

MENNYIRE ELLENÁLLÓ A RENDSZERÜNK? Hogyan határozzuk meg, vezessük be és tartjuk fenn rendszereink biztonsági alapkonzfigurációját? Hardening feladatok

VFP2 KiberVéd - NIS2 Audit felkészítés szakértői
állásfoglalás 2026/59

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.29	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A „hardening”, vagyis a rendszerek biztonsági megerősítése (keményítése) egyszerű gondolatra épül. A gyári alapállapotból olyan dokumentált és ellenőrzött konfigurációt kell kialakítani, amelyben csak az üzletileg szükséges funkciók, szolgáltatások és hozzáférések működnek, azok is az elvárt biztonságos beállításokkal. A sikeres támadások jelentős része ugyanis nem ismeretlen, „zero-day” hibákra épül, hanem régóta ismert, jól dokumentált gyenge beállításokra, például alapértelmezett jelszavakra, feleslegesen futó szolgáltatásokra, elavult protokollokra vagy túlzott jogosultságokra.

A hardening ezért nem egyszeri telepítési feladat, hanem a konfiguráció- és változáskezelés része. A megfelelő állapotot meg kell határozni és be kell vezetni, azután rendszeresen mérni kell, az eltéréseket pedig kockázatalapon kell kezelni.

A tartós eredményt nem egy egyszeri, mégoly alapos beállítás hozza meg. A szervezetnek elismert referenciára épülő, saját környezetére szabott és verziózott biztonsági alapkonfigurációval kell rendelkeznie, amelynek betartását lehetőleg automatizáltan kényszeríti ki, és rendszeresen méri. Az eltéréseket, köztük a tudatosan vállalt kivételeket is, a kockázatkezelés részeként kell kezelnie.

A következő auditon az a szervezet lesz jó helyzetben, amely bármelyik rendszeréről meg tudja mutatni, milyen alapkonfiguráció vonatkozik rá, hogyan vezették be, mikor mérték utoljára a megfelelést, milyen eltéréseket találtak, és azokat hogyan kezelték.

Az állásfoglalás a követelmények értelmezése mellett három, a hazai NIS2-érintett szervezeteknél gyakori rendszer példáján mutatja be, mit érdemes a gyakorlatban megvalósítani, és mivel lehet ezt az auditon hitelesen alátámasztani. A vizsgált rendszerek a következők.

- Microsoft Windows Server és Active Directory
- Távoli hozzáférést biztosító VPN
- Nextcloud fájlmeosztó

2. A VIZSGÁLANDÓ KÉRDÉS

Milyen jogszabályi követelmények vonatkoznak a rendszerek biztonsági alapkonfigurációjára (hardening), és hogyan kell ezeket a belső szabályozásban rögzíteni?

Milyen területekre kell kiterjednie a hardeningnek?

Hogyan tartható fenn a biztonságos állapot a rendszer életciklusa során, és mivel igazolható a megfelelés az auditon?

Hogyan valósítható meg mindez a gyakorlatban olyan tipikus rendszereknél, mint a Microsoft Windows Server és az Active Directory, a távoli hozzáférést biztosító VPN vagy a Nextcloud fájlmeosztó?

3. VÁLASZ

3.1 A hardening jogszabályi alapja, szabályozása és a biztonsági alapkonfiguráció

A 7/2024. (VI. 24.) MK rendelet szerint a szervezetnek ki kell alakítania, dokumentálnia és karban kell tartania az elektronikus információs rendszer (EIR) alapkonfigurációját. Az alapkonfigurációt meghatározott időközönként, a meghatározott körülmények által indokolt esetekben, valamint az EIR vagy elemeinek telepítésekor és frissítésekor felül kell vizsgálni, és szükség szerint frissíteni.

Alapkonfiguráció 6.2. A szervezet:

6.2.1. Kifejleszti, dokumentálja és karbantartja az EIR alapkonfigurációját.

6.2.2. Elvégzi az EIR alapkonfigurációjának felülvizsgálatát és frissítését:

6.2.2.1. meghatározott időközönként;

6.2.2.2. ha azt a meghatározott körülmények indokolják, vagy

6.2.2.3. az EIR vagy rendszerelemek telepítésekor vagy frissítésekor.

7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás

követelményeiről, valamint az egyes biztonsági osztályok esetében

alkalmazandó konkrét védelmi intézkedésekről, 2. melléklet 6.2. pont

(<https://njt.hu/jogszabaly/2024-7-20-7G>)

Az alapkonfiguráció tartalmát a konfigurációs beállításokra vonatkozó követelmény határozza meg. Eszerint a beállításoknak az üzemeltetési követelményekkel összhangban lévő „legkorlátozottabb üzemmódot” kell képviselniük, az ettől való eltéréseket pedig azonosítani, dokumentálni és jóváhagyni kell. Ez a hardening közvetlen jogszabályi alapja.

Konfigurációs beállítások 6.23. A szervezet:

6.23.1. Kialakítja és dokumentálja a rendszerelemekben alkalmazott egységes biztonsági konfigurációs beállításokat, amelyek az üzemeltetési követelményekkel összhangban lévő legkorlátozottabb üzemmódot képviselik.

6.23.2. Elvégzi a konfigurációs beállításokat az EIR valamennyi elemében.

6.23.3. Azonosítja, dokumentálja és elfogadja a meghatározott rendszerelemek konfigurációs beállításában a működési követelmények által meghatározott konfigurációs beállításoktól való eltéréseket.

6.23.4. Figyelemmel kíséri és ellenőrzi a konfigurációs beállítások változtatásait a szervezeti szabályzatokkal és eljárásokkal összhangban.

7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás

követelményeiről, valamint az egyes biztonsági osztályok esetében

alkalmazandó konkrét védelmi intézkedésekről, 2. melléklet 6.23. pont

(<https://njt.hu/jogszabaly/2024-7-20-7G>)

A hardening elemei ezen túl az azonosítás és hitelesítés, a hozzáférés-felügyelet, a naplózás és elszámoltathatóság, valamint a rendszer- és kommunikációvédelem intézkedéscsaládjában is megjelennek (lásd a 3.2. pontot).

Szabályozási szintek. A hardening a szervezet szabályozási rendjében két szinten jelenik meg.

- Átfogó szinten (informatikai biztonsági szabályzat, konfigurációkezelési eljárásrend) azt kell rögzíteni, hogy minden EIR-elemre kötelező biztonsági alapkonfigurációt alkalmazni. Itt kell meghatározni azt is, ki készíti el és ki hagyja jóvá az alapkonfigurációt, milyen elismert referenciára épül, milyen gyakran és milyen módszerrel ellenőrzik a megfelelést, és hogyan kell kezelni az eltéréseket.
- Rendszerszinten (a rendszerbiztonsági tervben, az üzemeltetési leírásban, illetve az ezekhez tartozó platformonkénti hardening leírásban) a konkrét beállításokat, azok indoklását és az elfogadott kivételeket kell rögzíteni.

Gyakori auditmegállapítás, hogy a szabályzat mindössze annyit rögzít, hogy „a rendszereken a gyártói ajánlásoknak megfelelő hardeninget kell végrehajtani”. Ez a megfogalmazás nem ellenőrizhető, így sem a szervezet, sem az auditor nem tudja megállapítani, hogy teljesül-e. Jó gyakorlat, ha a szabályozás platformonként, például a rendszerbiztonsági tervben, megnevezi a referencia-alapkonfigurációt és annak verzióját (például „a Windows Server 2025 kiszolgálókra a Microsoft Windows Server 2025 Security Baseline vonatkozik, a szervezeti eltéréseket az 5. számú melléklet tartalmazza”).

A 7/2024. (VI. 24.) MK rendelet szemléletével összhangban a hardening szintjét célszerű a biztonsági osztályhoz és az üzleti kritikussághoz igazítani. Nem szükséges, és sokszor nem is ésszerű, minden rendszerre a legszigorúbb profilt alkalmazni. Az internet felől elérhető, illetve a jogosultságkezelést kiszolgáló rendszereknél (például a címtárnál, a VPN-nél és a határvédelmi eszközöknél) azonban általában a szigorúbb szint indokolt.

Elismert referenciák. A biztonsági alapkonfigurációt a szervezetnek nem kell, és nem is érdemes, nulláról felépítenie. Nemzetközileg elismert, rendszeresen karbantartott referenciák állnak rendelkezésre, például a CIS Benchmarks (Center for Internet Security), a Microsoft Security Baselines (Security Compliance Toolkit), a DISA STIG-ek, a német BSI IT-Grundschutz moduljai, valamint a gyártók saját hardening útmutatói. Ezek adják a kiindulópontot, amelyet a szervezet a saját környezetére szab. A leggyakrabban használt források elérhetőségét a dokumentum melléklete tartalmazza.

A testreszabás a gyakorlatban azt jelenti, hogy a szervezet kiválasztja a referenciát és annak profilját (például CIS Level 1 vagy Level 2), majd kivételként rögzíti azokat a beállításokat, amelyeket üzleti vagy technikai okból nem tud alkalmazni. Minden kivételt dokumentáltan indokolni kell, és ha a kivétel kezelendő kockázatot hordoz, kiegészítő védelmi intézkedést is érdemes bevezetni. A cél tehát nem a 100%-os „benchmark-megfelelés”, hanem az, hogy minden eltérés tudatos, jóváhagyott és visszakereshető döntés legyen.

Célszerű a biztonsági alapkonfigurációt (angolul baseline) verziózott dokumentumként kezelni, és lehetőség szerint gépi formában is fenntartani, például csoportházirend-objektumok mentéseként, Intune-konfigurációs profilként, Ansible playbookként, mester lemezképként

vagy sablonként. Az így kezelt konfiguráció („configuration as code”) egyszerre biztosítja az egységes bevezetést és a változások követhetőségét, és auditbizonyítékként is szolgál.

3.2 A hardening tartalmi elemei

A hardening a gyakorlatban három, egymással szorosan összefüggő területet fed le. Ezek a támadási felület csökkentése (legsűkebb funkcionalitás), az identitások és az adminisztratív hozzáférések védelme, valamint a biztonsági események nyomon követhetősége (naplózás és időszinkron).

Legsűkebb funkcionalitás. Az elv szerint egy rendszeren csak az a szerepkör, szolgáltatás, alkalmazás és hálózati kapcsolat engedélyezett, amelyre az adott üzleti funkcióhoz ténylegesen szükség van. Ez a hardening talán leghatékonyabb eleme, mert közvetlenül csökkenti a támadási felületet. Amit nem futtatunk, azt nem kell frissíteni és monitorozni, és kihasználni sem lehet.

Legsűkebb funkcionalitás 6.26. A szervezet:

6.26.1. Az EIR-t úgy konfigurálja, hogy az csak az ügy- és üzletmenet szempontjából szükséges szolgáltatásokat nyújtsa.

6.26.2. Meghatározza a tiltott vagy korlátozott funkciókat, portokat, protokollokat, szoftvereket és szolgáltatásokat.

7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás

követelményeiről, valamint az egyes biztonsági osztályok esetében

alkalmazandó konkrét védelmi intézkedésekről, 2. melléklet 6.26. pont

(<https://njt.hu/jogszabaly/2024-7-20-7G>)

A gyakorlatban ez mindenekelőtt a nem használt szerepkörök, szolgáltatások és szoftverek eltávolítását jelenti. Rendszerenként nyilván kell tartani az engedélyezett portokat és protokollokat (portmátrix, kommunikációs mátrix), és a hálózati tűzfal mellett a gépek saját tűzfalát is használni kell. Tiltani kell az elavult, nem biztonságos protokollokat (például SMBv1, TLS 1.0 és 1.1, NTLMv1, Telnet, titkosítatlan FTP, SNMP v1 és v2c), a kritikus kiszolgálókon pedig, ahol ez arányos, alkalmazásengedélyezési megoldást érdemes bevezetni (például AppLocker vagy App Control for Business, korábbi nevén WDAC).

Fiókok, hitelesítés és adminisztratív hozzáférések. A hardening nemcsak technikai beállítások kérdése, hanem az identitások és a hozzáférések kezeléséé is. Üzembe helyezés előtt az alapértelmezett fiókokat le kell tiltani vagy át kell nevezni, az alapértelmezett jelszavakat pedig kivétel nélkül le kell cserélni. A helyi adminisztrátori jelszavaknak rendszerenként egyedinek kell lenniük. A szolgáltatásfiókokat nyilvántartásba kell venni, és ahol lehet, felügyelt szolgáltatásfiókokkal (például gMSA) kell kiváltani.

Az adminisztratív hozzáféréseknél bevált gyakorlat a felügyeleti felületek elkülönítése (dedikált menedzsmenthálózat, jump host vagy adminisztrátori munkaállomás), a többfaktoros hitelesítés kötelezővé tétele minden távoli és privilegizált hozzáférésnél, valamint a napi munkára és az adminisztrációra használt fiókok szétválasztása. Ezek a beállítások szorosan kapcsolódnak a jogosultságkezelési folyamathoz, ezért érdemes őket azzal együtt szabályozni és felülvizsgálni.

Naplózás és időszinkron. A hardeninghez a naplózás megfelelő beállítása is hozzátartozik. Egy rendszer csak akkor tekinthető megfelelően konfiguráltnak, ha rögzíti a biztonsági szempontból lényeges eseményeket (bejelentkezések, jogosultság- és konfigurációváltozások, adminisztratív tevékenység, folyamatindítások), a naplók mérete és megőrzési ideje elegendő, és a naplókat központi gyűjtőbe (például SIEM-be) továbbítja. Ehhez kapcsolódik a rendszeridő pontos, megbízható időforráshoz való szinkronizálása is, amely nélkül egy incidens kivizsgálásakor az események nem vethetők össze.

Gyakori hiba, hogy a naplózás alapértelmezett beállításokkal fut, és a helyi naplók néhány óra alatt felülíródnak. Az is előfordul, hogy a naplókat ugyan gyűjtik, de éppen azok az eseménykategóriák hiányoznak belőlük, amelyek egy támadás felderítéséhez kellenének.

3.3 A biztonságosan beállított állapot fenntartása és igazolása a rendszer életciklusában

A megerősített állapot idővel „elkopik” (configuration drift). Ennek jellemző okai a hibaelhárítás közben ideiglenesen módosított, majd visszaállítani elfelejtett beállítások, az új szoftverek telepítése, a gyártói frissítések által visszaállított alapértékek, valamint a szabványos folyamaton kívül, kézzel telepített rendszerek. A megerősített állapot ezért csak rendszeres, lehetőleg automatizált méréssel és az eltérések következetes kezelésével tartható fenn.

A megfelelés mérésére számos eszköz áll rendelkezésre, például a CIS-CAT, az OpenSCAP, a Microsoft Policy Analyzer, a sérülékenységszkenner konfigurációs (compliance) auditfunkciói, a végpontvédelmi megoldások konfigurációértékelő moduljai, Linux rendszereken a Lynis, Active Directory környezetben pedig a PingCastle vagy a Purple Knight. Célszerű rögzíteni a mérés gyakoriságát (például negyedévente, valamint minden jelentős változás után), az eredményeket megőrizni, az eltéréseket pedig a sérülékenység-, illetve kockázatkezelési folyamatba továbbítani.

A mérést érdemes mérőszámokkal is összekötni. Ilyen lehet a baseline-megfelelés aránya rendszercsoportonként, a nyitott eltérések száma és kora, a lejárt kivételek száma, valamint a hardening nélkül üzembe helyezett rendszerek száma. Ahol lehetséges, a kikényszerítést is érdemes automatizálni (csoportházirend, Intune, DSC, Ansible). Így az eltérés a következő szinkronizáláskor magától megszűnik, kézi ellenőrzésre pedig csak a kivételeknél van szükség.

A „jelentős” és a „magas” biztonsági osztályba sorolt rendszereknél az alapkonfiguráció automatizált támogatása nem csupán jó gyakorlat, hanem jogszabályi követelmény.

6.3. A szervezet automatizált mechanizmusokat alkalmaz az EIR naprakész, teljes, pontos és állandóan rendelkezésre álló alapkonfigurációjának karbantartására.

*7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről, 2. melléklet 6.3. pont
(<https://njt.hu/jogszabaly/2024-7-20-7G>)*

A hardening követelményeinek a rendszer teljes életciklusán át érvényesülniük kell. Beszerzéskor célszerű előírni, hogy a termék támogassa a biztonságos konfigurációt, legyen

hozzá gyártói hardening útmutató, a gyártó biztosítson biztonsági frissítéseket, és ismert legyen a támogatás megszűnésének időpontja. Üzembe helyezéskor a hardening átadás-átvételi feltétel, vagyis a rendszer csak akkor kerülhet éles üzembe, ha a hardening ellenőrzőlista teljesült, és a megfelelőségi mérés eredményét dokumentálták.

A változáskezelés során a biztonsági hatásvizsgálatnak arra is ki kell terjednie, hogy a változás érinti-e az alapkonzfigurációt. Ha igen, a változás csak jóváhagyással hajtható végre, és ilyenkor vagy a baseline-t kell módosítani, vagy az eltérést dokumentált kivételként kell nyilvántartani.

Biztonsági hatásvizsgálat 6.15. A szervezet még a változtatások bevezetése előtt megvizsgálja az EIR-ben tervezett változtatásoknak az információbiztonsági hatásait.

7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről, 2. melléklet 6.15. pont (<https://njt.hu/jogszabaly/2024-7-20-7G>)

Az életciklus végén a gyártói támogatás megszűnését kell szem előtt tartani. A támogatás nélküli rendszerek biztonsági frissítések hiányában nem tarthatók biztonságos állapotban (a Windows Server 2016 kiterjesztett támogatása például 2027. január 12-én ér véget), ezért ezekhez kivezetési tervet vagy dokumentált kiegészítő védelmi intézkedéseket kell rendelni. A témát részletesen tárgyalja a nem támogatott operációs rendszerek NIS2-kompatibilis használatáról szóló MKIK-állásfoglalás.

Jó auditbizonyítéknak számítanak a verziózott baseline-dokumentumok és a kivételnyilvántartás, a csoportházirend- és konfigurációs riportok, az időbélyeggel ellátott megfelelőségi mérési eredmények, a hardening ellenőrzőlistát tartalmazó átadás-átvételi jegyzőkönyvek, valamint a konfigurációt érintő változások jegyei a hozzájuk tartozó biztonsági hatásvizsgálattal.

Az auditon nem a hardening leírása a legerősebb bizonyíték, hanem két, eltérő időpontban végzett mérés eredménye és a köztük feltárt eltérések dokumentált kezelése. Ez igazolja, hogy a hardening nem egyszeri projekt, hanem működő folyamat.

3.4 Gyakorlati megvalósítás tipikus rendszereken

Az alábbi példák a hazai NIS2-érintett szervezeteknél gyakori rendszerek megerősítésének legfontosabb elemeit mutatják be. A példák nem helyettesítik a teljes referencia-alapkonzfigurációt (például a CIS Benchmarkot), hanem azokat a beállításokat emelik ki, amelyek a gyakorlati tapasztalatok szerint a legnagyobb kockázatcsökkentést hozzák, vagy amelyek hiánya a leggyakoribb auditmegállapítások közé tartozik. A konkrét beállítások bevezetése előtt mindig ellenőrizni kell a referencia aktuális verzióját és a gyártói dokumentációt, a bevezetést pedig a változáskezelési folyamat szerint kell végrehajtani.

3.4.1 Microsoft Windows Server és Active Directory

Az Active Directory a legtöbb szervezetnél a teljes informatikai környezet központja. Aki a címtár felett átveszi az irányítást, gyakorlatilag minden rendszerhez hozzáfér. A zsarolóvírus-támadások jelentős része is a tartományi rendszergazdai jogosultság megszerzésére épül, ezt a

jogosultságot pedig a támadók jellemzően nem szoftverhiba kihasználásával, hanem gyenge beállítások és rosszul kezelt hitelesítő adatok révén szerzik meg. Ezért kiemelt prioritás a Windows kiszolgálók és különösen a tartományvezérlők megfelelő beállítása.

Kiindulópontként a Microsoft Security Baseline tartományba léptetett kiszolgálóra (member server) és tartományvezérlőre vonatkozó profiljai vagy a CIS Microsoft Windows Server Benchmark ajánlott, csoportházirenddel kikényszerítve. A szervezeti eltéréseket (például a régi alkalmazások miatt szükséges protokollokat) kivételként kell nyilvántartani.

A hardening egyik alapja a rendszergazdai jogosultságok szintekre bontása (angolul tiering). Jellemzően három szintet különítenek el. A Tier 0 a tartományvezérlőket és a címtárat kezelő rendszereket, a Tier 1 a kiszolgálókat és az üzleti alkalmazásokat, a Tier 2 a munkaállomásokat és a felhasználói eszközöket foglalja magában. Mindegyik szintet külön rendszergazdai fiókkal kezelik, és csoportházirend tiltja, hogy egy magasabb szintű fiókkal alacsonyabb szintű gépre be lehessen jelentkezni. Így ha a támadó átveszi az irányítást egy munkaállomás felett, onnan nem jut hozzá a tartományi rendszergazda jelszávához vagy más hitelesítő adataihoz. A kiemelt jogosultságú fiókokat érdemes a Protected Users csoportba tenni, a tartományi rendszergazdai csoportokban pedig csak a feltétlenül szükséges fiókokat szabad megtartani.

A bevezetésnél fontos a fokozatosság, mert több beállítás (például az NTLM korlátozása, az LDAP channel binding kikényszerítése vagy az SMB-aláírás kötelezővé tétele) kompatibilitási gondot okozhat régebbi rendszereknél és eszközöknél, például multifunkciós nyomtatóknál vagy régi alkalmazásoknál. Bevált gyakorlat, hogy a beállítást először naplózó (audit) üzemmódban vezetik be, a naplók alapján feltérképezik az érintett rendszereket, majd ütemezetten kikényszerítik. Ez a folyamat maga is kiváló auditbizonyíték.

A kiemelt beállításokat és a hozzájuk kapcsolódó ellenőrzési módszereket az alábbi táblázat foglalja össze.

Terület	Javasolt beállítás / intézkedés	Ellenőrzés, auditbizonyíték
Privilegizált hozzáférés	Adminisztratív rétegzés (Tier 0/1/2); „Deny log on” szabályok; Protected Users csoport; külön adminisztrátori fiókok; minimális Domain Admins és Enterprise Admins tagság; dedikált adminisztrátori munkaállomás (PAW) vagy jump host.	Csoportházirend-riport; privilegizált csoporttagságok listája és felülvizsgálati jegyzőkönyve; PingCastle / Purple Knight riport.
Helyi adminisztrátori fiókok	Windows LAPS bevezetése minden tartományba léptetett kiszolgálón és munkaállomáson (a Windows Server 2016-on és a Windows LAPS-t nem támogató más régebbi rendszereken a korábbi Microsoft LAPS); beépített Administrator fiók letiltása vagy átnevezése.	LAPS-lefedettségriport; jelszóolvasási jogosultságok listája.
Elavult protokollok	SMBv1 eltávolítása; SMB-aláírás kötelezővé tétele; LM és NTLMv1 tiltása, NTLM használatának auditálása és fokozatos korlátozása; LLMNR és NetBIOS over TCP/IP tiltása; WDigest kikapcsolása.	Csoportházirend-riport; NTLM-auditnaplók; sérülékenységszkenner-eredmények.
Címtárprotokollok (LDAP)	LDAP-aláírás és LDAP channel binding kikényszerítése a tartományvezérlőkön (előtte audit üzemmódban).	Tartományvezérlő-naplók (nem aláírt kötésekre utaló események) elemzése; beállítási riport.

Terület	Javasolt beállítás / intézkedés	Ellenőrzés, auditbizonyíték
Hitelesítő adatok védelme	LSA védelem (RunAsPPL); Credential Guard, ahol támogatott; Kerberos RC4 titkosítás kivezetése, AES használata; hagyományos szolgáltatásfiók helyett gMSA, vagy hosszú, véletlenszerű jelszavak (Kerberoasting elleni védelem).	Konfigurációs riport; szolgáltatásfiók-nyilvántartás; SPN-nel rendelkező fiók listája.
Tartományvezérlők	Csak a szükséges szerepkörök; Print Spooler szolgáltatás letiltása; internetböngészés tiltása; krbtgt fiók jelszavának rendszeres (kétlépcsős) cseréje; AD CS tanúsítványsablonok felülvizsgálata.	Szolgáltatáslista; krbtgt jelszóváltoztatás dátuma; AD CS értékelő riport.
Naplózás	Speciális naplózási házirend (bejelentkezés, fiók- és csoportkezelés, címtárváltozások, folyamatindítás a parancssor rögzítésével); PowerShell Script Block Logging; megfelelő naplóméret; továbbítás SIEM-be.	A naplózási házirend riportja; SIEM-ben megjelenő eseményforrások; mintariasztások.
Támadási felület	Nem használt szerepkörök és szolgáltatások eltávolítása; Windows tűzfal bekapcsolása minden profilon; kritikus kiszolgálókon alkalmazásengedélyezés (AppLocker, App Control for Business) és ASR-szabályok mérlegelése.	Telepített szerepkörök listája; tűzfalszabály-export; megfelelőségi mérés.

3.4.2 Távoli hozzáférést biztosító VPN

A VPN-koncentrátorok és a VPN-funkciót is ellátó tűzfalak az internet felől közvetlenül elérhető határvédelmi eszközök. Az elmúlt években a legtöbbet kihasznált sérülékenységek jelentős része éppen ezeket a termékeket érintette, és sokszor ezek jelentették a zsarolóvírus-támadások kezdeti belépési pontját. A VPN biztonsági beállítása ezért nemcsak magát a VPN-szolgáltatást érinti, hanem az egész eszközt, vagyis az operációs rendszert vagy firmware-t, a menedzsmentfelületet, a fiókokat, a kriptográfiai beállításokat és a naplózást is.

A legfontosabb elvárás, hogy az eszköz menedzsmentfelülete ne legyen elérhető az internet felől, csak dedikált menedzsmenthálózathoz, többfaktoros hitelesítéssel. A firmware frissítésére különösen rövid javítási célidőt célszerű meghatározni, és folyamatosan figyelni kell a gyártói biztonsági közleményeket, valamint a hatósági riasztásokat (például az NBSZ Nemzeti Kiberbiztonsági Intézet figyelmeztetéseit). Kritikus, aktívan kihasznált sérülékenység esetén a javítás mellett azt is meg kell vizsgálni, hogy az eszköz nem kompromittálódott-e (például gyártói integritás-ellenőrző eszközzel vagy naplóelemzéssel), mert a támadók a javítás előtt már hátsó kaput („backdoor”) telepíthettek.

A felhasználói oldalon a többfaktoros hitelesítés ma már alapelvárás, lehetőség szerint az adathalász támadásoknak ellenálló módszerrel (például FIDO2 vagy tanúsítványalapú hitelesítéssel). A sikeres VPN-csatlakozás nem jelenthet korlátlan hozzáférést a belső hálózathoz. A VPN-felhasználók szerepkörük szerint csak a számukra szükséges rendszereket érhetik el (szegmentáció, szerepkörhöz rendelt címtartományok, tűzfalszabályok).

Neuralgikus pontot jelentenek a beszállítói távoli hozzáférések. Különösen rossz gyakorlat, ha a külső támogatást nyújtó cég állandó, széles jogosultságú hozzáféréssel rendelkezik, még rosszabb esetben közös felhasználói fiókkal. Alapvető elvárás, hogy a hozzáférés személyre szóló, időben korlátozott (például csak a karbantartás idejére érvényes), jóváhagyott és naplózott legyen, és csak a feltétlenül szükséges jogosultságokat biztosítsa.

Terület	Javasolt beállítás / intézkedés	Ellenőrzés, auditbizonyíték
Firmware és támogatás	Gyártó által támogatott verzió; rövidített javítási célidő a peremeszközökre; gyártói közlemények és hatósági riasztások figyelése; támogatás végének nyilvántartása.	Verzió- és frissítési napló; sérülékenységszkennelési jegyek; eszköznyilvántartás támogatási dátumokkal.
Menedzsmentfelület	Internet felől nem elérhető; csak menedzsmenthálózathoz vagy jump hostról; MFA; helyi adminisztrátori fiókok minimalizálása, névre szóló fiókok; alapértelmezett fiókok és jelszavak megszüntetése.	Külső portszkennelés eredménye; adminisztrátori fiókok listája; hozzáférési szabályok exportja.
Felhasználói hitelesítés	Kötelező MFA (lehetőség szerint FIDO2 vagy tanúsítvány); címtár-integráció; eszköztanúsítvány vagy eszközállapot-ellenőrzés (posture check); brute-force védelem, zárolás.	Hitelesítési profil konfigurációja; MFA-lefedettségriport; sikertelen bejelentkezések naplója.
Kriptográfia	IKEv2 / TLS 1.2 vagy újabb; erős titkosítási és integritásvédelmi algoritmusok (például AES-GCM, SHA-256 vagy erősebb, megfelelő erősségű DH-csoportok); elavult algoritmusok és protokollok tiltása.	Konfigurációs export; külső TLS-vizsgálat eredménye.
Támadási felület	Nem használt funkciók kikapcsolása (például kliens nélküli webportál, régi VPN-módok, nem használt szolgáltatások a külső interfészen).	Konfigurációs export; külső szkennelés; változáskezelési jegyek.
Hozzáférés a VPN mögött	Szerepkör szerinti szegmentáció; „any-any” szabályok tiltása; a split tunneling kérdésében dokumentált döntés; munkamenet- és tétlenségi időkorlát; beszállítói hozzáférés időkorlátosan, jóváhagyással.	Tűzfalszabály-export és felülvizsgálati jegyzőkönyv; beszállítói hozzáférési nyilvántartás.
Naplózás és felügyelet	Sikeres és sikertelen belépések, forrás IP, adminisztratív tevékenység naplózása; továbbítás SIEM-be; riasztás szokatlan eseményekre (például szokatlan országból érkező belépés, egyidejű munkamenetek, tömeges sikertelen belépés).	SIEM-eseményforrások listája; riasztási szabályok; kivizsgált riasztások jegyei.
Konfiguráció integritása	Rendszeres konfigurációmentés; konfigurációs eltérések figyelése; gyártói integritásellenőrzés kritikus sérülékenység után.	Mentési napló; konfigurációs összehasonlító riportok.

3.4.3 Nextcloud fájlmeosztó és együttműködési platform

A Nextcloud a felhőalapú fájlmeosztó szolgáltatások népszerű, saját üzemeltetésű alternatívája. Sok szervezet éppen érzékeny adatok (szerződések, személyes adatok, műszaki dokumentáció) tárolására és külső partnerekkel való megosztására használja, jellemzően az internet felől is elérhető módon. A hardeningje többretegű feladat, amely az operációs rendszert, a webkiszolgálót és a fordított proxyt (reverse proxy), a PHP-környezetet, az adatbázist és a gyorsítótárat, valamint magának a Nextcloud alkalmazásnak a konfigurációját egyaránt érinti.

Kiindulópontként a Nextcloud adminisztrátori kézikönyvében található hardening és biztonsági útmutató, valamint az alapul szolgáló platformok (Linux, webkiszolgáló, adatbázis) CIS Benchmarkjai használhatók. Egyszerű, de hasznos első lépés, hogy az adminisztrációs felület

beépített biztonsági és beállítási ellenőrzése figyelmeztetések nélkül fusson le¹, és hogy a nyilvánosan elérhető példányt a gyártó külső biztonsági ellenőrző szolgáltatásával (Nextcloud Security Scan) is megvizsgálják². Mindkét ellenőrzés eredménye könnyen menthető, és auditbizonyítékként is felhasználható.

Kiemelt figyelmet érdemel a megosztási házirend, mert az adatszivárgás kockázata itt jellemzően nem technikai hibából, hanem túl megengedő beállításokból fakad. Célszerű kötelezővé tenni a nyilvános linkek jelszavas védelmét és lejáratát idejét, a külső megosztást meghatározott csoportokra korlátozni, és a nem használt funkciókat letiltani (például a Nextcloud-kiszolgálók közötti közvetlen megosztást, az úgynevezett federated sharinget). A telepített alkalmazások (appok) körét a minimumra kell szorítani, mert mindegyik újabb kódot és ezzel újabb támadási felületet jelent.

A szerveroldali titkosítás bekapcsolása önmagában nem jelent magasabb biztonságot. Elsősorban külső tárhely használatakor indokolt, ugyanakkor hatással van a teljesítményre, a mentésre és a helyreállításra, és kulcskezelési kérdéseket is felvet. Alkalmazásáról ezért kockázatelemzés alapján, dokumentáltan érdemes dönteni. Ha a szervezet bevezeti, a mentések visszaállíthatóságát különösen gondosan kell tesztelni.

Terület	Javasolt beállítás / intézkedés	Ellenőrzés, auditbizonyíték
Verzió és frissítés	Támogatott főverzió, stabil frissítési csatorna; alkalmazások (appok) frissítése; PHP és operációs rendszer naprakészen tartása; tervezett frissítési ablak.	Verzió- és frissítési napló; változáskezelési jegyek.
Webkiszolgáló és TLS	Csak HTTPS; HSTS; TLS 1.2 vagy újabb; biztonsági HTTP-fejlécek; a trusted_domains és trusted_proxies helyes beállítása (fordított proxy mögött ez a brute force elleni védelem működéséhez is szükséges).	Beépített adminisztrációs ellenőrzés; külső TLS- és biztonsági szkennelés eredménye.
Fájlrendszer és PHP	Adatkönyvtár a webkiszolgáló dokumentumgyökerén kívül; minimális fájljogosultságok; PHP hardening (például open_basedir, felesleges modulok kikapcsolása); config.php védelme.	Konfigurációs export; megfelelőségi mérés (például Lynis).
Hitelesítés	Kötelező kétfaktoros hitelesítés (TOTP / WebAuthn) legalább adminisztrátoroknak és külső elérésnél; címtár-integráció vagy SSO; brute-force védelem bekapcsolva; jelszóházirend.	2FA kényszerítési beállítás; felhasználói lefedettség; sikertelen belépések naplója.
Megosztási házirend	Nyilvános linkek kötelező jelszóval és lejáratát idővel; külső megosztás csoportokra korlátozva; federated sharing tiltása, ha nincs rá szükség; alapértelmezett jogosultság csak olvasás.	Megosztási beállítások exportja; aktív nyilvános linkek rendszeres felülvizsgálata.
Alkalmazások és adminisztráció	Csak a szükséges appok engedélyezése; adminisztrátori csoport minimális tagsággal; adminisztrációs felület elérésének korlátozása (például forrás IP-cím alapján a fordított proxyn).	Engedélyezett appok listája (például az occ app:list parancs kimenete); adminisztrátori csoport tagsága.

¹ https://docs.nextcloud.com/server/latest/admin_manual/configuration_server/security_setup_warnings.html

² <https://scan.nextcloud.com/>

Terület	Javasolt beállítás / intézkedés	Ellenőrzés, auditbizonyíték
Háttérkomponensek	Adatbázis-felhasználó minimális jogosultsággal, csak helyi elérés; gyorsítótár (például Redis) jelszóval, csak helyi interfészen; ütemezett feladatok rendszerszintű cronnal.	Konfigurációs export; portszkennelés eredménye.
Naplózás és mentés	Megfelelő naplózási szint; adminisztratív és fájlműveletek naplózása (például az admin_audit alkalmazással); továbbítás SIEM-be; konzisztens mentés (karbantartási mód, adatbázis-mentés és adatkönyvtár együtt); rendszeres visszaállítási teszt.	SIEM-eseményforrás; mentési napló; visszaállítási teszt jegyzőkönyve.

4. FELHASZNÁLT FORRÁSOK

- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról (Kiberbiztonsági tv.) (<https://njt.hu/jogszabaly/2024-69-00-00>)
- 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről (<https://njt.hu/jogszabaly/2024-7-20-7G>)
- NBSZ Nemzeti Kiberbiztonsági Intézet, Konfigurációkezelés, EiR útmutató, 1.2 verzió (https://nki.gov.hu/wp-content/uploads/2026/01/06_Konfiguraciokezeles-ver.-1.2.pdf)
- A mellékletben felsorolt nemzetközi, hatósági és gyártói hardening útmutatók

MKIK Jogi állásfoglalások, „Milyen vonzatai vannak egy szerverbeszerzésnek NIS2-kötelezett vállalkozás esetén? Lehetséges-e használt szervert vásárolni?” (<https://nis2.mkik.hu/jogi-allasfoglalasok/49>)

MKIK Jogi állásfoglalások, „Nem támogatott operációs rendszerek NIS2-kompatibilis használata” (<https://nis2.mkik.hu/jogi-allasfoglalasok/38>)

MKIK Jogi állásfoglalások, „»Alap« biztonsági osztályban mi az elfogadott tűzfal technológia és konfiguráció” (<https://nis2.mkik.hu/jogi-allasfoglalasok/8>)

5. MELLÉKLET AZ ELTERJEDT HARDENING ÚTMUTATÓK LELŐHELYEIRŐL

Az alábbi táblázat a biztonsági alapkonzfiguráció kialakításához leggyakrabban használt, nemzetközileg elismert és rendszeresen karbantartott hardening referenciák elérhetőségét foglalja össze. A források kiindulópontként szolgálnak. A kiválasztott referenciát és annak verzióját a szervezetnek saját szabályozásában kell rögzítenie, és a környezetére kell szabnia.

#	Forrás	Kiadó / leírás	Link
Átfogó referenciák			
1.	CIS Benchmarks	Center for Internet Security. Több mint száz hardening útmutató huszonöttnél több gyártó termékcsaládjaihoz, Level 1 és Level 2 profilokkal.	https://www.cisecurity.org/cis-benchmarks
2.	CIS Critical Security Controls	Center for Internet Security. Kontrollkeretrendszer (jelenleg a 8.1-es verzió), amelynek 4. kontrollja a vállalati eszközök és szoftverek biztonságos konfigurációjáról szól.	https://www.cisecurity.org/controls
3.	DISA STIGs	DoD Cyber Exchange (USA). Az amerikai védelmi minisztérium konfigurációs előírásai, gépi (SCAP) ellenőrző tartalommal.	https://www.cyber.mil/stigs
4.	National Checklist Program (NCP) Repository	NIST (USA). Kereshető gyűjtemény a CIS, a DISA, a gyártók és más kiadók biztonsági ellenőrzőlistáiból.	https://ncp.nist.gov/repository
Európai és nemzeti hatósági források			
5.	IT-Grundschutz-Kompendium	BSI (Németország). Rendszerelem-típusonkénti követelménymodulok (például Windows Server, AD, webszerver). A BSI bejelentése szerint a kompendiumot fokozatosan a Grundschutz++ váltja fel.	https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
6.	NIS2 Technical Implementation Guidance	ENISA (EU). Gyakorlati útmutató az (EU) 2024/2690 végrehajtási rendelethez, bizonyítékpéldákkal és megfeleltetési táblával.	https://www.enisa.europa.eu/publications/nis2-technical-implementation-guidance

#	Forrás	Kiadó / leírás	Link
7.	Guides et recommandations	ANSSI (Franciaország). Hardening útmutatók többek között Active Directory, Linux és TLS témában.	https://cyber.gouv.fr/publications
8.	Device Security Guidance	NCSC (Egyesült Királyság). Platformonkénti konfigurációs ajánlások végponti eszközökre (okostelefonok, táblagépek, laptopok, asztali gépek).	https://www.ncsc.gov.uk/collection/device-security-guidance
9.	System hardening	ASD / ACSC (Ausztrália). Például a „Hardening Microsoft Windows 11 workstations” és a „Hardening Linux workstations and servers” útmutató.	https://www.cyber.gov.au/business-government/protecting-devices-systems/hardening-systems-applications/system-hardening
10.	Cybersecurity Advisories & Guidance	NSA (USA). Hardening útmutatók és tanácsok gyűjteménye (hálózati eszközök, Windows, felhő stb.).	https://www.nsa.gov/Cybersecurity/Cybersecurity-Advisories-Guidance/
11.	Secure Cloud Business Applications (SCuBA)	CISA (USA). Biztonsági baseline-ok Microsoft 365 és Google Workspace környezetekhez, ellenőrző eszközökkel (ScubaGear, ScubaGoggles).	https://www.cisa.gov/resources-tools/services/secure-cloud-business-applications-scuba-project
Gyártói és platformspecifikus források			
12.	Security Compliance Toolkit és Security Baselines	Microsoft. GPO-alapú baseline-ok (Windows Server 2016-tól 2025-ig, Windows 10 és 11, Microsoft 365 Apps) a Policy Analyzer és az LGPO eszközzel.	https://learn.microsoft.com/en-us/windows/security/operating-system-security/device-management/windows-security-configuration-framework/security-compliance-toolkit-10
13.	Best Practices for Securing Active Directory	Microsoft. Az Active Directory hardening és a privilegizált hozzáférés védelmének gyártói ajánlásai.	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
14.	Enterprise access model (Securing privileged access)	Microsoft. A kiemelt jogosultsági hozzáférések védelmének gyártói referenciamodellje. Leírja a klasszikus Active Directory szintmodell (Tier 0/1/2), és azt is, hogyan fejlesztette tovább a Microsoft hibrid és felhős környezetekre (control plane, management plane, data plane).	https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model
15.	Selecting and Hardening Remote Access VPN Solutions	NSA / CISA (USA). Távoli hozzáférést biztosító VPN-megoldások kiválasztása és megerősítése (2021. szeptember).	https://media.defense.gov/2021/Sep/28/2002863184/-1/-1/0/CSI_SELECTING-HARDENING-REMOTE-ACCESS-VPNS-20210928.PDF
16.	Hardening and security guidance	Nextcloud. A Nextcloud hivatalos adminisztrátori kézikönyvének hardening fejezete.	https://docs.nextcloud.com/server/latest/admin_manual/installation/harden_server.html

#	Forrás	Kiadó / leírás	Link
17.	Security Hardening (RHEL 9)	Red Hat. Red Hat Enterprise Linux kiszolgálók hardening útmutatója.	https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9/html/security_hardening/index
18.	Ubuntu Security Guide (USG)	Canonical. CIS és DISA STIG szerinti automatizált hardening és audit Ubuntu rendszerekre.	https://documentation.ubuntu.com/security/compliance/usg/
Eszközök és kiegészítő források			
19.	ComplianceAsCode / SCAP Security Guide	Nyílt forrású projekt (GitHub). Gépi formátumú baseline-ok (SCAP, Ansible, Bash), amelyek OpenSCAP-pal auditálhatók.	https://github.com/ComplianceAsCode/content
20.	TLSRef Configurator (korábban Mozilla SSL Configuration Generator)	TLSRef munkacsoport (korábban Mozilla). Ajánlott TLS-konfigurációs minták webszerverekhez és proxykhoz.	https://configurator.tlsref.org/
21.	OWASP Cheat Sheet Series	OWASP. Alkalmazás- és webszintű biztonsági, konfigurációs ajánlások tömör összefoglalói.	https://cheatsheetseries.owasp.org/

A hivatkozások a dokumentum összeállításakor elérhetőek voltak. A gyártói és hatósági oldalak címe idővel változhat, ezért a szabályozásban a referencia pontos nevét és verzióját is célszerű rögzíteni.