

Hogyan kell nyilvántartani a hitelesítő eszközöket?

VFP2 KiberVéd - NIS2 Audit felkészítés jogi
állásfoglalás 2026/35

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.02	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A 7/2024. (VI. 24.) MK rendelet nem határozza meg a hitelesítő eszköz fogalmát, és nem ír elő „hitelesítőeszköz-nyilvántartás” elnevezésű dokumentumot sem. A fogalom a rendelet alapjául szolgáló NIST SP 800-53 kontrollkatalógus „authenticator” kifejezésének fordítása: mindaz, amit a felhasználó, a szolgáltatás vagy az eszköz birtokol, és a hitelesítés során bemutat annak igazolására, hogy valóban az, akinek mondja magát. Ide tartozik a jelszó és a PIN-kód, a hardveres és a szoftveres token, az intelligens kártya, a tanúsítvány és a privát kulcs, az API-kulcs, a biometrikus jellemző, továbbá a fizikai belépést biztosító kitűző, belépőkártya és kulcs.

A nyilvántartási kötelezettség ennek ellenére fennáll, mert a rendelet több, minden biztonsági osztályban kötelező követelménye csak nyilvántartás alapján teljesíthető. A rendelet a hitelesítő eszközök kiadását adminisztratív eljáráshoz és az átvevő identitásának ellenőrzéséhez köti, az elvesztett vagy kompromittált eszközök kezelését és a visszavonást pedig eljárásrendben követeli meg. Előírja a kilépő munkatárs és a külső személy valamennyi hitelesítő eszközének visszavonását, a fizikai belépést ellenőrző eszközökről pedig kifejezetten nyilvántartás vezetését várja el. Mindez csak akkor igazolható, ha a szervezet bármikor meg tudja mondani, kinek milyen hitelesítő eszközt adott ki, az mihez ad hozzáférést, és mi a státusza.

A nyilvántartás nem tartalmazhatja magát a titkot, vagyis a jelszót, a kulcsot vagy a token magját. A rendelet a hitelesítő eszközök tartalmát az illetéktelen nyilvánosságra hozatal ellen védeni rendeli, ezért a nyilvántartásban csak az eszköz azonosítója, típusa, birtokosa, célja, kiadásának és visszavonásának adatai szerepelhetnek.

Kis- és középvállalkozások számára a legjobb megoldás, ha nem külön táblázatot építenek, hanem a már meglévő rendszereket teszik a nyilvántartás forrásává: a központi identitáskezelőt a fiókokhoz és a többtényezős hitelesítéshez, a titoktárat a szolgáltatásfiókokhoz és az API-kulcsokhoz, a tanúsítványlistát a kulcsokhoz, egy egyszerű, de fegyelmezetten vezetett listát pedig a fizikai tokenekhez és a belépőkártyákhoz. A be- és kiléptetési ellenőrzőlista és a legalább évenkénti felülvizsgálat teszi teljessé a rendszert.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy NIS2-kötelezett szervezet (a továbbiakban mint „Szervezet”) az információbiztonsági szabályzatának és eljárásrendjeinek kidolgozása során azzal szembesül, hogy a 7/2024. (VI. 24.) MK rendelet több helyen említi a „hitelesítő eszköz” fogalmát, a fogalmat azonban nem határozza meg, és nem mondja ki egyértelműen, hogy ezekről milyen nyilvántartást kell vezetni. A vizsgálandó kérdés az, hogy a Rendelet mit ért hitelesítő eszköz alatt, és milyen előírások vonatkoznak a hitelesítő eszközök kiadására és nyilvántartására, valamint hogyan tud egy kis- vagy középvállalkozás ezeknek a követelményeknek aránytalan teher nélkül megfelelni.

A jelszavakra vonatkozó technikai követelmények és a többtényezős hitelesítés bevezetésének módja nem tárgya ennek az állásfoglalásnak.

3. GYAKORLATI JAVASLATOK

3.1 A nyilvántartás javasolt adattartalma

A rendelet nem írja elő a nyilvántartás adattartalmát, az a fenti követelményekből azonban levezethető. Javasoljuk, hogy a nyilvántartás hitelesítő eszközönként legalább a következőket tartalmazza:

- a) Az eszköz típusa és azonosítója például jelszó, hitelesítő alkalmazás, hardveres kulcs, intelligens kártya, tanúsítvány, API-kulcs, belépőkártya, kulcs; sorozatszám, tanúsítvány-ujjlenyomat, kulcsazonosító vagy kártyaszám. A titok maga soha.
- b) A birtokos, természetes személy (munkatárs vagy külső személy, a foglalkoztató szervezet megjelölésével), szolgáltatásfiók, eszköz vagy csoport, valamint a hozzá tartozó azonosító.
- c) A cél és a hatókör, melyik fiókhoz, rendszerhez vagy helyiséghez ad hozzáférést, és milyen szerepet tölt be (egyedüli hitelesítő, többtényezős hitelesítés egyik tényezője, privilegizált hozzáférés).
- d) Az életciklus adatai: a kiadás időpontja, a kiadó és az átvevő, az identitás ellenőrzésének módja, az aktiválás, a tervezett lejárat vagy csere, a visszavonás vagy visszavétel időpontja és oka, a selejtezés.
- e) A státusz, aktív, felfüggesztett, elveszett vagy kompromittált, visszavont, selejtezett.
- f) A felülvizsgálat, az utolsó felülvizsgálat időpontja és eredménye.

3.2 Jó gyakorlatok és megoldások KKV-k számára

Egy kis- vagy középvállalkozásnak nem kell külön nyilvántartó rendszert beszereznie. A cél az, hogy a fenti adattartalom bármikor előállítható és bemutatható legyen. Ehhez a legtöbb esetben a meglévő rendszerek elegendők, ha a Szervezet tudatosan azokat jelöli ki a nyilvántartás forrásának.

A központi címtár és identitáskezelő (helyi Active Directory, Microsoft Entra ID, Google Workspace vagy más identitásszolgáltató) a jelszavak, a hitelesítő alkalmazások és a regisztrált biztonsági kulcsok hiteles forrása. Ezek a rendszerek felhasználónként mutatják, milyen hitelesítési módszerek vannak beállítva, mikor történt az utolsó jelszócsere, és naplózzák a regisztrációt és a törlést. Ezt nem kell táblázatban megismételni: elég, ha a Szervezet a szabályzatában rögzíti, hogy a logikai hitelesítők nyilvántartása az identitáskezelő rendszer. Az auditon a rendszerből lekért, dátummal ellátott jelentés igazol.

A hardveres tokenek és az intelligens kártyák esetében az identitáskezelő csak a regisztráció tényét mutatja, a fizikai eszköz sorozatszámát, az átvételt és a visszavételt nem. Erre elegendő egy egyszerű, verziókövetett táblázat vagy az eszköznyilvántartó, illetve hibajegykezelő rendszer egy kategóriája, amelyben minden eszközhöz átadás-átvételi bejegyzés tartozik. A tokeneket célszerű a rendszerelem-leltárral azonos eszközazonosítóval nyilvántartani, hogy a két nyilvántartás összeérjen.

A szolgáltatásfiókok, az API-kulcsok és a beágyazott titkok a KKV-k leggyakrabban elfelejtett hitelesítő eszközei. Ezekhez titoktár (üzleti jelszókezelő vagy titokkezelő szolgáltatás)

használatát javasoljuk, amely minden bejegyzéshez tulajdonost, célt és lejáratot rendel, a hozzáférést naplózza, és a titkot titkosítva tárolja. A titoktár bejegyzéslistája, a titkok értéke nélkül exportálva, egyben a nyilvántartás is.

A tanúsítványokról és a kulcsokról lejárati dátummal ellátott lista szükséges, amelyet a kibocsátó rendszer vagy egy egyszerű felügyeleti eszköz automatikusan is előállíthat. A lejárt tanúsítvány miatt leálló szolgáltatás a KKV-knál gyakori, jól megelőzhető incidens.

A belépőkártyákról a beléptető rendszer kártyalistája, a kulcsokról kulcsnyilvántartó füzet vagy táblázat vezetendő, kiadási és visszavételi aláírással. Ez a 12.6.6. pont szerinti kötelező nyilvántartás.

A rendszereket a be- és kiléptetési ellenőrzőlista köti össze. A belépéskor kitöltött lista rögzíti, mely hitelesítő eszközöket adták ki, a kilépéskor kitöltött lista pedig tételesen igazolja a visszavonást és a visszavételt. Ezt a dokumentumot kéri az auditor a 14.5. pont ellenőrzésekor, ezért a kilépő munkatárs utolsó munkanapján kell elkészülnie, nem utólag.

Végül a felülvizsgálat: a nyilvántartást a Szervezet által meghatározott gyakorisággal, legalább évente, valamint minden jelentős szervezeti változáskor össze kell vetni a valósággal (kinél van ténylegesen token, mely szolgáltatásfiókok élnek, mely tanúsítványok érvényesek), és az eltéréseket dokumentáltan rendezni kell. A felülvizsgálatot célszerű a fiókok rendszeres ellenőrzésével egy időben elvégezni.

3.3 A javasolt eljárás

A hitelesítő eszközök kezelését célszerű az alábbi lépésekben kialakítani:

- a) Szabályozás, az azonosítási és hitelesítési szabályzat és eljárásrend kiegészítése a hitelesítő eszközök típusaival, a kiadás, a csere és a visszavonás eljárásával, a nyilvántartás forrásainak és felelősenek kijelölésével.
- b) Felmérés, a Szervezetnél használt valamennyi hitelesítőeszköz-típus azonosítása, ideértve a szolgáltatásfiókokat, az API-kulcsokat, a tanúsítványokat és a fizikai belépőeszközöket, a meglévő nyilvántartások hiányainak feltárása.
- c) Nyilvántartás, a fenti adattartalom szerinti nyilvántartás felállítása a kijelölt forrásrendszerekben, a titkok kizárásával és a hozzáférés korlátozásával.
- d) Kiadási eljárás, az identitás ellenőrzésének, az átvétel dokumentálásának és a kezdeti tartalom cseréjének beépítése a beléptetési folyamatba, a közreműködői szerződések kiegészítése a személyi változások bejelentésével.
- e) Visszavonási eljárás, a kiléptetési ellenőrzőlista bevezetése, az elveszett vagy kompromittált eszközök azonnali letiltása, a visszavonás és a selejtezés dokumentálása.
- f) Felülvizsgálat, a nyilvántartás rendszeres egyeztetése a valósággal, az eredmény rögzítése, a kiberbiztonsági audithoz szükséges bizonyítékok megőrzése.

4. VÁLASZ ÉS RÉSZLETES INDOKOLÁS

4.1 A vizsgálat kiindulópontjai

Az állásfoglalás abból indul ki, hogy a Szervezet a Kiberbiztonsági tv. 1. § (1) bekezdés d) pontja alá tartozik, és kiberbiztonsági felügyeletét a Szabályozott Tevékenységek Felügyeleti Hatósága (SZTFH) látja el. A válasz lényege a többi szervezettípusra is irányadó, az 1. § (1) bekezdés a)-c) és f) pontja alá tartozó szervezetek eltéréseit »A közsférába tartozó szervezetek« című fejezet foglalja össze.

A kérdés a Szervezet vezetőjének két törvényi feladatához kapcsolódik:

- az elektronikus információs rendszerek (EIR) védelmével kapcsolatos szerepkörök, felelősök és feladatok meghatározásához¹,
- valamint a felhasználókra és az elektronikus információbiztonsági követelményekre vonatkozó információbiztonsági szabályzat kiadásához.²

A részletes követelményeket a 7/2024. (VI. 24.) MK rendelet 2. mellékletének 8. (Azonosítás és hitelesítés), 12. (Fizikai és környezeti védelem) és 14. (Személyi biztonság) követelménycsoportja tartalmazza.

A törvény a védelmet az adatkezelésre használt eszközök, az eljárások és az ezeket kezelő személyek együttesére írja elő.³ A hitelesítő eszköz védelmének során három tényezőt kell figyelembe vennünk:

- fizikai vagy logikai eszköz,
- amelyet egy eljárás szerint adnak ki és vonnak vissza,
- amelyet egy személy birtokol.

A nyilvántartás az a dokumentum, amely a hármat összeköti.

4.2 A hitelesítő eszköz fogalma

4.2.1 A rendelet nem ad meghatározást, a fogalom a NIST katalógusból ered

A 7/2024. (VI. 24.) MK rendelet sem a normaszövegben, sem a mellékleteiben nem definiálja a hitelesítő eszközt. A fogalmat a 2. melléklet több követelménye használja, a legrészletesebben a 8.21. pont, amelynek címe „A hitelesítésre szolgáló eszközök kezelése”. A Nemzeti Kiberbiztonsági Intézet alkalmazási útmutatója szerint a rendelet védelmi intézkedései a NIST SP 800-53 ötödik kiadásának kontrollkatalógusára épülnek.⁴ A 8.21. pont a NIST katalógus IA-5 (Authenticator Management) kontrolljának magyar megfelelője, a kilenc alpont sorrendben követi az IA-5 a)-i) pontjait. A magyar „hitelesítő eszköz” tehát az angol „authenticator” fordítása.

¹ Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv)

² 2024. évi LXIX. tv. 23. § (1) bekezdés b) pont

³ 2024. évi LXIX. tv. 6. § (3) bekezdés 2. pont

⁴ 2024. évi LXIX. tv. 6. § (3) bekezdés 7. pont

A NIST meghatározása szerint az authenticator az, amit a hitelesítést kérő fél birtokol és az ellenőrzése alatt tart (jellemzően egy kriptográfiai modul vagy egy jelszó), és amelyet az identitásának hitelesítésére használ.⁵ Az IA-5 kontroll magyarázata példaként a jelszavakat, a kriptográfiai eszközöket, a biometrikus jellemzőket, a tanúsítványokat, az egyszer használatos jelszót előállító eszközöket és az azonosító kártyákat sorolja fel.⁶

Két dolog következik ebből. A hitelesítő eszköz nem feltétlenül tárgy, a jelszó és a tanúsítvány ugyanúgy hitelesítő eszköz, mint a hardveres token. A magyar „eszköz” szó félrevezető lehet, a rendelet azonban a tágabb jelentést használja, hiszen a 8.21.2. pont a hitelesítő eszköz „kezdeti tartalmáról”, a 8.21.5. pont annak első használat előtti megváltoztatásáról beszél, ami hardverre nem, jelszóra viszont értelmezhető. A másik következmény, hogy a hitelesítő eszköz nem csak személyhez tartozhat, a 8.21.1. pont szerint hitelesítő eszközt egyén, csoport, szerepkör, szolgáltatás vagy eszköz kaphat. A szolgáltatásfiók jelszava, az alkalmazások közötti kommunikációt védő API-kulcs és a szerver tanúsítványához tartozó privát kulcs tehát ugyanúgy a rendelet hatálya alá tartozik, mint a munkatársak bejelentkezési jelszava.

4.2.2 Példák a hitelesítő eszközökre

A rendelet szövegéből és a NIST forrásból a gyakorlatban a következő csoportok állíthatók össze.

- Tudásalapú hitelesítők, úgymint a jelszó, jelmondat, a PIN-kód, a biztonsági kérdésre adott válasz. Ezekre a 8.22. pont külön követelményeket ír elő.
- Birtoklásalapú fizikai eszközök, a hardveres OTP-token, a FIDO2 vagy más szabvány szerinti biztonsági kulcs, az intelligens kártya, a tanúsítványt hordozó kártya vagy USB-eszköz. A rendelet a 8.6. pontban kifejezetten említi a rendszertől különálló eszközt mint a többtényezős hitelesítés egyik tényezőjét.
- Birtoklásalapú szoftveres eszközök, ilyen a mobiltelefonra telepített hitelesítő alkalmazás (egyszer használatos kódot előállító vagy push-értesítéssel jóváhagyó alkalmazás), valamint az SMS-ben vagy e-mailben érkező kódok fogadására szolgáló csatorna.
- Kriptográfiai hitelesítők, mint a felhasználói és az eszköztanúsítvány a hozzá tartozó privát kulccsal, az SSH-kulcs, az API-kulcs, a hozzáférési token, a szolgáltatásfiók jelszava vagy titka, az alkalmazásba beágyazott hitelesítő adat. Ezekre a 8.23. pont nyilvános kulcsú hitelesítési követelményei⁷, valamint a kriptográfiai kulcsok kezelésére vonatkozó 17.49. pont vonatkozik.⁸
- Biometrikus hitelesítők, ilyen az ujjlenyomat, az arckép, az írisz. A rendelet ezekre a 8.30. és a 8.34. pontban opcionális követelményeket fogalmaz meg. Különleges személyes adatról van szó, ezért a nyilvántartás soha nem tartalmazhatja magát a

⁵ 2024. évi LXIX. tv. 5. § (2) bekezdés

⁶ Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet: Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója, Előkészületek, 1.0 verzió (2024. augusztus). Elérhető az NKI honlapján.

⁷ NIST SP 800-53 Rev. 5, Appendix A (Glossary), „authenticator”: „Something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant’s identity.”

⁸ NIST SP 800-53 Rev. 5, IA-5 Authenticator Management, Discussion: „Authenticators include passwords, cryptographic devices, biometrics, certificates, one-time password devices, and ID badges.”

biometrikus mintát, csak azt, hogy az adott felhasználónál biometrikus hitelesítés van beállítva.

- Fizikai belépést biztosító hitelesítők, a kitűző, az azonosító kártya, a belépőkártya, a hagyományos és az elektronikus kulcs, a hozzáférési kód. Ezeket a rendelet a fizikai védelem körében nevesíti:

12.2. A szervezet

[...]

12.2.2. Belépési jogosultságot igazoló dokumentumokat, hitelesítő eszközöket (például: kitűzők, azonosító kártyák, intelligens kártyák) bocsát ki a belépni szándékozó részére. [7/2024. (VI. 24.) MK rendelet 2. melléklet 12.2. pont] (A, J, M)

Ez az egyetlen hely, ahol a rendelet példákkal világítja meg a fogalmat. A példák a fizikai belépéshez kötődnek, a 8.21. pont szövegösszefüggése alapján azonban a fogalom a logikai hozzáférés hitelesítőire ugyanúgy kiterjed.

4.2.3 Elhatárolások: mi az, ami nem minősül hitelesítő eszköznek?

A nyilvántartás felépítéséhez három elhatárolás fontos.

Az azonosító nem hitelesítő eszköz. A felhasználónév, az e-mail-cím, a dolgozói szám, az eszköz hálózati neve azonosításra szolgál, és a rendelet külön, a 8.14. pont alatt rendelkezik a kezeléséről. Az azonosító nem titkos, a hitelesítő eszköz tartalma viszont az. Ugyanahhoz a felhasználóhoz egy azonosító és több hitelesítő eszköz tartozhat.

A fiók nem hitelesítő eszköz. A fiókok kezelését a 2.2. pont szabályozza, a nyilvántartás ott a fiókokra, a jogosultságokra és a fiókokhoz tartozó jellemzőkre vonatkozik. A hitelesítő eszköz a fiókhoz tartozó belépési „kulcs”, nem maga a fiók. A két nyilvántartás összefügg, de nem azonos: egy közös használatú fiók esetén például egyetlen fiókhoz több személynél lévő hitelesítő eszköz tartozik, és éppen ezért írja elő a rendelet a hitelesítési adatok megváltoztatását, amikor a csoportból valaki kikerül.

A hitelesítést végző rendszerelem nem hitelesítő eszköz. A címtárszerver, az identitáskezelő szolgáltatás, a beléptető rendszer vezérlője a hitelesítés infrastruktúrája, amely a rendszerelem-leltár tárgya. A hardveres token viszont egyszerre rendszerelem és hitelesítő eszköz, ezért mindkét nyilvántartásban meg kell jelennie, vagy a kettőt célszerű összekapcsolni.

4.3 A hitelesítő eszközök kiadására vonatkozó előírások

A kiadás szabályait a 8.21. pont első öt alpontja tartalmazza, amelyek minden biztonsági osztályban kötelezők:

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. [7/2024. (VI. 24.) MK rendelet 2. melléklet 8.21. pont] (A, J, M)

Az identitás ellenőrzése (8.21.1.) azt jelenti, hogy a hitelesítő eszközt nem lehet „ismeretlennek” kiadni, az átvevőt a kiadás előtt azonosítani kell, és a kiadás tényét hozzá kell kötni. A gyakorlatban ez átvételi elismervényt, a beléptetési folyamatban dokumentált átadást vagy az identitáskezelő rendszer naplóját jelenti. A kezdeti tartalom meghatározása és első használat előtti megváltoztatása (8.21.2. és 8.21.5.) az ideiglenes jelszó cseréje, a token aktiválása és a gyári PIN-kód lecserélése. Az erősség követelménye (8.21.3.) azt kívánja meg, hogy a hitelesítő eszköz típusa a védett rendszer biztonsági osztályához igazodjon. Ugyanezt fogalmazza meg a jelentős és a magas osztályban kötelező 8.25. pont is:

8.25. A szervezet a hitelesítő eszközöket az információk biztonsági besorolásának megfelelő védelemmel látja el, amelyekhez a hitelesítő eszköz a hozzáférést biztosítja. [7/2024. (VI. 24.) MK rendelet 2. melléklet 8.25. pont] (J, M)

A 8.21.4. pont az, amely a nyilvántartás követelményét megalapozza. Az adminisztratív eljárás az alábbi élethelyzetre terjed ki:

- a kezdeti kiosztásra,
- az elvesztésre, kompromittálódásra vagy sérülésre,
- valamint a visszavonásra.

A második és a harmadik nem hajtható végre anélkül, hogy a Szervezet tudná, mit adott ki és kinek. Ha egy munkatárs elveszíti a hardveres tokenjét, a Szervezetnek azonnal meg kell tudnia állapítani, melyik token az, mely rendszerekhez ad hozzáférést, és le kell tiltania. Ha egy szolgáltató szerződése megszűnik, vissza kell vonni az általa használt API-kulcsokat és tanúsítványokat. Ez csak akkor kérhető számon, ha a kiadásról nyilvántartás készült.

A rendelet opcionális követelményként lehetővé teszi, hogy a Szervezet a különleges hitelesítő eszközök kiadását személyes jelenléthez vagy megbízható külső fél közreműködéséhez és meghatározott személyek jóváhagyásához kösse. Ugyancsak opcionális, de jó gyakorlat, hogy a rendszerelemek fejlesztői és telepítői az alapértelmezett hitelesítő adatokat az átadás előtt megváltoztassák, és hogy az alkalmazásokba ne legyenek beépítve titkosítatlan, statikus hitelesítők.

4.4 A hitelesítő eszközök nyilvántartására vonatkozó előírások

4.4.1 A nyilvántartást a rendelet közvetve, de egyértelműen elvárja

A 7/2024. (VI. 24.) MK rendelet nem tartalmaz olyan követelményt, amely szó szerint „hitelesítőeszköz-nyilvántartás” vezetését írná elő. Álláspontunk szerint a nyilvántartási kötelezettség ettől függetlenül fennáll, mert több, minden biztonsági osztályban kötelező követelmény teljesítése csak nyilvántartás mellett igazolható.

Az első ilyen a fenti 8.21.4. pont szerinti adminisztratív eljárás. A második a személyi biztonság körében a munkaviszony megszűnésekor teljesítendő kötelezettség:

14.5. A szervezet az egyéni munkaviszony megszűnésekor:

14.5.1. Meghatározott időn belül letiltja a rendszerhez való hozzáférést.

14.5.2. Megszünteti vagy visszavonja az adott személyhez kapcsolódó összes hitelesítő eszközt és jogosultságot.

[...]

14.5.4. Visszaveszi az összes biztonsági szempontból releváns szervezeti EIR-hez kapcsolódó biztonsági eszközöket. [7/2024. (VI. 24.) MK rendelet 2. melléklet 14.5. pont] (A, J, M)

Az „összes” hitelesítő eszköz visszavonása és az „összes” biztonsági eszköz visszavétele csak akkor igazolható, ha a Szervezet személyenként tudja, mi van kiadva. Az auditor ezt jellemzően úgy ellenőrzi, hogy kiválaszt néhány, az elmúlt időszakban kilépett munkatársat, és kéri annak igazolását, hogy minden hitelesítő eszközüket visszavonták. Nyilvántartás nélkül ez az igazolás nem adható meg. Ugyanez vonatkozik az áthelyezésre és a munkakörváltásra, amikor a logikai és a fizikai hozzáférési jogosultságokat felül kell vizsgálni.⁹

A harmadik a külső személyekre vonatkozó követelmény:

14.11. A szervezet:

[...]

14.11.4. Megköveteli a külső szolgáltatóktól, hogy a meghatározott időn belül értesítsék a meghatározott személyeket vagy szerepköröket minden olyan külső személy áthelyezéséről vagy kilépéséről, akik szervezeti hitelesítő eszközzel, belépőkártyával vagy rendszerjogosultsággal rendelkeztek. [7/2024. (VI. 24.) MK rendelet 2. melléklet 14.11. pont] (A, J, M)

Ez a pont azt is megmutatja, hogy a nyilvántartásnak a Szervezet saját munkatársain túl a közreműködők és a külső üzemeltetők személyzetére is ki kell terjednie. A Kiberbiztonsági tv. a közreműködők igénybevétele esetén a kiberbiztonsági követelmények szerződéses érvényesítését írja elő; a hitelesítő eszközök kiadásának, visszaadásának és a személyi változások bejelentésének szabályai ennek a szerződéses kötelelemnek a részét képezik.

A negyedik a közös használatú hitelesítő eszközökre vonatkozik. Magas osztályban a Szervezetnek a felhasználókat egyénileg azonosítania kell, mielőtt a közös használatú fiókhoz vagy hitelesítő eszközhez hozzáférést ad, ehhez pedig vezetnie kell, kik jogosultak a közös eszköz használatára. A közös fiókok hitelesítő eszközeinek tagváltáskor történő megváltoztatása minden osztályban kötelező, ehhez szintén tudni kell, kik a tagok.

⁹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 8.22. pont (A, J, M)

4.4.2 A fizikai belépést biztosító eszközök kifejezett nyilvántartása

A fizikai védelem körében a rendelet már nem közvetve, hanem kifejezetten írja elő a nyilvántartást:

12.6. A szervezet:

[...]

12.6.5. Megóvja a kulcsokat, hozzáférési kódokat és az egyéb fizikai hozzáférést biztosító eszközöket.

12.6.6. Nyilvántartást vezet a fizikai belépést ellenőrző eszközökről, és meghatározott gyakorisággal frissíti azt.

12.6.7. Meghatározott rendszerességgel megváltoztatja a hozzáférési kódokat és kulcsokat, illetve ha a kulcs elveszik, a hozzáférési kód kompromittálódik, vagy az azokkal rendelkező személy elveszíti a belépési jogosultságát. [7/2024. (VI. 24.) MK rendelet 2. melléklet 12.6. pont] (A, J, M)

A belépőkártyákról, a kulcsokról és a hozzáférési kódokról tehát minden biztonsági osztályban nyilvántartást kell vezetni, azt a Szervezet által meghatározott gyakorisággal frissíteni kell, és ez a nyilvántartás az alapja annak, hogy elvesztés vagy jogosultságvesztés esetén a kódot vagy a kulcsot le lehessen cserélni. Ehhez kapcsolódik a belépésre jogosultak listájának vezetése, felülvizsgálata és a már nem jogosultak törlése is.

Álláspontunk szerint nincs ésszerű indoka annak, hogy a logikai hozzáférés hitelesítő eszközeit a Szervezet kevésbé szigorúan tartsa nyilván, mint a fizikai belépőkártyákat. Egy privilegizált rendszergazdai fiókhoz tartozó hardveres kulcs jellemzően nagyobb kockázatot hordoz, mint egy irodai belépőkártya. A rendelet eltérő szóhasználata a NIST katalógus szerkezetét követi, amely a fizikai hozzáférést biztosító eszközöknél kifejezetten leltárt, a hitelesítőknél adminisztratív eljárást ír elő.

4.4.3 A rendszerelem-leltár és a kriptográfiai kulcsok

A fizikai hitelesítő eszközök (tokenek, intelligens kártyák, olvasók) rendszerelemek is. A rendszerelem-leltárnak minden osztályban pontosan tükröznie kell az EIR-t, és tartalmaznia kell a rendszeren belül található összes elemet, jelentős és magas osztályban pedig azt minden telepítéskor, eltávolításkor és frissítéskor frissíteni kell. A hardveres tokenek beszerzése, kiosztása, visszavétele és selejtezése ezért a leltárban is nyomon követendő.

A tanúsítványokra és a kulcsokra a kriptográfiai kulcskezelés szabályai vonatkoznak:

17.49. A szervezet előállítja és kezeli a kriptográfiai kulcsokat a szervezet által meghatározott előállítási, szétosztási, tárolási, hozzáférési és megsemmisítési követelményekkel összhangban. [7/2024. (VI. 24.) MK rendelet 2. melléklet 17.49. pont] (A, J, M)

A szétosztás, a hozzáférés és a megsemmisítés követelményeinek betartása a kulcsok nyilvántartása nélkül nem lehetséges: tudni kell, hol milyen kulcs van használatban, ki fér hozzá, mikor jár le, és mikor semmisítették meg. Jelentős és magas osztályban a nyilvános kulcsú

hitelesítésnél emellett biztosítani kell a privát kulcshoz való jogosult hozzáférést, és össze kell kapcsolni a hitelesített azonosítót az egyén vagy a csoport fiókjával. A tanúsítvány- és kulcsnyilvántartás így a hitelesítőeszköz-nyilvántartás része.

4.4.4 A nyilvántartás védelme: mi az, amit a nyilvántartás nem tartalmazhat?

A nyilvántartás felépítésénél a legfontosabb korlátot a 8.21. pont második fele adja:

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

[...]

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. [7/2024. (VI. 24.) MK rendelet 2. melléklet 8.21. pont] (A, J, M)

A hitelesítő eszköz „tartalma” maga a titok, a jelszó, a privát kulcs, a token magja, az API-kulcs értéke. A nyilvántartás célja az elszámoltathatóság, nem a titok őrzése. Egy táblázat, amely a felhasználók jelszavait vagy az API-kulcsok értékét tartalmazza, nem nyilvántartás, hanem a 8.21.7. pont megsértése, és egyben a Szervezet legértékesebb támadási célpontja. A nyilvántartásban ezért kizárólag a hitelesítő eszköz metaadatai szerepelhetnek:

- típusa, azonosítója, birtokosa,
- a fiók vagy rendszer, amelyhez tartozik,
- a kiadás és a visszavonás időpontja,
- valamint a státusz.

Ha a titkot magát is központilag kell tárolni (például szolgáltatásfiókok jelszavát vagy a vészhelyzeti hozzáférés adatait), arra titkosított, hozzáférés-vezérelt és naplózott titoktár szolgál. A jelszavakat a rendelet szerint egyébként is csak szózott kulcsszármaztatási függvénnyel, hash formában szabad tárolni.

A nyilvántartás maga is védendő adat. A benne szereplő információ (ki, mihez, milyen eszközzel fér hozzá) egy támadó számára térkép, ezért a hozzáférést a legkisebb jogosultság elve szerint kell korlátozni. A személyes adatokat a munkaviszony megszűnése után csak a szükséges ideig, a kiberbiztonsági audit bizonyítási igényére tekintettel legalább a következő auditig kell megőrizni.

4.5 Az életciklus többi lépése, a csere és a visszavonás

A 8.21.6. pont a hitelesítő eszközök tartalmának meghatározott gyakoriságú vagy eseményhez kötött cseréjét írja elő. A gyakoriságot és az eseményeket a Szervezetnek kell meghatároznia az azonosítási és hitelesítési szabályzatában. Jelszónál a mai gyakorlat az eseményvezérelt csere (kompromittálódás gyanúja, fiók-visszaállítás, kilépés a csoportból), amit a rendelet is tükröz, amikor fiók-visszaállítás esetén a jelszó azonnali megváltoztatását követeli meg. Tanúsítványnál a lejárat, tokennél az élettartam és az elvesztés, API-kulcsnál a szolgáltatóváltás és a kompromittálódás a jellemző esemény. A nyilvántartás ezeknek az eseményeknek a naplója: rögzíti, mikor cserélték az eszközt és miért.

A visszavonás (8.21.4. és 14.5.2.) a folyamat vége. A rendelet „megszünteti vagy visszavonja” fordulata a logikai hitelesítőknél letiltást vagy törlést, a fizikai eszközöknél visszavételt és letiltást jelent. A visszavont eszköz nem tűnhet el a nyilvántartásból: a visszavonás tényét, idejét és a visszavevő személyt rögzíteni kell, mert a kiberbiztonsági audit során ezek a bejegyzések igazolják a 14.5. pont teljesítését. A visszavont fizikai eszközök selejtezését is dokumentálni kell, ahogyan a rendszerelemek selejtezésénél általában.

4.6 A közzsférába tartozó szervezetek

A 418/2024. (XII. 23.) Korm. rendelet a hitelesítő eszközök kiadására és nyilvántartására külön szabályt nem tartalmaz, ezért a fentiek a Kiberbiztonsági tv. 1. § (1) bekezdés a)-c) és f) pontja alá tartozó szervezetekre is változatlanul irányadók. Két eltérés érdemel figyelmet. Ezek a szervezetek az információbiztonsági szabályzatukat, amelynek az azonosítási és hitelesítési szabályzat is része, a törvény hatálya alá kerülést követő 180 napon belül megküldik a nemzeti kiberbiztonsági hatóságnak.¹⁰ Az elektronikus információs rendszer biztonságáért felelős személy pedig folyamatos és tervezett ellenőrzésekkel vizsgálja a belső normák megvalósulását, és megállapításait írásban rögzíti a szervezet vezetője számára.¹¹ A hitelesítőeszköz-nyilvántartás ezeknél a szervezeteknél így hatósági nyilvántartásba vett szabályzaton alapul, és a belső ellenőrzés tárgya.

5. FELHASZNÁLT FORRÁSOK

- Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (NIS 2 irányelv)
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről
- 418/2024. (XII. 23.) Korm. rendelet Magyarország kiberbiztonságáról szóló törvény végrehajtásáról
- NBSZ Nemzeti Kiberbiztonsági Intézet: Elektronikus Információs Rendszerek és Szervezetek Kiberbiztonsági Követelménykatalógusának Alkalmazási Útmutatója, Előkészületek (1.0 verzió, 2024)

¹⁰ 7/2024. (VI. 24.) MK rendelet 2. melléklet 8.6. pont (O)

¹¹ 7/2024. (VI. 24.) MK rendelet 2. melléklet 8.23. pont (J, M)

- NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations (IA-5 Authenticator Management, PE-3 Physical Access Control, Appendix A Glossary)