervezetnek biztosítania kell, hogy a központi tárhely megfelelően védett legyen a kiberfenyegetésektől. Ez magában foglalhatja a tűzfalakat, az adatok titkosítását, a hozzáférési jogosultságok kezelését és más biztonsági intézkedések alkalmazását.
6. A szervezetnek dokumentálnia kell a folyamatot, beleértve az attribútumok gyűjtését, tárolását és védelmét, hogy bizonyítani tudja a kiberbiztonsági követelményeknek 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

IA-4(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a védett központi tárhely meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.21. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE

8.21. A szervezet a hitelesítő eszközöket az alábbiak szerint kezeli:

8.21.1. A kezdeti hitelesítő eszköz kiosztásának részeként ellenőrzi a hitelesítő eszközt megkapó egyén, csoport, szerepkör, szolgáltatás vagy eszköz identitását.

8.21.2. Meghatározza a szervezet által kiadott hitelesítő eszköz kezdeti tartalmát.

8.21.3. Biztosítja, hogy a hitelesítő eszközök a tervezett felhasználáshoz megfelelő erősségű mechanizmussal rendelkezzenek.

8.21.4. Adminisztratív eljárásokat alakít ki és hajt végre a kezdeti hitelesítő eszközök kiosztásához, az elveszett, kompromittált vagy sérült hitelesítő eszközökhöz, valamint a hitelesítő eszközök visszavonásához.

8.21.5. Gondoskodik a hitelesítő eszközök kezdeti tartalmának megváltoztatásáról az első használat előtt.

8.21.6. Gondoskodik a hitelesítő eszközök tartalmának megváltoztatásáról vagy frissítéséről meghatározott gyakorisággal, vagy amikor meghatározott események bekövetkeznek.

8.21.7. Megvédi a hitelesítő eszközök tartalmát az illetéktelen nyilvánosságra hozatal és módosítás ellen.

8.21.8. Megköveteli, hogy az egyének és eszközök konkrét védelmi intézkedéseket alkalmazzanak, illetve hajtsanak végre a hitelesítő eszközök védelme érdekében.

8.21.9. Megváltoztatja a csoporthoz vagy szerepkörhöz rendelt fiókok hitelesítő eszközeinek tartalmát, amikor a fiókokhoz tartozó tagok közül valaki eltávolításra kerül.

MAGYARÁZAT

A hitelesítésre alkalmas mechanizmusok közé tartoznak a jelszavak, a kriptográfiai eszközök, a biometrikus adatok, a tanúsítványok, az egyszer használatos jelszó eszközök és az azonosító kártyák. Hitelesítő eszközök fejlesztői gyári alapértelmezett hitelesítési adatokkal szállíthatják az eszközeiket, hogy lehetővé tegyék a kezdeti telepítést és konfigurációt. Alapértelmezett adatnak hívjuk a hitelesítő eszköz tartalmát az inicializációs lépés után (pl. egy kezdeti jelszó "password" alapbeállítással). Az alapértelmezett hitelesítési adatok gyakran jól ismertek, könnyen felfedezhetők és jelentős kockázatot jelentenek. Ezzel szemben a hitelesítő eszköz tartalmának követelményei specifikus kritériumokat vagy jellemzőknek kell megfeleljenek (pl.

a jelszó minimális hossza). Az érintett szervezetnek támogatnia kell a hitelesítő eszközök kezelését meghatározott beállításokkal és korlátozásokkal a különböző hitelesítő eszközök sajátos jellemzői alapján (pl. a jelszó minimális hossza, az időszinkron egy alkalommal használatos tokenek érvényesítési időablaka, és a biometrikus hitelesítés ellenőrzési szakaszában megengedett elutasítások száma). Lépéseket lehet tenni továbbá az egyéni hitelesítő eszközök védelme érdekében, beleértve a hitelesítő eszközök birtoklásának fenntartását, a hitelesítő eszközök másokkal való megosztásának elkerülését, és az elveszett, ellopott vagy kompromittált hitelesítő eszközök azonnali bejelentését. A hitelesítő eszközök kezelése magában foglalja a hitelesítő eszközök kiadását és visszavonását az ideiglenes hozzáféréshez, amikor már nincs rájuk szükség.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet számba veszi és dokumentálja azon rendszereket, melyek elérése hitelesítő eszközhöz kötött.
2. A szervezet számba veszi és dokumentálja azon egyének, csoportok, szerepkörök, szolgáltatások vagy eszközök identitását, akik hitelesítő eszközöket kaphatnak. Ez magában foglalhatja a személyazonosság igazolását, a szerepkörök ellenőrzését és a csoporttagság megerősítését.
3. A szervezet meghatározza a hitelesítő eszközök tartalma és konfigurációja felé támasztott követelményeket, ezeket szabályzatba foglalja. Ebbe beleértendő a kezdeti tartalom definiálása és beállítása.
4. A szervezet létrehozza a hitelesítő eszközök kezelésének szabályzatát. Ez magába foglalja a kiosztásra, használatra, a tartalom rendszeres, meghatározott gyakorisággal való frissítésére, elveszett, vagy kompromittált eszközök visszavonására, a tartalom védelmére és a követelmények betartásának nem teljesítése esetére vonatkozó intézkedések leírását.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése
2.60. Legkisebb jogosultság elve
6.23. Konfigurációs beállítások
8.2. Azonosítás és hitelesítés

8.14. Azonosító kezelés

8.37. Hitelesítés kriptográfiai modul esetén

8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

8.41. Szolgáltatás azonosítása és hitelesítése

10.11. Távoli karbantartás

12.2. A fizikai belépési engedélyek

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

3.3.9.5. A hitelesítésre szolgáló eszközök kezelése

ISO/IEC 27001:2023 REFERENCIA

A.5.16; A.5.17

NIST SP 800-53 REV.5 REFERENCIA

IA-5

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

8.22. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – JELSZÓ ALAPÚ HITELESÍTÉS

8.22. A szervezet:

8.22.1. Fenntartja a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáját, és ezt a listát a szervezet által meghatározott gyakorisággal frissíti, továbbá minden olyan esetben, amikor a szervezeti jelszavakat közvetlenül vagy közvetett módon veszélyeztetik.

8.22.2. Ellenőrzi, hogy a felhasználók által létrehozott vagy módosított jelszavak szerepelnek-e a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáján.

8.22.3. A jelszavakat csak kriptográfiailag védett csatornákon keresztül továbbítja.

8.22.4. A jelszavakat egy jóváhagyott, sózott kulcsszármaztatási funkcióval, lehetőleg egykulcsos hash-t használva tárolja.

8.22.5. Megköveteli a jelszó azonnali megváltoztatását fiókvisszaállítás esetén.

8.22.6. Engedélyezi a felhasználóknak hosszú jelszavak és jelmondatok kiválasztását, beleértve a szóközöket és a nyomtatható karaktereket.

8.22.7. Automatizált eszközökkel támogatja a felhasználókat az erős jelszavak kiválasztásában.

8.22.8. A jelszavakra a szervezet által meghatározott összetételi és komplexitási szabályokat érvényesíti.

MAGYARÁZAT

Az érintett szervezet jelszóalapú hitelesítést alkalmaz a jelszavakra, függetlenül attól, hogy azokat egyszintű vagy többszintű hitelesítésben használja-e. A hosszú jelszavak vagy jelmondatok előnyösebbek a rövidebb jelszavaknál. A szervezet által meghatározott és betartatott jelszóösszetételi szabályok (bonyolultság - pl. kötelező speciális karakterek, számok stb.) nem jelentenek jelentős biztonsági előnyt, miközben csökkentik a használhatóságot. Az érintett szervezet bizonyos körülmények között dönthet úgy, hogy szabályokat állapít meg a jelszógeneráláshoz (pl. fiókvisszaállítás). A kriptográfiailag védett jelszavak magukban foglalják a jelszavak sózott egyirányú kriptográfiai hash-eit. A gyakran használt, kompromittált vagy várható jelszavak listája tartalmazza a korábbi adatszivárgásokból származó jelszavakat,

szótári szavakat és ismétlődő vagy sorozatos karaktereket, valamint a kontextusspecifikus szavakat is, mint például az EIR neve, a felhasználónév és annak derivatívái.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezet fenntartja a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáját, és ezt a listát a szervezet által meghatározott gyakorisággal frissíti.
2. Ellenőrzi, hogy a felhasználók által létrehozott vagy módosított jelszavak szerepelnek-e a gyakran használt, könnyen kitalálható vagy kompromittált jelszavak listáján.
3. A jelszavakat csak kriptográfiailag védett csatornákon keresztül továbbítja.
4. A jelszavakat egy jóváhagyott, sózott kulcsszármaztatási funkcióval, lehetőleg egykulcsos hash-t használva tárolja.
5. Megköveteli a jelszó azonnali megváltoztatását fiókvisszaállítás esetén.
6. Engedélyezi a felhasználóknak hosszú jelszavak és jelmondatok kiválasztását, beleértve a szóközöket és a digitálisan megjeleníthető karaktereket.
7. Automatizált eszközökkel támogatja a felhasználókat az erős jelszavak kiválasztásában.
8. A jelszavakra az érintett szervezet által meghatározott összetételi és komplexitási szabályokat érvényesíti. Ez magában foglalhatja például a hosszú jelszavak minimális karakterhosszát.
9. Dokumentálja és rendszeres időközönként felülvizsgálja a jelszókezelési folyamatokat, hogy biztosítsa a szabályok betartását és az esetleges szabálytalanságok azonnali észlelését.

KAPCSOLÓDÓ INTÉZKEDÉSEK

8.36. Hitelesítési információk visszajelzésének elrejtése

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

3.3.9.5. A hitelesítésre szolgáló eszközök kezelése

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IA-5(1)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

8.23. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – NYILVÁNOS KULCS ALAPÚ HITELESÍTÉS

8.23.1. A nyilvános kulcs alapú hitelesítés esetén:

8.23.1.1. A szervezet biztosítja a megfelelő privát kulcshoz való jogosult hozzáférést.

8.23.1.2. A szervezet összekapcsolja a hitelesített azonosítót az egyén vagy csoport fiókjával.

8.23.1.2.1. Amikor a nyilvános kulcsú infrastruktúra (PKI) kerül felhasználásra:

8.23.1.3. Ellenőrzi a tanúsítványokat egy elfogadott megbízható pontig tartó tanúsítványlánc felépítésével és ellenőrzésével, beleértve a tanúsítvány állapot információ ellenőrzését is.

8.23.1.4. Megvalósítja a visszavonási adatok helyi tárolását a tanúsítványlánc felépítésének és ellenőrzésének támogatására arra az esetre, amikor a visszavonási információk a hálózaton keresztül nem elérhetők.

MAGYARÁZAT

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

KAPCSOLÓDÓ INTÉZKEDÉSEK

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

ISO/IEC 27001:2023 REFERENCIA

NIST SP 800-53 REV.5 REFERENCIA

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

8.24. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – HITELESÍTŐK MÓDOSÍTÁSA AZ ÁTADÁS ELŐTT

8.24. A szervezet a rendszerelemek fejlesztőit és telepítőit arra kötelezi, hogy egyedi hitelesítő adatokat biztosítsanak, vagy változtassák az alapértelmezett hitelesítő adatokat az átadás és telepítés előtt.

MAGYARÁZAT

Az alapértelmezett hitelesítő adatok átadás és telepítés előtti megváltoztatása kiterjeszti az érintett szervezet követelményét, hogy az EIR telepítésekor változtassák meg az alapértelmezett hitelesítő adatokat, úgy, hogy a fejlesztőket illetve telepítőket kötelezi arra, hogy egyedi hitelesítő adatokat biztosítsanak, vagy változtassák meg az alapértelmezett hitelesítő adatokat a rendszerelemek átadása illetve telepítése előtt. Azonban ez általában nem vonatkozik a kereskedelmi forgalomban kapható információs technológiai termékek fejlesztőire. Az egyedi hitelesítő adatokra vonatkozó követelményeket az érintett szervezetek belefoglalhatják a beszerzési dokumentumokba, amikor EIR-t vagy rendszerelemeket szereznek be. A naplóban rögzíteni kell az ilyen változtatásokat, hogy nyomon követhető legyen a hitelesítő adatok kezelése.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek olyan követelményeket kell kialakítania, amelyek kötelezik az EIR fejlesztőit és telepítőit, hogy biztosítsanak egyedi hitelesítő adatokat, vagy változtassák meg az alapértelmezett hitelesítő adatokat az átadás és telepítés előtt.
2. A szervezetnek be kell építenie ezt a követelményt a beszerzési dokumentumokba, amikor EIR-t vagy rendszerelemeket szerez be.
3. A szervezetnek ellenőriznie kell, hogy a fejlesztők és telepítők betartják-e ezt a követelményt. Ez magában foglalhatja a fejlesztési és telepítési folyamatok naplózását, valamint a hitelesítő adatok ellenőrzését.
4. A szervezetnek biztosítania kell, hogy a követelményeket betartják, és hogy a hitelesítő adatokat megfelelően kezelik és tárolják.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a követelményeket, hogy biztosítsa azok relevanciáját és hatékonyságát a változó kiberbiztonsági környezetben.
Fontos megjegyezni, hogy ez a követelmény általában nem vonatkozik a kereskedelmi forgalomban kapható információs technológiai termékek fejlesztőire.

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

IA-5(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.25. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – A HITELESÍTŐ ESZKÖZÖK VÉDELME

8.25. A szervezet a hitelesítő eszközöket az információk biztonsági besorolásának megfelelő védelemmel látja el, amelyekhez a hitelesítő eszköz a hozzáférést biztosítja.

MAGYARÁZAT

Az érintett szervezetnek gondoskodnia kell arról, hogy a hitelesítő eszközök megfelelő védelmet kapjanak. Ez azt jelenti, hogy a hitelesítő eszközök védelmi szintjének arányban kell állnia az EIR-ben tárolt információk biztonsági besorolásával. Például, ha az EIR magas biztonsági besorolású információkat tartalmaz, akkor a hitelesítő eszközöket is magas szintű védelemmel kell ellátni.

A biztonsági besorolás folyamata során az érintett szervezet meghatározza az információk biztonsági kategóriáit. Ez a folyamat magában foglalja az információk értékelését, a potenciális kockázatok felmérését és a szükséges védelmi intézkedések meghatározását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia az EIR-en tárolt információk biztonsági besorolását. Ez a folyamat magában foglalja az információk értékelését, és a hozzájuk tartozó biztonsági kategóriák meghatározását.
2. A szervezetnek biztosítania kell, hogy az EIR-en belül megbízható fizikai vagy logikai szeparáció legyen az egyes biztonsági kategóriák között. Ha ez nem lehetséges, akkor a hitelesítő eszközöket a legmagasabb biztonsági kategóriával kell védeni.
3. A szervezetnek meg kell terveznie és implementálnia kell a hitelesítő eszközök védelmét. Ez magában foglalhatja a hitelesítő eszközök titkosítását, a hozzáférési jogosultságok szigorú kezelését és a hitelesítő eszközök rendszeres frissítését.
4. A szervezetnek naplóznia kell a hitelesítő eszközök használatát, hogy nyomon követhető legyen, ki, mikor és milyen információhoz fér hozzá. A naplózás segít az esetleges biztonsági események gyors felismerésében és kezelésében.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hitelesítő eszközök védelmét, hogy megfeleljen a legújabb biztonsági követelményeknek és fenyegetéseknek.

Kapcsolódó intézkedések

15.2. Biztonsági osztályba sorolás

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

IA-5(6)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

8.26. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – NINCSENEK BEÁGYAZOTT TITKOSÍTATLAN STATIKUS HITELESÍTŐK

8.26. Az EIR biztosítja, hogy ne legyenek titkosítatlan, statikus hitelesítők beépítve az alkalmazásokba vagy más statikus tárolási formákba.

MAGYARÁZAT

Az EIR biztosítja azt, hogy ne legyenek titkosítatlan, statikus hitelesítők az alkalmazásokban vagy más statikus tárolási formákban. Ez azt jelenti, hogy az EIR megakadályozza a titkosítatlan hitelesítők használatát, mivel ezek könnyen hozzáférhetővé válhatnak a rosszindulatú személyek számára, ami súlyos biztonsági kockázatot jelenthet.
Az EIR ezenkívül naplózza a hitelesítők használatát is, hogy az nyomon követhető legyen, azaz, ki, mikor és milyen hitelesítőt használt. Ez lehetővé teszi az érintett szervezet számára azt, hogy gyorsan reagáljon a potenciális biztonsági eseményekre, és megakadályozza a további adatszivárgást vagy a hozzáférést.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy vannak-e beépített vagy tárolt hitelesítők az EIR-ben, és ha igen, ezek titkosítottak vagy titkosítatlanok. Ez magában foglalja az alkalmazásokat, hozzáférési scripteket stb.
2. Amennyiben a szervezet beépített vagy tárolt hitelesítőket használ, akkor meg kell győződnie arról, hogy ezek titkosított formában vannak-e tárolva. Ha a hitelesítők tárolt formában vannak használva, akkor ezeket titkosítatlan hitelesítőknek tekintjük.
3. A szervezetnek meg kell változtatnia a hitelesítők tárolásának módját, ha azok jelenleg titkosítatlan formában vannak tárolva. Ez magában foglalhatja a hitelesítők titkosítását, vagy a hitelesítők tárolásának módjának megváltoztatását, hogy ne legyenek statikusak.
4. A szervezetnek dokumentálnia kell a hitelesítők használatát és tárolását, hogy biztosítsa a kiberbiztonsági követelményeknek való megfelelést. Ez magában foglalhatja a hitelesítők használatának, tárolásának és titkosításának nyomon követését.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hitelesítők használatát és tárolását, hogy biztosítsa a kiberbiztonsági követelményeknek való folyamatos megfelelést. Ez magában foglalhatja a hitelesítők használatának, tárolásának és titkosításának rendszeres felülvizsgálatát és frissítését.

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

IA-5(7)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.27. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – TÖBB RENDSZERBELI FELHASZNÁLÓ FIÓKOK

8.27. A szervezet biztonsági követelményeket határoz meg, hogy kezelje a több rendszerben is fiókkal rendelkező egyének általi kompromittálási kockázatot.

MAGYARÁZAT

Amikor ugyanazoknak a személyeknek több EIR-ben is fiókjuk van és ugyanazokat az hitelesítőket, például jelszavakat használják, fennáll a veszélye annak, hogy egy fiók kompromittálódása esetén más fiókok is veszélybe kerülhetnek.
Az érintett szervezet biztonsági követelményeket határoz meg, hogy kezelje a több EIR-ben is fiókkal rendelkező egyének általi kompromittálási kockázatot. Ezek a követelmények magukban foglalhatják a jelszavak erősségének, a hitelesítési eljárásoknak és a naplózási gyakorlatoknak a szabályozását. A naplózás segíthet azonosítani a rendellenes hozzáférési kísérleteket és a rendszerrel kapcsolatos egyéb biztonsági eseményeket. A hitelesítési eljárások, mint például a többtényezős hitelesítés, tovább csökkenthetik a kompromittálódás kockázatát.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek fel kell mérnie a kockázatot, amelyet az egyének több EIR-ben való fiókkal rendelkezése jelent. Ez magában foglalja a kompromittálás kockázatának értékelését, ha az egyén ugyanazt az hitelesítőt, például jelszót használja több EIR-ben.
2. A szervezetnek meg kell határoznia a biztonsági követelményeket, amelyek segítenek kezelni ezt a kockázatot. Ez magában foglalhatja a különböző hitelesítők használatát minden EIR-ben, egyetlen bejelentkezési vagy szövetségi mechanizmus alkalmazását, vagy valamilyen egyszeri jelszavak használatát minden EIR-ben.
3. A szervezetnek szabályokat és eljárásokat kell kidolgoznia a viselkedésre és hozzáférési megállapodásokat, hogy csökkentse a több EIR fiók kockázatát.
4. A szervezetnek naplóznia és monitoroznia kell, hogy nyomon követhesse a felhasználói tevékenységeket és azonosíthassa a szabálytalanságokat. Ez magában foglalja a hitelesítési kísérletek, a hozzáférési kísérletek és a rendszeres felhasználói tevékenységek naplózását.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a biztonsági követelményeket és a viselkedési szabályokat, hogy biztosítsa azok relevanciáját és hatékonyságát a változó kiberbiztonsági környezetben.

KAPCSOLÓDÓ INTÉZKEDÉSEK

14.9. Hozzáférési megállapodások

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

IA-5(8)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biztonsági követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.28. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – EGYESÍTETT HITELESÍTŐ ADATOK KEZELÉSE

8.28. A szervezet meghatározza, hogy mely külső szervezetekkel kapcsolatban használható vagy engedélyezhető a hitelesítő adatok egyesítése.

MAGYARÁZAT

Az érintett szervezetnek meg kell határoznia, hogy mely külső szervezetekkel kapcsolatban használható vagy engedélyezhető a hitelesítő adatok egyesítése. Ez azt jelenti, hogy az érintett szervezetnek előre meg kell határoznia és jóvá kell hagynia azokat a külső szervezeteket, amelyekkel az EIR hitelesítő adatait megoszthatja vagy egyesítheti.
Ez a követelmény fontos a kiberbiztonság szempontjából, mivel megakadályozza, hogy illetéktelen szervezetek hozzáférjenek az EIR hitelesítő adataihoz. A jóváhagyott szervezetek listájának használata biztosítja azt, hogy csak a megbízható és átvizsgált szervezetek férhetnek hozzá ezekhez az adatokhoz.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, mely külső szervezetekkel kíván egyesített hitelesítő adatokat használni vagy engedélyezni.
2. A szervezetnek létre kell hoznia egy specifikus listát azokról a külső szervezetekről, amelyekkel a hitelesítő adatok egyesítése engedélyezett.
3. Az érintett szervezetnek biztosítania kell, hogy a listán szereplő külső szervezetek megfelelően ellenőrizve és megbízhatónak találtattak.
4. A szervezetnek implementálnia kell a hitelesítő adatok egyesítését az EIR-ben a listán szereplő külső szervezetekkel.
5. A szervezetnek naplózni kell az összes hitelesítési eseményt, beleértve az egyesített hitelesítő adatok használatát is.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a külső szervezetek listáját, hogy biztosítsa a kiberbiztonsági követelményeknek való megfelelést.
7. A szervezetnek biztosítania kell, hogy a hitelesítő adatok egyesítésének használata megfelel az összes releváns jogi és szabályozási követelménynek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

4.22. Naplóbejegyzések csökkentése és jelentéskészítés

4.51. Szervezeten átívelő naplózás

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

IA-5(9)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a külső szervezetek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.29. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – DINAMIKUS HITELESÍTÉSI ADATKAPCSOLAT

8.29. A szervezet képes a felhasználói személyazonosságokat és a hitelesítő adatokat dinamikusan összekapcsolni a szervezeti szabályok alapján.

MAGYARÁZAT

A hitelesítéshez valamilyen formában össze kell kapcsolni a személyazonosságot és a hitelesítés megerősítésére használt hitelesítő eszközt. A hagyományos megközelítésekben a kapcsolat úgy jön létre, hogy az EIR előzetesen biztosítja mind a személyazonosságot, mind a hitelesítőt. Például a felhasználónév és a jelszó (azaz a hitelesítő) közötti kapcsolat úgy valósul meg, hogy az azonosító és a hitelesítő egy párként van megadva a rendszerben. Az új hitelesítési technikák lehetővé teszik azt, hogy a személyazonosság és a hitelesítő közötti kapcsolat az EIR-en kívül valósuljon meg. Például az intelligens kártyás hitelesítő adatok esetében a személyazonosság és a hitelesítő az intelligens kártyán kerül összekapcsolásra. E hitelesítő adatok használatával az EIR-ek hitelesíthetik az előre nem megadott személyazonosságokat, és a hitelesítést követően dinamikusan biztosíthatják a személyazonosságot. Ezekben a helyzetekben a szervezetek előreláthatják a dinamikus identitások alakulását. A személyazonosságok és az ezekhez kapcsolódó hitelesítő adatok hitelesítéséhez elengedhetetlenek az előre kialakított bizalmi kapcsolatok és a megfelelő hatóságokkal kialakított mechanizmusok.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a felhasználói személyazonosságok és a hitelesítő adatok közötti kapcsolatot. Ez a hitelesítési folyamat része, amelyben az EIR-nek bizonyítania kell a felhasználó személyazonosságát.
2. A szervezetnek előre be kell állítania a személyazonosságokat és a hitelesítő adatokat az EIR-ben. Például a felhasználónév és a jelszó (azaz hitelesítő adat) összekapcsolása az EIR-ben történik, ahol a személyazonosság és a hitelesítő adat párosítva van.
3. A szervezetnek lehetőséget kell biztosítania a személyazonosságok és a hitelesítő adatok dinamikus összekapcsolására.

4. A szervezetnek előre meg kell határoznia a személyazonosságok dinamikus beállítását. Ehhez szükségesek a megbízható kapcsolatok és mechanizmusok az illetékes hatóságokkal, hogy érvényesítsék a személyazonosságokat és a kapcsolódó hitelesítő adatokat.
5. A szervezetnek dokumentálnia kell a személyazonosságokat és hozzájuk kapcsolt a hitelesítő adatokat, valamint ezek összekapcsolásának formáját és helyét. Ez segít nyomon követni és ellenőrizni a hitelesítési folyamatot, és biztosítja, hogy az összes személyazonosság megfelel a szervezeti szabályoknak.

Kapcsolódó intézkedések

4.51. Szervezeten átívelő naplózás
8.21. A hitelesítésre szolgáló eszközök 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

IA-5(10)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat a kötelező érvényű szabályok meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

8.30. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – BIOMETRIKUS HITELESÍTÉS HATÉKONYSÁGA

8.30. A szervezet olyan biometrikus hitelesítési mechanizmusokat alkalmaz, amelyek megfelelnek a biometrikus eszközökkel szemben meghatározott minőségi követelményeknek.

MAGYARÁZAT

A jelszóalapú hitelesítéssel ellentétben, amely a felhasználó által megadott jelszavak és a tárolt jelszavak pontos egyezését biztosítja, a biometrikus hitelesítés nem biztosít pontos egyezést. A biometrikus adat típusától és a gyűjtési mechanizmustól függően a bemutatott biometrikus adat és az összehasonlítás alapjául szolgáló tárolt biometrikus adat között valószínűleg van némi eltérés. Az egyezési teljesítmény az az arány, amellyel a biometrikus algoritmus helyesen talál egyezést egy valódi felhasználóval, és elutasítja a többi felhasználót. A biometrikus teljesítményre vonatkozó követelmények közé tartozik az egyezési arány, amely a rendszer által használt biometrikus egyezési algoritmus pontosságát tükrözi.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a biometrikus hitelesítési mechanizmusokat, amelyeket az EIR-ben alkalmazni kíván. Ez magában foglalhatja az ujjlenyomat-, arcfelismerés-, íriszfelismerés- és hangfelismerés-alapú hitelesítést.
2. A szervezetnek ki kell választania a megfelelő biometrikus eszközöket, amelyek megfelelnek a minőségi követelményeknek. Ez magában foglalhatja a biometrikus adatok gyűjtésére, tárolására és feldolgozására képes eszközöket.
3. A szervezetnek implementálnia kell a kiválasztott biometrikus hitelesítési mechanizmusokat az EIR-ben. Ez magában foglalhatja a biometrikus adatok gyűjtésének, tárolásának és feldolgozásának folyamatát.
4. A szervezetnek ellenőriznie kell a biometrikus hitelesítési mechanizmusok működését, hogy biztosítsa a megfelelő működést és a minőségi követelményeknek való megfelelést. Ez magában foglalhatja a biometrikus adatok gyűjtésének, tárolásának és feldolgozásának ellenőrzését, valamint a biometrikus hitelesítési algoritmusok pontosságának ellenőrzését.

5. A szervezetnek naplóznia kell a biometrikus hitelesítési mechanizmusok használatát, hogy nyomon követhesse a rendszer működését és az esetleges problémákat. Ez magában foglalhatja a biometrikus adatok gyűjtésének, tárolásának és feldolgozásának naplózását, valamint a biometrikus hitelesítési algoritmusok használatának naplózását.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a biometrikus hitelesítési mechanizmusokat, hogy biztosítsa a minőségi követelményeknek való folyamatos megfelelést. Ez magában foglalhatja a biometrikus adatok gyűjtésének, tárolásának és feldolgozásának folyamatainak felülvizsgálatát, valamint a biometrikus hitelesítési algoritmusok pontosságának felülvizsgálatát.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.71. Sikertelen bejelentkezési kísérletek

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

IA-5(12)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a biometrikus minőségi követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.31. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – A GYORSÍTÓTÁRBAN TÁROLT HITELESÍTŐK LEJÁRATA

8.31. A szervezet tiltja a gyorsítótárazott hitelesítési adatok meghatározottnál hosszabb idejű használatát.

MAGYARÁZAT

Az érintett szervezetben a gyorsítótárazott (cache) hitelesítők olyan eszközök, amelyeket a helyi EIR-hez történő hitelesítéshez használnak, amikor a hálózat nem érhető el. Ha a gyorsítótárazott hitelesítési információk elavultak, a hitelesítési információk érvényessége megkérdőjelezhető.

Ezért az érintett szervezet tiltja a gyorsítótárazott hitelesítési adatok meghatározottnál hosszabb idejű használatát. Ez azt jelenti, hogy a gyorsítótárazott hitelesítési adatokat csak egy meghatározott időtartamig használhatják, mielőtt frissíteni kell őket. Ez a követelmény segít megelőzni a hitelesítési adatokkal kapcsolatos biztonsági problémákat, például az elavult vagy kompromittált adatok használatát. A gyorsítótárazott hitelesítési adatok korlátozott idejű használata biztosítja, hogy az EIR-ben tárolt hitelesítési információk mindig naprakészek és érvényesek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a gyorsítótárazott hitelesítési adatok maximális élettartamát. Ez az időtartam nem lehet hosszabb, mint amit a szervezet által meghatározott szabályozó megenged.
2. A szervezetnek be kell állítania az EIR-t úgy, hogy az ne engedélyezze a gyorsítótárazott hitelesítési adatok túl hosszú ideig történő használatát. Ez magában foglalhatja a hitelesítési adatok automatikus törlését a gyorsítótárazásból a megadott időtartam után.
3. A szervezetnek be kell állítania az EIR naplózását úgy, hogy az rögzítse a gyorsítótárazott hitelesítési adatok használatát. Ez lehetővé teszi a szervezet számára, hogy nyomon követhesse, mely felhasználók használták a gyorsítótárazott hitelesítési adatokat, és mennyi ideig.

4. A szervezetnek rendszeresen ellenőriznie kell az EIR naplóit, hogy biztosítsa a gyorsítótárazott hitelesítési adatok megfelelő használatát. Ha a naplókban bármilyen szabálytalanságot észlelnek, az érintett szervezetnek azonnal cselekednie kell.
5. A szervezetnek továbbá biztosítania kell, hogy a gyorsítótárazott hitelesítési adatokat csak akkor használják, ha a hálózat nem érhető el. Ha a hálózat elérhető, a felhasználóknak friss hitelesítési adatokat kell használniuk.
6. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a gyorsítótárazott hitelesítési adatok használatára vonatkozó szabályzatait és eljárásait, hogy biztosítsa azok relevanciáját és hatékonyságát.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 referencia

Nincs vonatkozó referencia.

NIST SP 800-53 rev.5 referencia

IA-5(13)

A követelményhez meghatározandó paraméterek

A követelményponthoz kapcsolódó szervezeti feladat az idő intervallum meghatározása.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

8.32. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – A MEGBÍZHATÓ PKI TANÚSÍTVÁNYTÁRAK KEZELÉSE

8.32. A szervezet a PKI-alapú hitelesítéshez egy szervezeti szintű módszertant alkalmaz, ami meghatározza a megbízható PKI tanúsítványtárak tartalmának kezelését minden platformon, beleértve a hálózatokat, operációs rendszereket, böngészőket és alkalmazásokat.

MAGYARÁZAT

Az érintett szervezet a PKI-alapú hitelesítők pontosságának és naprakészségének javítása érdekében egy szervezeti szintű módszertant alkalmaz a megbízható PKI tanúsítványtárak tartalmának kezelésére. Ez a módszertan magában foglalja a tanúsítványtárak tartalmának rendszeres felülvizsgálatát és frissítését, valamint a tanúsítványok érvényességének ellenőrzését.

Az érintett szervezet minden platformon alkalmazza ezt a módszertant, beleértve az EIR-eket, és EIR-ek rendszerelemeit, például hálózatokat, operációs rendszereket és alkalmazásokat. Ez azt jelenti, hogy a módszertan a tanúsítványtárak kezelését szabályozza az összes EIR-en, és biztosítja, hogy a tanúsítványok naprakészek és megbízhatóak legyenek.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell dolgoznia egy szervezeti szintű módszertant a PKI-alapú hitelesítéshez. Ez a módszertan meghatározza, hogyan kezelik a megbízható PKI tanúsítványtárak tartalmát minden EIR-en, beleértve a hálózatokat, operációs rendszereket, böngészőket és alkalmazásokat.
2. A szervezetnek be kell állítania és fenn kell tartania a PKI tanúsítványtárakat, amelyek tartalmazzák a hitelesítési adatokat. Ezeknek a táraknak naprakészeknek és pontosnak kell lenniük.
3. A szervezetnek biztosítania kell, hogy minden EIR, beleértve a hálózatokat, operációs rendszereket, böngészőket és alkalmazásokat, megfelelően kezeli a PKI tanúsítványtárakat. Ez magában foglalja a tanúsítványtárak frissítését, a hitelesítési adatok ellenőrzését és a tanúsítványok érvényességének ellenőrzését.

4. A szervezetnek naplót kell vezetnie a PKI tanúsítványtárak kezeléséről. Ez magában foglalja a tanúsítványtárak frissítéseit, a hitelesítési adatok ellenőrzését és a tanúsítványok érvényességének ellenőrzését. A napló segít az érintett szervezetnek nyomon követni a PKI tanúsítványtárak kezelését és biztosítani a hitelesítési adatok pontosságát és naprakészségét.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a PKI-alapú hitelesítési megoldásait, hogy biztosítsa annak hatékonyságát és relevanciáját a változó kiberbiztonsági környezetben.

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

IA-5(14)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

8.33. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – SZEMÉLYES JELENLÉT MELLETTI VAGY MEGBÍZHATÓ KÜLSŐ FÉL ÁLTALI HITELESÍTŐESZKÖZ KIBOCSÁTÁS

8.33. A szervezet előírja, hogy a meghatározott típusú vagy különleges hitelesítőeszközök kiadása személyes jelenlét mellett vagy egy megbízható külső fél által történjen, a szervezet által meghatározott hitelesítés szolgáltató előtt, a szervezet által meghatározott személyek vagy szerepkörök jóváhagyása után.

MAGYARÁZAT

A követelmény előírja, hogy az érintett szervezet bizonyos típusú vagy különleges hitelesítőeszközök kiadását személyes jelenlét mellett vagy egy megbízható külső fél által végezze. Ez azt jelenti, hogy a hitelesítőeszközök kiadása nem történhet meg anélkül, hogy a felhasználó személyesen jelen lenne, vagy egy megbízható harmadik fél ellenőrizné a folyamatot.

Az érintett szervezet továbbá előírja, hogy a hitelesítőeszközök kiadása csak a szervezet által meghatározott hitelesítési szolgáltató előtt történjen. Ez azt jelenti, hogy a hitelesítőeszközök kiadásának folyamatát egy olyan szolgáltató végzi, aki megfelel az érintett szervezet által meghatározott követelményeknek.

Végül, a hitelesítőeszközök kiadása csak az érintett szervezet által meghatározott személyek vagy szerepkörök jóváhagyása után történhet. Ez azt jelenti, hogy a hitelesítőeszközök kiadása nem történhet meg anélkül, hogy a folyamatot jóváhagynák azok a személyek vagy szerepkörök, akiket az érintett szervezet erre felhatalmazott.

Ez a követelmény biztosítja, hogy az EIR-ben tárolt információk védelme megfelelő szintű legyen, és hogy a hitelesítőeszközök kiadása során betartják a szükséges biztonsági előírásokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, milyen típusú vagy különleges hitelesítőeszközöket szeretne kiadni.
2. A szervezetnek döntenie kell arról, hogy a hitelesítőeszközök kiadása személyes jelenlét mellett történjen-e, vagy egy megbízható külső fél által.
3. Ha a személyes jelenlét mellett dönt, akkor az érintett szervezetnek biztosítania kell, hogy a hitelesítőeszközök kiadása a szervezet által meghatározott hitelesítés szolgáltató előtt történjen.
4. Ha egy megbízható külső fél által dönt, akkor az érintett szervezetnek meg kell bízni ezt a külső felet, és biztosítania kell, hogy a hitelesítőeszközök kiadása a szervezet által meghatározott hitelesítés szolgáltató előtt történjen.
5. A szervezetnek meg kell határoznia, mely személyek vagy szerepkörök jóváhagyása szükséges a hitelesítőeszközök kiadásához.
6. A szervezetnek naplót kell vezetnie a hitelesítőeszközök kiadásáról, beleértve a kiadás időpontját, a kiadott hitelesítőeszköz típusát, a kiadást jóváhagyó személyeket vagy szerepköröket, és a hitelesítőeszköz kiadásának módját.
7. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hitelesítőeszközök kiadásának szabályzatait és eljárásait, hogy biztosítsa azok megfelelőségét a kiberbiztonsági követelményeknek.
8. A szervezetnek biztosítania kell, hogy az EIR megfelelően védett és biztonságos, hogy megvédje a hitelesítőeszközök kiadásának információit a nem kívánt hozzáféréstől vagy manipulációtól.

KAPCSOLÓDÓ INTÉZKEDÉSEK

8.44. Személyazonosság igazolása

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

IA-5(16)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a meghatározott típusú vagy különleges hitelesítőeszközök illetve a fiókok regisztrációját végző szerv meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.34. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – HAMIS BIOMETRIKUS ADATOKAT FELHASZNÁLÓ TÁMADÁSOK

8.34. A szervezet biometrikus azonosításon alapuló hitelesítéseknél olyan mechanizmusokat alkalmaz, amelyek képesek a támadások - beleértve a hamis biometrikus adatok (például: ujjlenyomat, arckép) használatával elkövetett támadások - észlelésére.

MAGYARÁZAT

Az érintett szervezetnek olyan mechanizmusokat kell alkalmaznia a biometrikus azonosításon alapuló hitelesítéseknél, amelyek képesek a támadások észlelésére, beleértve a hamis biometrikus adatok használatával elkövetett támadásokat. A biometrikus jellemzők nem minősülnek titkoknak. Ilyen jellemzőket online webhelyekről, valakinek a kamerás telefonnal történő lefényképezésével (akár tudtával, akár anélkül), valakinek az érintett tárgyakról történő felvételével (például egy rejtett ujjlenyomat), vagy nagy felbontású kép (például egy íriszminta) rögzítésével lehet megszerezni.

A prezentációs támadások észlelési technológiái, beleértve az életjelek észlelését, csökkenthetik ezeknek a támadásoknak a kockázatát, mivel nehezíti a biometrikus érzékelő átverésére szánt bizonyítékok előállítását. Az EIR-nek képesnek kell lennie arra, hogy észlelje és naplózza ezeket a támadásokat, és megfelelő intézkedéseket tegyen a támadások megelőzése érdekében. Az érintett szervezetnek folyamatosan frissítenie kell az EIR-t, hogy képes legyen azonosítani és kezelni a legújabb fenyegetéseket és támadási vektorokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek be kell vezetnie a prezentációs támadások észlelésének technológiáit.
2. A szervezetnek ki kell dolgoznia és be kell vezetnie olyan mechanizmusokat, amelyek képesek a támadások észlelésére, beleértve a hamis biometrikus adatok (például: ujjlenyomat, arckép) használatával elkövetett támadásokat.
3. A szervezetnek rendszeresen ellenőriznie kell az EIR-t, hogy biztosítsa a biometrikus hitelesítési rendszerek megfelelő működését és a támadások észlelését.

4. A szervezetnek naplót kell vezetnie minden biometrikus azonosítási eseményről, beleértve a sikeres és sikertelen hitelesítéseket, valamint a támadások észlelését. Ez lehetővé teszi az érintett szervezet számára, hogy nyomon követhesse a rendszer teljesítményét és az esetleges biztonsági réseket.
5. A szervezetnek folyamatosan frissítenie és fejlesztenie kell a biometrikus azonosítási rendszereket és a támadások észlelésének mechanizmusait, hogy lépést tudjon tartani a fejlődő fenyegetésekkel és technológiákkal.

Kapcsolódó intézkedések

2.71. Sikertelen bejelentkezési kísérletek

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

IA-5(17)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

8.35. A HITELESÍTÉSRE SZOLGÁLÓ ESZKÖZÖK KEZELÉSE – JELSZÓKEZELŐK

8.35. A szervezet:

8.35.1. Meghatározott jelszókezelőt használ a jelszavak előállításához és kezeléséhez.

8.35.2. A jelszavakat a szervezet által meghatározott ellenőrző mechanizmusokkal védi.

MAGYARÁZAT

Azokban az EIR-kben, ahol statikus jelszavakat alkalmaznak, gyakran kihívást jelent biztosítani, hogy a jelszavak megfelelően bonyolultak legyenek, és hogy ugyanazokat a jelszavakat ne alkalmazzák több EIR-en. A jelszókezelő erre a problémára jelent megoldást, mivel automatikusan generál és tárol erős és egymástól eltérő jelszavakat a különböző fiókokhoz. A jelszókezelők használatának egy lehetséges kockázata, hogy a támadók célba vehetik a jelszókezelő által generált jelszavak gyűjteményét.

Az érintett szervezetnek mechanizmusokat kell meghatároznia, amelyekkel védi a jelszavakat. Ezek a mechanizmusok lehetnek például a jelszavak titkosítása, a jelszavak gyűjteményének offline tárolása, a jelszavak rendszeres megváltoztatása, a jelszavak erősségének ellenőrzése, stb.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek ki kell választania egy meghatározott jelszókezelőt, amely automatikusan előállít és tárol erős és különböző jelszavakat a különböző EIR-ek számára.
2. A szervezetnek biztosítania kell, hogy a jelszókezelő megfelelően bonyolult jelszavakat hozzon létre, és, hogy a felhasználó ne használja ugyanazt a jelszót több rendszerben.
3. A szervezetnek védelmet kell biztosítania a jelszókezelő által generált jelszavak gyűjteményének.
4. A szervezetnek ellenőriznie kell, hogy a jelszavakat megfelelően védik-e a meghatározott mechanizmusok.
5. A szervezetnek dokumentálnia kell a jelszókezelő használatát és a jelszavak védelmét, hogy biztosítsa a folyamat átláthatóságát és ellenőrizhetőségét.

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

IA-5(18)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

8.36. HITELESÍTÉSI INFORMÁCIÓK VISSZAJELZÉSÉNEK ELREJTÉSE

8.36. Az EIR fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt a jogosulatlan személyek általi felfedésétől és felhasználásától.

MAGYARÁZAT

Az EIR visszacsatolása nem szolgáltathat olyan információt, amely lehetővé tenné a jogosulatlan személyek számára a hitelesítési mechanizmusok kijátszását. Egyes típusú eszközöknél, mint például a viszonylag nagy monitorral rendelkező asztali számítógépek vagy notebookok, a fenyegetés jelentős lehet. Más típusú eszközöknél, mint például a kis kijelzővel rendelkező mobil eszközök, a fenyegetés kevésbé jelentős, és arányos a kis billentyűzetek miatti beviteli hibák megnövekedett valószínűségével, így a hitelesítési visszacsatolás elfedésének eszközét ennek megfelelően választhatja ki egy szervezet. A visszacsatolás elhomályosítása (obfuscation) magában foglalja a csillag karakterek megjelenítését, amikor a felhasználók jelszavakat írnak be a beviteli mezőkbe, vagy a visszacsatolás nagyon korlátozott ideig történő megjelenítését, mielőtt a rendszer elfedné azt.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek először meg kell határoznia, hogy mely eszközök esetében jelentős a jogosulatlan személyek általi hitelesítési információ felfedezésének és kihasználásának veszélye.
2. A szervezetnek ki kell választania a megfelelő módszert a visszacsatolás elrejtésére.
3. A szervezetnek implementálnia kell a kiválasztott módszert az EIR-ekben. Ez magában foglalhatja a szoftverfrissítéseket, a beállítások módosítását, vagy új hardverek beszerzését.
4. A szervezetnek dokumentálnia kell a változtatásokat, hogy nyomon követhető legyen a folyamat, és bizonyítékot szolgáltathasson a megfelelőségről.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hitelesítési visszacsatolás elrejtésének módszerét, hogy biztosítsa a folyamatos védelmet a jogosulatlan hozzáférés ellen.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése

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

3.3.9.6. A hitelesítésre szolgáló eszköz visszacsatolása: Az elektronikus információs rendszer fedett visszacsatolást biztosít a hitelesítési folyamat során, hogy megvédje a hitelesítési információt jogosulatlan személyek esetleges felfedésétől, felhasználásától.

ISO/IEC 27001:2023 REFERENCIA

A.8.5

NIST SP 800-53 REV.5 REFERENCIA

IA-6

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

8.37. HITELESÍTÉS KRIPTOGRÁFIAI MODUL ESETÉN

8.37. Az EIR olyan mechanizmusokat alkalmaz a kriptográfiai modul hitelesítéséhez, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának, a hatályos törvényeknek, a végrehajtási utasításoknak, szabályzatoknak, szabványoknak.

MAGYARÁZAT

Az EIR kriptográfiai moduljában hitelesítési mechanizmusokra lehet szükség annak érdekében, hogy hitelesítse a modulhoz hozzáférő operátort, és ellenőrizze, hogy az operátor jogosult-e a kért szerep betöltésére és a szerephez tartozó szolgáltatások végrehajtására.
Az EIR hitelesítési mechanizmusai a kriptográfiai modul hitelesítési útmutatójának, a hatályos törvényeknek, a végrehajtási utasításoknak, szabályzatoknak és szabványoknak megfelelően működnek. Ezek a mechanizmusok biztosítják, hogy csak a megfelelően hitelesített és jogosult felhasználók férjenek hozzá az EIR kriptográfiai moduljához, és végezzenek el műveleteket.
Az EIR hitelesítési mechanizmusai közé tartozhatnak jelszavak, digitális aláírások, biometrikus adatok, hardveres kulcsok és más, a hitelesítési útmutatóban meghatározott eszközök. Ezek a mechanizmusok biztosítják, hogy az EIR kriptográfiai modulja csak a megfelelően hitelesített és jogosult felhasználók számára legyen hozzáférhető.
Az érintett szervezetnek gondoskodnia kell arról, hogy az EIR hitelesítési mechanizmusai megfelelően működjenek, és naplózzák a hitelesítési eseményeket.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, hogy milyen kriptográfiai modul hitelesítési mechanizmusokat kíván alkalmazni.
2. A szervezetnek implementálnia kell ezeket a mechanizmusokat az EIR-en belül.
3. A szervezetnek biztosítania kell, hogy az EIR képes legyen azonosítani és hitelesíteni azokat a felhasználókat, akik hozzáférnek a kriptográfiai modulhoz.
4. A szervezetnek naplózni kell minden hozzáférési kísérletet és műveletet, amelyet a kriptográfiai modulon belül végeznek. Ez lehetővé teszi a szervezet számára, hogy nyomon kövesse és ellenőrizze a modul használatát, és azonosítsa az esetleges biztonsági problémákat.

5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a kriptográfiai modul hitelesítési mechanizmusait, hogy biztosítsa azok hatékonyságát és megfelelőségét a jelenlegi biztonsági követelményeknek.
6. A szervezetnek biztosítania kell, hogy a kriptográfiai modul hitelesítési mechanizmusai megfelelnek a hatályos törvényeknek, szabályzatoknak és szabványoknak.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése
8.21. A hitelesítésre szolgáló eszközök kezelése
16.7. Beszerzések
17.49. Kriptográfiai kulcs előállítása és kezelése
17.53. Kriptográfiai védelem

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

3.3.9.7. Hitelesítés kriptográfiai modul esetén: Az elektronikus információs rendszer egy adott kriptográfiai modulhoz való hitelesítésre olyan mechanizmusokat használ, amelyek megfelelnek a kriptográfiai modul hitelesítési útmutatójának.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IA-7

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

8.38. AZONOSÍTÁS ÉS HITELESÍTÉS (SZERVEZETEN KÍVÜLI FELHASZNÁLÓK)

8.38. Az EIR egyedileg azonosítja és hitelesíti a szervezeten kívüli felhasználókat, tevékenységüket, valamint a nevükben futó folyamatokat.

MAGYARÁZAT

A nem szervezeti felhasználók közé tartoznak azon felhasználók, akik a szervezeti felhasználóktól eltérnek, úgy, mint például szerződéses partnerek, külső projekt résztvevők stb. Ezeket a személyeket a szervezet egyedileg azonosítja és hitelesíti, kivéve a meghatározott és dokumentált hozzáférések esetében. A szervezet a kockázatértékelések alkalmazásával meghatározzák a hitelesítési igényeket. Ennek során az információs rendszerekhez történő egyszerű hozzáférés mellett figyelembe veszik a skálázhatóságot, hatékonyságot és biztonságot is, ezáltal garantálva a kockázatok csökkentését és a fenyegetések enyhítését.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia, kiket tekint nem szervezeti felhasználóknak.
2. A szervezetnek biztosítania kell, hogy a nem szervezeti felhasználók egyedileg azonosíthatók és hitelesíthetők legyenek az EIR-ben.
3. A szervezetnek meg kell fontolnia a nem szervezeti felhasználók egyedi azonosítását és hitelesítését, amikor az EIR-hez való hozzáférnek.
4. A szervezetnek figyelembe kell vennie számos tényezőt - beleértve a biztonságot, az adatvédelmi követelményeket, melyek más jogszabályokból származhatnak, a skálázhatóságot és a használhatóságot - amikor mérlegeli a szervezeti információkhoz és az EIR-hez való hozzáférés könnyű használatának szükségességét a kockázatok megfelelő mérséklésének és védelmének szükségességével.
5. A szervezetnek naplóznia kell a nem szervezeti felhasználók tevékenységét és az ő nevükben futó folyamatokat az EIR-ben. Ez segít azonosítani és nyomon követni a potenciális veszélyeket és kockázatokat.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.2. Fiókkezelés

2.60. Legkisebb jogosultság elve

2.88. Azonosítás vagy hitelesítés nélkül engedélyezett tevékenységek

2.100. Távoli hozzáférés

2.108. Vezeték nélküli hozzáférés

4.13. Naplóbejegyzések felülvizsgálata, elemzése és jelentéstétel

8.2. Azonosítás és hitelesítés

8.14. Azonosító kezelés

8.21. A hitelesítésre szolgáló eszközök kezelése

8.42. Helyzetfüggő hitelesítés

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

3.3.9.8. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

ISO/IEC 27001:2023 REFERENCIA

A.5.16

NIST SP 800-53 REV.5 REFERENCIA

IA-8

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

8.39. AZONOSÍTÁS ÉS HITELESÍTÉS (SZERVEZETEN KÍVÜLI FELHASZNÁLÓK) – MEGHATÁROZOTT AZONOSÍTÁSI PROFILOK HASZNÁLATA

8.39. A szervezet meghatározott profilokat alkalmaz az azonosítási folyamat során.

MAGYARÁZAT

Az érintett szervezet nyílt személyazonosság-kezelési szabványok alapján azonosítási profilokat határoz meg a személyazonosság-kezeléshez. Annak biztosítása érdekében, hogy a nyílt személyazonosság-kezelési szabványok a dokumentáltak szerint életképesek, szilárdak, megbízhatóak, fenntarthatóak és interoperábilisak legyenek, az arra feljogosított állami szervek értékelhetik a szabványokat és a technológiai megvalósításokat, és a vonatkozó törvények, végrehajtási rendeletek, irányelvek, szabályok, szabályzatok, szabványok és iránymutatások alapján vizsgálják azokat.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia az azonosítási profilokat, amelyeket az azonosítási folyamat során alkalmazni kíván.
2. A szervezetnek biztosítania kell, hogy választott és használt nyílt személyazonosság-kezelési szabvány életképes, megbízható, fenntartható és interoperábilis más rendszerekkel, rendszerelemekkel.
3. A szervezetnek értékelnie kell a szabványokat és a technológiai megvalósításokat az alkalmazandó törvények, rendeletek, irányelvek, szabályozások és irányelvek alapján.
4. A szervezetnek be kell vezetnie az EIR-ben az azonosítási profilokat.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a meghatározott azonosítási profilokat az EIR-ben, annak érdekében, hogy biztosítsa azok folyamatos megfelelőségét.

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

IA-8(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az identitáskezelési profilok meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

8.40. AZONOSÍTÁS ÉS HITELESÍTÉS (SZERVEZETEN KÍVÜLI FELHASZNÁLÓK) – PKI ALAPÚ HITELESÍTŐ ADATOK ELFOGADÁSA

8.40. A szervezet elfogadja és ellenőrzi a PKI hitelesítő adatokat, amelyek megfelelnek a szervezet által meghatározott előírásoknak.

MAGYARÁZAT

A PKI (Public Key Infrastructure - Nyilvános Kulcs Infrastruktúra) egy biztonsági megoldás, amely titkosított kommunikációt tesz lehetővé. A PKI használatával a szervezetek digitális tanúsítványokat használhatnak a felhasználók, szerverek és kliensgépek azonosítására.
A szervezet csak azokat a PKI hitelesítő adatokat fogadja el és használja, melyek megfelelnek az általa előzetesen meghatározott biztonsági szabványoknak és előírásoknak. Ez magában foglalhatja például a tanúsítási szolgáltatók (CA) megbízhatóságának ellenőrzését, a tanúsítvány kiadásának és használatának szabályainak betartását, és annak biztosítását, hogy a tanúsítványokat megfelelően tárolják és kezelik.
Az ellenőrzési folyamat része a PKI rendszernek, amelynek során a szervezet megbizonyosodik arról, hogy a tanúsítványok érvényesek-e, nem lettek-e visszavonva, és hogy a titkosítás megfelelő szintű-e. A hitelesítő adatok ellenőrzése segít megvédeni a szervezetet a veszélyektől, mint például a közbeiktatásos támadásoktól (Man-in-the-Middle támadások), a hamis tanúsítványoktól vagy a hitelesítő adatok illetéktelen felhasználásától.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia a PKI hitelesítő adatokra vonatkozó előírásokat. Ezek az előírások tartalmazhatják a hitelesítő adatok típusát, a hitelesítési folyamatot, a hitelesítő adatok érvényességi idejét, stb.
2. A szervezetnek implementálnia kell egy rendszert, amely képes elfogadni és ellenőrizni a PKI hitelesítő adatokat. Ez a rendszer lehet egy belső EIR, vagy egy külső szolgáltató által biztosított rendszer.

3. A szervezetnek biztosítania kell, hogy az EIR képes legyen ellenőrizni a PKI hitelesítő adatokat. Ez magában foglalja a hitelesítő adatok ellenőrzését, a hitelesítő adatok érvényességének ellenőrzését, és a hitelesítő adatok hitelesítésének ellenőrzését.
4. A szervezetnek naplóznia kell minden PKI hitelesítő adat elfogadást és ellenőrzést. Ez a napló tartalmazza az elfogadott és ellenőrzött hitelesítő adatokat, az ellenőrzés időpontját, az ellenőrzést végző személyt, stb.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a PKI hitelesítő adatokra vonatkozó előírásokat, hogy biztosítsa azok relevanciáját és hatékonyságát.
6. A szervezetnek biztosítania kell, hogy minden érintett személy tisztában van a PKI hitelesítő adatok elfogadásának és ellenőrzésének folyamatával, és képesek betartani az előírásokat.

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

IA-8(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a szabályzat meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.41. SZOLGÁLTATÁS AZONOSÍTÁSA ÉS HITELESÍTÉSE

8.41. A szervezet egyedileg azonosítja és hitelesíti a meghatározott rendszerszolgáltatásokat és alkalmazásokat, mielőtt kapcsolatot létesítene az eszközökkel, felhasználókkal, szolgáltatásokkal vagy alkalmazásokkal.

MAGYARÁZAT

Azonosítást és hitelesítést igénylő szolgáltatások lehetnek például a digitális tanúsítványokat használó webes alkalmazások vagy az adatbázisokat lekérdező szolgáltatások vagy alkalmazások. A rendszerszolgáltatások és alkalmazások azonosítási és hitelesítési módszerei közé tartozik például az információ vagy kód aláírás és a szolgáltatások forrását jelző elektronikus aláírások. Az azonosítási és hitelesítési igények érvényességére vonatkozó döntéseket az e döntések alapján eljáró szolgáltatásoktól független szolgáltatások is meghozhatják. Ez előfordulhat például földrajzilag vagy másképp elosztott architektúrákban. Ilyen helyzetekben az azonosítási és hitelesítési döntéseket (a tényleges azonosítók és hitelesítési adatok helyett) a döntést végrehajtó szolgáltatások kapják meg.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek azonosítania kell azokat a szolgáltatásokat és alkalmazásokat, amelyek egyedi azonosítást és hitelesítést igényelnek.
2. A szervezetnek implementálnia kell az egyedi azonosítást és hitelesítési rendszerét az EIR-jében a meghatározott rendszerszolgáltatások, alkalmazások esetében. Figyelembe veszi a helyi sajátosságokat elosztott rendszer esetén.
3. A szervezetnek naplózza az egyedi azonosítási és hitelesítési kéréseket, hogy nyomon követhesse és ellenőrizhesse az azonosítási és hitelesítési folyamatokat.
4. A szervezet dokumentálja és rendszeresen felülvizsgálja a kialakított rendszer dokumentációját, hogy nyomon követhesse a rendszer változásait és megfeleljen a változó kiberbiztonsági követelményeknek.

KAPCSOLÓDÓ INTÉZKEDÉSEK

8.10. Eszközök azonosítása és hitelesítése

8.14. Azonosító kezelés

8.21. A hitelesítésre szolgáló eszközök kezelése

17.40. Az adatátvitel bizalmassága és sértetlensége

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

IA-9

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a rendszerszolgáltatások és alkalmazások meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.42. HELYZETFÜGGŐ HITELESÍTÉS

8.42. A szervezet megköveteli, hogy a rendszerhez hozzáférő egyének meghatározott kiegészítő hitelesítési technikákat vagy eszközöket alkalmazzanak meghatározott konkrét körülmények vagy helyzetek esetén.

MAGYARÁZAT

A támadók kompromittálhatják az érintett szervezet által alkalmazott egyéni hitelesítési mechanizmusokat, és ezt követően megpróbálhatják magukat legitim felhasználóknak kiadni. E fenyegetés kezelésére a szervezet speciális technikákat vagy mechanizmusokat alkalmazhat, és protokollokat hozhat létre a gyanús viselkedés értékelésére. A gyanús viselkedés magában foglalhatja az olyan információkhoz való hozzáférést, amelyekhez a szervezethez köthető személyek általában nem férnek hozzá feladataik, szerepük vagy felelősségi körük részeként; nagyobb mennyiségű információhoz való hozzáférést, mint amihez az egyének rutinszerűen hozzáférnek; vagy gyanús hálózati címekről való hozzáférési kísérletet. Előre meghatározott feltételek vagy kiváltó okok bekövetkezésekor az érintett szervezet további hitelesítési információk megadására kötelezheti a felhasználókat. Az adaptív hitelesítés másik lehetséges felhasználási módja a mechanizmus erősségének növelése a hozzáférni kívánt rekordok száma vagy típusa alapján. A kiegészítő hitelesítés nem helyettesíti a többfaktoros hitelesítési mechanizmusokat, és nem arra szolgál, hogy elkerülje azok használatát, hanem kiegészítheti a többfaktoros hitelesítés megvalósítását.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia és alkalmaznia kell azokat a hitelesítési technikákat vagy eszközöket, amelyeket az EIR-hez hozzáférő felhasználóknak bizonyos körülmények vagy helyzetek esetén használniuk kell.
2. A szervezetnek szabályokat kell meghatároznia és beállítania a gyanús viselkedés értékelésére.
3. Amikor az előre meghatározott feltételek vagy kiváltó okok bekövetkeznek, a szervezet rendszere további hitelesítési információkat kérhet be az egyénektől.

KAPCSOLÓDÓ INTÉZKEDÉSEK

8.2. Azonosítás és hitelesítés

8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

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

IA-10

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a kiegészítő hitelesítési technikák vagy eszközök illetve a körülmények vagy helyzetek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

8.43. ÚJRAHITELESÍTÉS

8.43. A szervezet meghatározott körülmények vagy helyzetek esetén megköveteli a felhasználótól az újrahitelesítést.

MAGYARÁZAT

Az eszközök zárolásával kapcsolatos újrahitelesítési követelményeken túl az érintett szervezet bizonyos helyzetekben megkövetelheti az egyének újrahitelesítését, beleértve, amikor a szerepkörök, hitelesítők vagy a hitelesítéssel kapcsolatos adatok megváltoznak. Emellett akkor is kérheti egy érintett szervezet az újrahitelesítést, amikor az EIR biztonsági osztálya megváltozik, illetve privilegizált funkciók futnak le egy meghatározott időszak után, vagy időszakosan.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek meg kell határoznia azokat a körülményeket vagy helyzeteket, amikor újrahitelesítést kér az egyénektől. Ilyen körülmény vagy helyzet lehet például szerepkört, hitelesítőt vagy hitelesítési adatokat érintő változás, az EIR biztonsági osztályának változása, privilegizált funkciók rendszeres vagy meghatározott időszak utáni végrehajtása.
2. A szervezetnek szabályoznia kell az újrahitelesítést, melynek során meghatározza az újrahitelesítési eljárásokat és kritériumokat. Ez magában foglalhatja a hitelesítési adatok újbóli megadását, a biometrikus adatok használatát, vagy a többtényezős hitelesítést.
3. A szervezetnek biztosítania kell, hogy az EIR képes legyen kezelni az újrahitelesítési kéréseket. Ez magában foglalhatja a szükséges hardver- és szoftverfrissítések végrehajtását, valamint a hitelesítési protokollok és mechanizmusok beállítását.
4. A szervezetnek naplóznia kell az újrahitelesítési eseményeket. Ez lehetővé teszi az érintett szervezet számára, hogy nyomon kövesse és elemezze az újrahitelesítési tevékenységeket, és szükség esetén beavatkozzon.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell az újrahitelesítésre vonatkozó szabályzatát és eljárásrendjeit annak érdekében, hogy biztosítsa azok hatékonyságát és aktualitását. Ez magában foglalhatja a szabályzat és eljárásrendek felülvizsgálatát, a

felhasználói visszajelzések és a naplóelemzések alapján történő módosításokat, valamint a legújabb biztonsági trendek és fenyegetések figyelembevételét.

KAPCSOLÓDÓ INTÉZKEDÉSEK

2.15. Hozzáférés-ellenőrzés érvényesítése
2.82. Eszköz zárolása
8.2. Azonosítás és hitelesítés
8.10. Eszközök azonosítása és hitelesítése
8.14. Azonosító kezelés
8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

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

IA-11

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat a körülmények vagy helyzetek esetén szükséges újrahitelesítés meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
X	X	X

8.44. SZEMÉLYAZONOSSÁG IGAZOLÁSA

8.44. A szervezet:

8.44.1. Azonosítja azokat a felhasználókat, akiknek a rendszerekhez való logikai szintű hozzáféréshez olyan felhasználói fiókra van szükségük, ami teljesíti a vonatkozó szabványokban vagy irányelvekben meghatározott szintű, a személyazonosság bizonyítására vonatkozó követelményeket.

8.44.2. A felhasználói azonosítókat hozzárendeli egy egyedi személyhez.

8.44.3. Összegyűjti, hitelesíti és ellenőrzi a személyazonosságot igazoló bizonyítékokat.

MAGYARÁZAT

A személyazonosság igazolása a felhasználó kilétéhez köthető információk összegyűjtésének, hitelesítésének és ellenőrzésének folyamata, amelynek célja a hitelesítő adatok létrehozása, melyek lehetővé teszik az EIR-hez történő hozzáférést. A személyazonosság igazolása arra irányul, hogy csökkentse a felhasználók regisztrációjával és fiókjaik létrehozásával kapcsolatos fenyegetéseket. Az érintett szervezeteknek figyelembe kell venniük a jogszabályi előírásokat, illetve az ennek megfelelően kialakított belső szabályzataikat a személyazonosságot igazoló bizonyítékok gyűjtése során. A személyazonosságot igazoló bizonyítékokat érintő jogi és belső, szervezeti szabályzattal kapcsolatos kérdések vonatkozásában az érintett szervezet munkavállalói állásfoglalást kérhetnek a jogi, illetve egyéb, az említett témakör megválaszolásában kompetenciával rendelkező felelős szervezeti területtől.

A KÖVETELMÉNY ALKALMAZÁSÁNAK LÉPÉSEI

1. A szervezetnek igazolnia kell azoknak a felhasználóknak a személyazonosságát, akiknek az EIR-hez hozzáférésre van szükségük.
2. A felhasználói azonosítókat hozzá kell rendelnie egy egyedi személyhez.
3. A szervezetnek össze kell gyűjtenie, hitelesítenie és ellenőriznie a személyazonosságot igazoló bizonyítékokat. Ez magában foglalja a személyazonosságot igazoló dokumentumok, például személyi igazolványok, útlevelek vagy jogosítványok ellenőrzését és hitelesítését.
4. A szervezetnek tisztában kell lennie azzal, hogy milyen törvények, rendeletek, irányelvek, szabályozások vonatkozhatnak a személyazonosságot igazoló bizonyítékok gyűjtésére.

5. A szervezetnek dokumentálnia kell a felhasználói hozzáféréseket és az azonosítási folyamatokat, hogy biztosítsa a folyamatok átláthatóságát és ellenőrizhetőségét.

Kapcsolódó intézkedések

2.59. Felelősségek szétválasztása
8.1. Szabályzat és eljárásrendek
8.2. Azonosítás és hitelesítés
8.10. Eszközök azonosítása és hitelesítése
8.14. Azonosító kezelés
8.21. A hitelesítésre szolgáló eszközök kezelése
8.36. Hitelesítési információk visszajelzésének elrejtése
8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

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

IA-12

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	X	X

8.45. Személyazonosság igazolása – Felettes jóváhagyása

8.45. A szervezet előírja, hogy a logikai hozzáféréshez szükséges fiók regisztrációs folyamatában szerepeljen a felettes vagy a támogató (vezető) engedélye.

Magyarázat

A felettes vagy támogató engedélyének beépítése a regisztrációs folyamatba egy további ellenőrzési szintet biztosít annak érdekében, hogy a menedzsment tudomással bírjon a felhasználói fiók létezéséről, megbizonyosodjon arról, hogy a felhasználói fiók használata szükséges a szervezet céljainak és üzleti folyamatainak végrehajtásához, illetve, hogy a felhasználó jogosultságai megfelelőek a szervezeten belül elvárt feladataihoz/felelősségi köréhez.

A követelmény alkalmazásának lépései

1. A szervezetnek szabályzatba kell foglalnia, hogy a logikai hozzáféréshez szükséges felhasználói fiók regisztrációs folyamatában szerepeljen a felettes vagy a támogató jóváhagyásának szükségessége. Az érintett szervezetnek az ehhez szükséges eljárásrendet is meg kell alkotnia és át kell ültetnie a gyakorlatba.
2. A szervezetnek biztosítania kell, hogy a felettesek vagy vezetők a felhasználói fiókok jóváhagyásához megfelelően képzettek legyenek. Az érintett szervezet mindezt biztonságtudatossági képzéssel és a felhasználói fiókokat érintő regisztrációs folyamatokkal kapcsolatos oktatás biztosításával érheti el.
3. A szervezetnek képesnek kell lennie nyomon követni és naplózni a felhasználói fiókok regisztrálásának folyamatát, beleértve a felettesek vagy vezetők jóváhagyását. Ez lehetővé teszi az érintett szervezet számára annak ellenőrzését, hogy a szabályzatokat és eljárásrendeket betartják-e.
4. A szervezetnek rendszeresen felül kell vizsgálnia és értékelnie kell a felhasználói fiókokat érintő regisztrációs folyamatot, illetve a felettesek vagy vezetők jóváhagyásának folyamatát, annak érdekében, hogy biztosítsa a folyamat hatékonyságát és biztonságát. Ez magában foglalhatja a naplók áttekintését és a folyamatok felülvizsgálatát.

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

IA-12(1)

A követelményhez meghatározandó paraméterek

Nincs meghatározandó paraméter.

A követelmény biztonsági osztálya

Alap	Jelentős	Magas
-	-	-

8.46. Személyazonosság igazolása – Személyazonosság bizonyítéka

8.46. A szervezet megköveteli a személyazonosságot igazoló bizonyíték bemutatását a fiókok regisztrációját végző szervnél.

Magyarázat

A személyazonosságot igazoló bizonyítékok - mint például dokumentumok bemutatása bizonyítékként vagy dokumentumok és biometrikus adatok együttes alkalmazása - csökkentik annak a valószínűségét, hogy egyének hamis bizonyítékok bemutatásával igazolják személyazonosságukat, illetve növelik egy lehetséges támadás végrehajtásának idejét. Az elfogadható bizonyítékok formái összhangban vannak a felhasználói fiókhoz kapcsolódó EIR-ekkel, szerepkörökkel és jogosultságok kockázataival.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a személyazonosság igazolására szolgáló bizonyítékokat. Ezek lehetnek dokumentumok, biometrikus adatok, vagy ezek kombinációja.
2. A szervezetnek meg kell bizonyosodnia arról, hogy a személyazonosság igazolására szolgáló bizonyítékok csökkentik egy jogosulatlan fél belépésének lehetőségét, illetve növelik egy sikeres támadás végrehajtásának idejét.
4. A szervezetnek meg kell követelnie a személyazonosságot igazoló bizonyíték bemutatását a fiókok regisztrációját végző szervnél.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a személyazonosságot igazoló bizonyítékokkal kapcsolatos szabályzatait és eljárásrendjeit, hogy biztosítsa azok hatékonyságát és relevanciáját.

Kapcsolódó intézkedések

Nincs kapcsolódó követelménypont!

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

Nincs vonatkozó referencia.

ISO/IEC 27001:2023 REFERENCIA

Nincs vonatkozó referencia.

NIST SP 800-53 REV.5 REFERENCIA

IA-12(2)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

8.47. Személyazonosság igazolása – Személyazonossági bizonyítékok hitelesítése és ellenőrzése

8.47. A szervezet megköveteli a bemutatott személyazonosságot igazoló bizonyíték meghatározott módszerekkel történő hitelesítését és ellenőrzését.

Magyarázat

A személyazonosságot igazoló bizonyítékok hitelesítése és ellenőrzése segít megbizonyosodni arról, hogy a fiókok és azonosítók a megfelelő felhasználó számára kerültek létrehozásra, és az azonosítást elősegítő eszközök is a megfelelő felhasználóhoz köthetők. A hitelesítés azt a folyamatot jelenti, amely megerősíti, hogy a bizonyíték valódi és hiteles, valamint a bizonyítékban szereplő adatok helyesek, naprakészek és egy egyénhez köthetők. A bemutatott bizonyíték alapján az ellenőrzés megerősíti és összeköti a vélt személyazonosságot a felhasználó valós állapotával. A személyazonosságot igazoló bizonyítékok hitelesítésére és ellenőrzésére szolgáló módszerek összhangban vannak a felhasználói fiókhoz kapcsolódó EIR-ekkel, szerepkörökkel és beállított jogosultságok kockázataival.

A követelmény alkalmazásának lépései

1. A szervezetnek meg kell határoznia a személyazonosság igazolására szolgáló bizonyítékot. Ez lehet hivatalos okmány vagy digitális azonosító (pl.: felhasználónév és jelszó, biometrikus adatok).
2. A szervezetnek ki kell dolgoznia egy hitelesítési és ellenőrzési eljárást, amely meghatározza, hogyan ellenőrzi és hitelesíti a bemutatott személyazonossági bizonyítékot. Ez magában foglalhatja a dokumentumok vizuális ellenőrzését, digitális aláírások ellenőrzését, biometrikus adatok összehasonlítását, stb.
3. A szervezetnek be kell építenie ezt az eljárást az EIR-be, hogy automatikusan ellenőrizze és hitelesítse a személyazonossági bizonyítékot minden alkalommal, amikor egy felhasználó hozzáférni próbál az EIR-hez.

4. A szervezetnek naplóznia kell minden hitelesítési és ellenőrzési tevékenységet, hogy nyomon követhető legyen, ki, mikor és milyen bizonyítékot mutatott be.
5. A szervezetnek rendszeresen felül kell vizsgálnia és frissítenie kell a hitelesítési és ellenőrzési eljárásokat, hogy biztosítsa, hogy azok továbbra is megfelelnek a kiberbiztonsági követelményeknek és választ adnak a legújabb fenyegetésekre.
6. Az érintett szervezetnek biztosítania kell, hogy a hitelesítési és ellenőrzési eljárások megfelelnek a vonatkozó jogszabályoknak és szabványoknak, beleértve a kiberbiztonsági előírásokat.

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

IA-12(3)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az hitelesítésre és ellenőrzésre vonatkozó módszerek meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

8.48. Személyazonosság igazolása – Személyes jelenlét melletti hitelesítés és ellenőrzés

8.48. A szervezet megköveteli, hogy a személyazonosságot igazoló bizonyítékok hitelesítését és ellenőrzését személyes jelenlét mellett a fiókok regisztrációját végző szerv előtt kell elvégezni.

Magyarázat

A személyes jelenlét során, fizikai formában meglévő személyazonosságot igazoló dokumentumok bemutatása, illetve a fiókok regisztrációját végző szervvel történő személyes interakciók csökkentik a hamis dokumentumok általi azonosítás lehetőségét.

A követelmény alkalmazásának lépései

1. A szervezetnek létre kell hoznia egy, a felhasználói fiókok regisztrálását végző szervet, amely felelős lesz a személyazonosságot igazoló bizonyítékok hitelesítéséért és ellenőrzéséért.
2. A szervezetnek biztosítania kell, hogy a regisztrációs szerv megfelelően képzett és felkészült a személyazonosságot igazoló bizonyítékok hitelesítésének és ellenőrzésének elvégzésére.
3. A szervezetnek szabályzatba kell foglalnia, hogy a személyazonosságot igazoló bizonyítékok hitelesítését és ellenőrzését személyes jelenlét mellett kell elvégezni.
4. A szervezetnek be kell vezetnie egy naplózási rendszert, amely rögzíti és nyomon követi a személyazonosságot igazoló bizonyítékok hitelesítésének és ellenőrzésének minden lépését.
5. A szervezetnek biztosítania kell, hogy a hitelesítési és ellenőrzési eljárások megfelelnek a vonatkozó jogszabályoknak és szabványoknak, beleértve a kiberbiztonsági előírásokat.

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

IA-12(4)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	X

8.49. Személyazonosság igazolása – Cím megerősítése

8.49. A szervezet megköveteli, hogy egy regisztrációs kód vagy megerősítő értesítés egy másodlagos csatornán keresztül kerüljön kézbesítésre, hogy a felhasználók nyilvántartásba vett (fizikai vagy elektronikus) címe ellenőrzésre kerüljön.

Magyarázat

Az érintett szervezet másodlagos megoldásokat használ annak megerősítésére, hogy a személyek nyilvántartásba vett címe megegyezzen azzal a személlyel, aki részt vett a regisztrációs folyamatban. Ezzel az érintett szervezet megnehezítheti a támadók számára, hogy legitim felhasználóknak adják ki magukat a személyazonosság igazolására szolgáló folyamat során. A megerősítés lehet egy ideiglenes regisztrációs kód vagy egy megerősítő értesítés. Ezeknek a kézbesítési címét nem a felhasználó által önként választott, hanem a szervezet nyilvántartásból származik. A cím lehet fizikai vagy elektronikus cím. A lakcím például fizikai címnek minősül, míg az e-mail címek és a telefonszámok a digitális címekhez sorolhatók.

A követelmény alkalmazásának lépései

1. A szervezetnek be kell vezetnie egy másodlagos csatornát a regisztrációs kód vagy megerősítő értesítés kézbesítésére.
2. Az érintett szervezetnek naplóznia kell, hogy nyomon követhesse a regisztrációs kódok és megerősítő értesítések kézbesítését. A naplózás segít az érintett szervezetnek abban, hogy ellenőrizze, hogy a kódok és értesítések valóban eljutottak-e a felhasználókhoz.
3. A szervezetnek meg kell bizonyosodnia róla, hogy a regisztrációs folyamat megfelel a kiberbiztonsági követelményeknek. Ez magában foglalja a másodlagos csatorna használatának ellenőrzését, illetve a regisztrációs kódok és megerősítő értesítések kézbesítésének ellenőrzését.

Kapcsolódó intézkedések

8.44. Személyazonosság igazolása

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

IA-12(5)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

Nincs meghatározandó paraméter.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	X	X

8.50. Személyazonosság igazolása – Külsőleg hitelesített személyazonosság elfogadása

8.50. A szervezet elfogadja a külsőleg igazolt személyazonosságokat a szervezet által meghatározott személyazonosság megbízhatósági szinten.

Magyarázat

A személyazonosságok felesleges újbóli igazolásának érdekében, különösen a személyazonosság igazolására kártyát nem használók esetében, az érintett szervezet elfogadja azokat az igazolásokat, amelyeket más szervezetek azonos biztonsági szint mellett végeztek. Az igazolás összhangban van az érintett szervezet biztonsági szabályzatával és a személyazonossági igazolásának szintje megfelel a hozzáférhető EIR-nek, alkalmazásnak vagy információnak. A külsőleg igazolt személyazonosságok elfogadása alapvető része a összevont személyazonosságok kezelésének az érintett szervezetek között.

A követelmény alkalmazásának lépései

1. A szervezetnek először meg kell határoznia a személyazonosság megbízhatósági szintjét, amelyet a hozzáférhető EIR-ek, alkalmazások vagy információk igényelnek.
2. A szervezetnek ki kell dolgoznia egy szabályzatot, amely összhangban van a személyazonosság megbízhatósági szintjével.
3. A szervezetnek meg kell bizonyosodnia arról, hogy a külső szervezetek által végzett személyazonosság igazolás megfelel a saját biztonsági szabályzatának és a személyazonosság megbízhatósági szintjének.
4. Az szervezetnek kezelnie kell az összevont személyazonosságokat, amelyek a külső szervezetek által igazolt személyazonosságokat tartalmazzák.

Kapcsolódó intézkedések

8.10. Eszközök azonosítása és hitelesítése
8.14. Azonosító kezelés
8.21. A hitelesítésre szolgáló eszközök kezelése
8.38. Azonosítás és hitelesítés (szervezeten kívüli felhasználók)

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

IA-12(6)

A KÖVETELMÉNYHEZ MEGHATÁROZANDÓ PARAMÉTEREK

A követelményponthoz kapcsolódó szervezeti feladat az a személyazonosság bizonyítására vonatkozó követelmények meghatározása.

A KÖVETELMÉNY BIZTONSÁGI OSZTÁLYA

Alap	Jelentős	Magas
-	-	-

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

hatosag@nki.gov.hu

+36 (1) 206 9320

2024