

Mikro- és kisvállalkozások számára ajánlott mentési stratégia és mentőeszközök

VFP3 KiberVéd - NIS2 Audit felkészítés szakértői
állásfoglalás 2026/55

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.09.24	Kálmán és Társa Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

- **A szinkronizálás nem mentés.** A OneDrive vagy a Google Drive a zsarolóvírus által titkosított fájlt is továbbviszi, az adatokért pedig nem a szolgáltató, hanem a vállalkozás felel. A Microsoft 365 és a Google Workspace adatairól ezért is független mentés kell.
- **A mentés annyit ér, amennyit vissza lehet állítani belőle.** A mérce a 3-2-1-1-0 szabály, vagyis három példány két különböző adathordozón, egy a telephelyen kívül, egy offline vagy megváltoztathatatlan formában, a próba-visszaállításon pedig nulla hiba. A helyreállítás képessége és annak rendszeres tesztelése alapvető elvárás.
- **Mikrovállalkozásnál a minimum egy független felhőbe való mentés és egy lecsatlakoztatott külső lemez.** Az optimális megoldás egy kétlemezes NAS megváltoztathatatlan pillanatképekkel, amely a gépeket és a felhős fiókokat is menti, és amelyről titkosított másolat kerül a felhőbe vagy váltott lemezre.
- **Kisvállalkozásnál a mentés rendszer, nem eszköz.** 10+ fő esetén központilag felügyelt mentésre van szükség a felhős adatokra, a gépekre és a szerverekre, egy helyi és egy telephelyen kívüli, megváltoztathatatlan példánnyal. Az optimális szinthez elkülönített mentési adminisztrátori fiók, riasztás és negyedéves próba-visszaállítás tartozik.
- **A támadók először a mentést keresik.** Védelmet a megváltoztathatatlan tárolás, a hálózatról leválasztott példány, a többfaktoros hitelesítés és a napi munkától elkülönített adminisztrátori fiók ad.
- **A NIS2 irányelv közvetve a kisvállalkozást is eléri.** A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény (a továbbiakban „Kiberbiztonsági tv.”) főszabály szerint a mellékleteiben felsorolt ágazatokban működő közép- és nagyvállalkozásokat kötelezi, a hatálya alá tartozó megrendelők azonban a beszállítóiktól is elvárják a mentést.

2. A VIZSGÁLANDÓ KÉRDÉS

Egy mikro- vagy kisvállalkozás (a továbbiakban „Vállalkozás”) jellemzően Microsoft 365 vagy Google Workspace előfizetéssel és laptopokon dolgozik, és ha nagyobb, NAS-t vagy kisebb szervert is üzemeltet. Az állásfoglalás az alábbi kérdéseket vizsgálja:

- Milyen mentési stratégiát kövessen egy néhány fős mikrovállalkozás, illetve egy 10-49 fős kisvállalkozás, és mi ezekben a minimális és az optimális megoldás?
- Milyen felhőalapú mentési lehetőségek érhetők el?
- Milyen offline mentési lehetőségek vannak?
- Hogyan védhetők a mentések a zsarolóvírusok ellen?

A méretkategóriákat az állásfoglalás a kis- és középvállalkozásokról szóló törvény szerint használja.¹ Nem tárgya az állásfoglalásnak a hiteles elektronikus archiválás, a teljes üzletmenet-folytonossági terv és az egyes termékek részletes beállítása.

3. GYAKORLATI JAVASLATOK

3.1 Mikrovállalkozás (1-9 fő)

A cél az, hogy egyetlen hiba, lopás vagy támadás se semmisítse meg az összes példányt, és a rendszer informatikus nélkül is működtethető legyen.

Terület	Minimális megoldás	Optimális megoldás
Microsoft 365 vagy Google Workspace	Verziókezelés, lomtár és megőrzés beállítása, többfaktoros hitelesítés, független felhős mentési szolgáltatás (SaaS-mentés) európai adatközponttal, például IDrive vagy Afi.	Mentés a saját NAS-ra díjmentes alkalmazással (Synology Active Backup for Microsoft 365, illetve Active Backup for Google Workspace).
Laptopok, asztali gépek	Felhős végpontmentés EU-régióval (Backblaze Business, IDrive 360) vagy mentés külső lemezre (Windows alatt lemezkép a Veeam Agent for Microsoft Windows FREE programmal, macOS alatt Time Machine).	Napi központi mentés a NAS-ra (Synology Active Backup for Business, QNAP HDP for PC).
Offline vagy megváltoztathatatlan példány	Két titkosított külső lemez heti cserével, az egyik mindig a telephelyen kívül, csak a mentés idejére csatlakoztatva.	Megváltoztathatatlan pillanatkép a NAS-on 14-30 napra, titkosított másolat Object Lock védelemmel a felhőbe (Synology C2, Backblaze B2) vagy váltott lemezre.
Próba	Évente egy teljes gép és néhány fájl visszaállítása, rövid jegyzőkönyvvel.	Félévente dokumentált próba-visszaállítás.
Költségszint	Évi mintegy 20 USD felhasználónként és 30-100 USD gépenként, plusz két külső lemez.	Kétlemezes NAS lemezekkel bruttó 340-450 ezer Ft, plusz a felhős tárhely díja.

3.2 Kisvállalkozás (10-49 fő)

Tíz fő felett megjelennek a közös állományok, a szerverek és a külső informatikai partner, a mentés ezért nem bízható az egyes munkatársakra.

Terület	Minimális megoldás	Optimális megoldás
Microsoft 365 vagy Google Workspace	Független, központilag felügyelt SaaS-mentés EU-adatközponttal és megváltoztathatatlan tárolással (Veeam Data Cloud, Keepit, Afi, partneren keresztül Acronis, Datto) vagy a NAS díjmentes alkalmazásával.	Mint a minimumnál, kiegészítve a Microsoft Entra ID mentésével és egy második, más szolgáltatónál tárolt példánnyal.
Gépek és szerverek	Központi mentés NAS-ra vagy mentőszerverre (Synology Active Backup for Business, QNAP HDP, Veeam Backup & Replication Community Edition 10 munkaterhelésig) megváltoztathatatlan pillanatképekkel.	Dedikált, a céges címtártól független mentőszerver vagy négylemezes NAS (Veeam hardened repository, Proxmox Backup Server, Synology WriteOnce).
Telephelyen kívüli példány	Titkosított, Object Lock védelmű felhős másolat (Backblaze B2, Wasabi, IDrive e2, Synology C2, Veeam Data Cloud Vault) vagy heti lemezrotáció.	Felhős megváltoztathatatlan másolat EU-régióban és havi offline lemezpéldány, vagyis teljes 3-2-1-1-0 megfelelés.
Szervezés	Írásos mentési szabályzat, kijelölt felelős, helyreállítási célok a fő rendszerekre, évente dokumentált próba.	Elkülönített mentési adminisztrátori fiók, riasztás, negyedéves próba, évente teljes helyreállítási gyakorlat, a partnerszerződésben vállalt helyreállítási idő.

¹ 2004. évi XXXIV. törvény a kis- és középvállalkozásokról, fejlődésük támogatásáról 3. § (2) és (3) bekezdés

Költségszint	Négylemezes NAS lemezekkel bruttó 850-1050 ezer Ft, SaaS-mentés havi 2-4 USD/fő nagyságrendben.	A minimumon felül második NAS vagy lemezrotáció bruttó 270-450 ezer Ft, valamint a felhős tárhely díja.
---------------------	---	---

3.3 A javasolt eljárás

A mentési rend bevezetését mindkét méretkategóriában az alábbi lépésekben javasoljuk.

- Felmérés és célok, annak rögzítése, hol vannak az adatok (felhős előfizetések, gépek, NAS, szerver, ügyviteli program, MI-szolgáltatások), és rendszerenként mennyi adatvesztés (RPO) és mennyi kiesési idő (RTO) fogadható el.
- Eszközválasztás, a 4.3. és 4.4. pontban bemutatott megoldások közül a mérethez illő kombináció, európai adatközponttal és megváltoztathatatlan tárolással.
- Keményítés és szabályozás, a 4.5.3. pontban leírt intézkedések, valamint rövid mentési szabályzat a felelősről, a mentési rendről és a visszaállítás menetéről.
- Próba és felülvizsgálat, dokumentált próba-visszaállítás, a mentési naplók havi áttekintése, évenkénti felülvizsgálat.

4. VÁLASZ ÉS RÉSZLETES INDOKOLÁS

4.1 A vizsgálat kiindulópontjai

A mentés az adatok olyan, a forrástól elkülönített másolata, amelyből egy korábbi állapot visszaállítható. A szinkronizálás a törlést és a titkosított fájlt is azonnal továbbviszi, amire a brit Nemzeti Kiberbiztonsági Központ (NCSC) kifejezetten figyelmeztet.²

A mikro- és kisvállalkozásoknál a mentés kötelezettsége elsősorban az adatvédelmi jogból következik. Minden vállalkozás kezel személyes adatot, legalább munkavállalóinak és ügyfeleinek adatait, a GDPR pedig az adatbiztonság elemei között kifejezetten nevesíti a helyreállítás képességét és az intézkedések tesztelését.

(1) Az adatkezelő és az adatfeldolgozó [...] megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja, [...]

c) fizikai vagy műszaki incidens esetén az arra való képességet, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani;

d) az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást. [GDPR 32. cikk (1) bekezdés c) és d) pont]

A zsarolóvírus-támadás, amely a személyes adatokat hozzáférhetetlenné teszi, adatvédelmi incidens, amelyet főszabály szerint 72 órán belül be kell jelenteni a hatóságnak.³ Az Európai

² NCSC, Mitigating malware and ransomware attacks (felülvizsgálva 2021. szeptember 9.)

³ GDPR 33. cikk (1) bekezdés

Adatvédelmi Testület szerint, ha a Vállalkozás megfelelő mentésből rövid időn belül helyreállította az adatokat, és kiszivárgás nem történt, a bejelentés elmaradhat, az incidenst azonban belső nyilvántartásban dokumentálni kell.⁴ A jó mentés tehát a hatósági eljárás kockázatát is csökkenti.

A Kiberbiztonsági tv. a mikro- és kisvállalkozásokat főszabály szerint nem kötelezi.

(1) E törvénynek a szervezetek kötelezettségeire és a kiberbiztonsági hatósági felügyeletre vonatkozó rendelkezéseit kell alkalmazni [...] d) a 2. és 3. melléklet szerinti szervezetekre, amelyek a kis- és középvállalkozásokról, fejlődésük támogatásáról szóló törvény szerint középvállalkozásoknak minősülnek vagy meghaladják a középvállalkozásokra vonatkozóan előírt küszöbértékeket, [...] [2024. évi LXIX. törvény 1. § (1) bekezdés d) pont]

Méretre tekintet nélkül a törvény hatálya alá tartozik néhány szolgáltatói kör, például az elektronikus hírközlési szolgáltatók, a bizalmi szolgáltatók és a DNS-szolgáltatók.⁵ A többi kis cégnél a hatás közvetett, mert a törvény hatálya alá tartozó szervezetek szerződésben követelik meg, hogy a beszállító által nyújtott rendszerek megfeleljenek a saját biztonsági követelményeiknek. Erre az MKIK [„Milyen információbiztonsági kockázatok merülnek fel általános célú MI-rendszerek \(LLM\) vállalati használatánál? NIS2 és AI Act előírások a kockázatok kezelésére”](#) című jogi állásfoglalása is rámutat.⁶ A mentés ezek között alapkövetelmény, amely az MKIK [„Milyen információbiztonsági kockázatok merülnek fel meghatározó MI-komponenst tartalmazó célszoftverek vállalati használatánál? NIS2 és AI Act előírások a kockázatok kezelésére”](#) című állásfoglalása szerint minden biztonsági osztályban kiterjed a rendszerszintű információkra is.⁷

A mentés szakmai mércéje a 3-2-1 szabály, amelyet a Nemzeti Kibervédelmi Intézet is ajánl azzal, hogy egy példány teljesen offline legyen.⁸ A piaci gyakorlat ezt 3-2-1-1-0 formára bővítette, ahol az utolsó két elem az offline vagy megváltoztathatatlan példány és a hibátlan próba-visszaállítás.⁹ A stratégia két kulcsszáma az RPO, vagyis hogy legfeljebb mennyi munka vesztet el, és az RTO, vagyis hogy mennyi idő alatt kell a rendszernek újra működni.

4.2 Milyen mentési stratégiát kövessen a mikro- és a kisvállalkozás?

4.2.1 Mit kell menteni

⁴ Európai Adatvédelmi Testület, 01/2021. számú iránymutatás az adatvédelmi incidensek bejelentésével kapcsolatos példákról (2.0 változat), 2.1. pont, CASE No. 01

⁵ 2024. évi LXIX. törvény 1. § (1) bekezdés e) pont

⁶ MKIK, VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/43 (2026. szeptember 17.), nis2.mkik.hu/jogi-allasfoglalasok/45

⁷ MKIK, VFP3 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/45 (2026. szeptember 18.), nis2.mkik.hu/jogi-allasfoglalasok/48

⁸ Nemzeti Kibervédelmi Intézet, Tudástár, Zsarolóvírus (Ransomware) (2019. június 4.)

⁹ Veeam, Air Gap vs Immutable Backups (frissítve 2026. augusztus 5.)

2024-ben a hazai 10-49 fős vállalkozásoknak csak mintegy 60 százaléka mentett külön helyre, az uniós átlag 77 százalék volt, a mikrovállalkozásokra pedig nincs ilyen adat.¹⁰ A leggyakoribb hiba, hogy a Vállalkozás a gépeket menti, a felhőben lévő levelezést és dokumentumokat viszont nem. A Microsoft maga javasolja a beépített eszközök mellett a Microsoft 365 Backup vagy egy elismert partnermegoldás használatát, a Google pedig rögzíti, hogy a Vault nem mentési eszköz.¹¹

A mentésnek ki kell terjednie a felhős fiókokra, a gépekre, az ügyviteli programok adatbázisára, a NAS-ra, a szerverekre és a beállításokra, újabban pedig az MI-szolgáltatásokra is. Az MKIK 2026/45. számú jogi állásfoglalása szerint a meghatározó MI-komponenst tartalmazó célszoftver a modellfájl és a tanítóadat mentése nélkül nem állítható helyre, a 2026/43. számú pedig arra figyelmeztet, hogy az eltérített MI-ügynök fájl is törölhet, és hogy az MI-szolgáltatás kiesésével az üzletmenet-folytonossági tervben számolni kell.

4.2.2 A mikrovállalkozás stratégiája

Néhány fős cégnél a legnagyobb kockázat az ellopott vagy tönkrement laptop, a véletlen törlés és a tömeges, automatizált zsarolóvírus-támadás. A minimum ezért két, egymástól független példány. A felhős példány automatikusan készül, a lecsatlakoztatott lemez pedig akkor is megmarad, ha a felhős fiókot feltörik. Az optimális szinten egyetlen eszköz, a NAS menti licencdíj nélkül a gépeket és a felhős fiókokat, a megváltoztathatatlan pillanatképet pedig sem egy fertőzött gép, sem egy ellopott jelszó nem tudja törölni.

4.2.3 A kisvállalkozás stratégiája

A kisvállalkozásnál a központi felügyelet a döntő különbség, a mentés hibájáról valakinek értesítést kell kapnia. Az optimális szint lényege az elkülönítés. A támadók a rendszergazdai jogosultság megszerzése után a mentőkonzolt is megkeresik, ezért a mentőrendszer ne legyen tagja a céges címtárnak, saját, többfaktoros hitelesítéssel védett adminisztrátori fiókja legyen, és a mentés törlése ne legyen egyetlen jelszóval végrehajtható.¹² Ha a mentést külső partner végzi, legalább egy példány felett a Vállalkozásnak magának is rendelkeznie kell.

4.3 Milyen felhőalapú mentési lehetőségek vannak?

A Microsoft 365 a OneDrive és a SharePoint törölt elemeit 93 napig őrzi, és a teljes tartalom 30 napra visszamenőleg állítható vissza. A Google Drive a régi verziókat 30 napig, legfeljebb 100 verzióig tartja meg. Ezek hasznos első védvonalak, de ugyanazzal a jogosultsággal érhetők el, mint az éles adat. A fizetős Microsoft 365 Backup (0,15 USD/GB/hó) gyors visszaállítást ad, de a Microsoft saját infrastruktúráján belül marad, ezért független példányt nem pótol.¹³ A független felhős mentés fő típusai a következők.

Típus	Ismert megoldások	Tudnivalók, tájékoztató árak
-------	-------------------	------------------------------

¹⁰ Eurostat, ICT security in enterprises, isoc_cisce_ra tábla, E_SECMOSBU mutató (2024)

¹¹ Microsoft Learn, Ransomware protection in Microsoft 365 (frissítve 2025. szeptember 29.); Google Vault súgó (support.google.com)

¹² NCSC, Principles for ransomware-resistant on-premises backups (2024. november 22.), 1. és 3. alapelv

¹³ Microsoft Learn, Microsoft 365 Backup dokumentáció (frissítve 2026. augusztus 18.); Google Drive súgó, verzióelőzmények

SaaS-mentés felhőszolgáltatásként	Veeam Data Cloud for Microsoft 365, Keepit, Afi, IDrive, Acronis, Datto SaaS Protection, NinjaOne SaaS Backup, AvePoint, Druva, CrashPlan	Veeam 10-50 fő esetén 3,50 USD/fő/hó, EU-adatközponttal. IDrive 20 USD/fő/év. A dán Keepit saját európai adatközpontokat használ, a CrashPlan az Egyesült Államokban tárol.
SaaS-mentés saját eszközre	Synology Active Backup for Microsoft 365 és for Google Workspace, Veeam Backup for Microsoft 365 Community Edition, QNAP HDP for SaaS	A Synology alkalmazása a NAS-on licencdíj nélkül használható, a Veeam közösségi kiadása 10 felhasználóig ingyenes, a QNAP 9,49 USD/fő/év.
Gépek mentése a felhőbe	Backblaze Computer Backup, IDrive 360, CrashPlan, Acronis True Image, Carbonite, Synology C2 Backup, Magyar Telekom Adatparki biztonsági mentés	Backblaze 99 USD/gép/év, az EU-régió csak a fiók létrehozásakor választható. IDrive 360 öt eszközre 149,50 USD/év. A Telekom hazai adatközpontban tárol.
Felhős tárhely Object Lock zárolással (a NAS vagy a mentőszoftver célhelye)	Backblaze B2, Wasabi, IDrive e2, Synology C2, QNAP myQNAPcloud One, Veeam Data Cloud Vault, Hetzner, OVHcloud, Scaleway, AWS S3, Azure Blob	B2 6,95 USD/TB/hó amszterdami régióval. Wasabi 7,99 USD/TB/hó, de 1 TB minimális díjjal és 90 napos minimális tárolással. IDrive e2 6 USD/TB/hó. A Veeam Vault zárolása nem kapcsolható ki.
Szinkronizáló tárhely verziókezeléssel	OneDrive, Google Drive, Dropbox, Tresorit, pCloud, Proton Drive	Önmagában nem mentés. A magyar alapítású Tresorit végponttól végpontig titkosít, de a korábbi verziók csak fájlként tölthetők le.

Felhős mentésnél a szolgáltató adatfeldolgozónak minősül, ezért a GDPR 28. cikke szerinti adatfeldolgozási szerződés kötelező, előnyt jelent továbbá az Európai Unión belüli adatközpont és a szolgáltatótól független titkosító kulcs. Az európai régiót több amerikai szolgáltatónál csak a fiók létrehozásakor lehet kiválasztani.

4.4 Milyen offline mentési lehetőségek vannak?

A legegyszerűbb offline megoldás a külső USB-lemez, amely csak a mentés idejére csatlakozik. A lemezt titkosítani kell (BitLocker To Go, a Time Machine titkosított mentése vagy a mentőszoftver titkosítása). A hardveresen titkosított, írásvédett módot is kínáló eszközök (Kingston IronKey Vault Privacy 80, Apricorn Aegis Padlock) a kulcskezelést is egyszerűsítik.

A kis cégek számára a NAS a legjobb ár-érték arányú helyi mentési cél, ha nem hálózati meghajtóként, hanem mentőszerverként használják, amely maga kéri le az adatokat a gépekről.

Gyártó	Mentőalkalmazások	Zsarolóvírus elleni funkciók, megjegyzés
Synology	Active Backup for Business (gépek, szerverek, VMware, Hyper-V), Active Backup for Microsoft 365 és Google Workspace, Hyper Backup, licencdíj nélkül	Megváltoztathatatlan pillanatkép és WriteOnce mappa a támogatott modelleken. A harmadik féltől származó lemezekre vonatkozó 2025-ös korlátozást a DSM 7.3 a SATA-meghajtóknál feloldotta.
QNAP	Hybrid Backup Sync 3, HDP for PC/VM, HDP for SaaS	Megváltoztathatatlan pillanatkép a QuTS hero h6.0 rendszertől. A 2021-es QLocker támadás a mentőalkalmazás hibáján át törölte a pillanatképeket, a frissítés ezért kiemelten fontos.
Asustor, TerraMaster	ASUSTOR Backup Plan, TerraMaster Business Backup Suite	WORM, illetve zárolt pillanatkép egyes modelleken. Beszerzés előtt a hazai szerviz- és partnerhálózatot érdemes ellenőrizni.
UGREEN	UGOS Pro beépített mentés	A gyártó szerint a pillanatképek nem megváltoztathatatlanok, ezért az eszköz zsarolóvírus-álló célhelyként ma kevésbé alkalmas.

A mentőszoftvereknél a licencfeltétel is számít, mert több ismert ingyenes kiadás csak otthoni használatra engedélyezett.

- Beépített eszközök, a Windows Fájlelőzmények a Vezérlőpultból ma is elérhető, a Windows Backup alkalmazás viszont csak a OneDrive-ra ment, munkahelyi fiókkal nem

használható, a régi rendszerkép-készítő pedig elavult. macOS gépen a titkosított külső lemezre vagy NAS-ra mentő Time Machine jó választás.

- b) Üzleti célra is ingyenes megoldások, a Veeam Agent for Microsoft Windows FREE teljes lemezképet készít, a Veeam Backup & Replication Community Edition 10 munkaterhelésig használható, a Cobian Reflector fájl szintű mentést végez, a nyílt forráskódú restic, Kopja, Duplicati és UrBackup informatikai támogatással jól működik.
- c) Fizetős termékek, az Acronis True Image és a Macrium Reflect X csak előfizetéssel érhető el, a Macrium üzleti célra Workstation vagy Server licencet igényel. A Macrium Reflect 8 és annak ingyenes kiadása már nem kap biztonsági frissítést, az AOMEI Backupper Standard, az EaseUS Todo Backup Free és a Paragon Backup & Recovery CE pedig csak otthoni, nem üzleti használatra engedélyezett.
- d) Szerverek, a Veeam hardened repository megváltoztathatatlan tárolást ad, a Proxmox Backup Serverben a mentett gép jogosultsága a korábbi mentések törlésére nem terjed ki. A Windows Server Backup hálózati megosztáson csak egy verziót tart meg.

Az LTO-szalagos meghajtó ára kis cégnél ritkán térül meg, az RDX-kazetták gyártója pedig 2024-ben fizetéseképtelenné vált, ezért egyiket sem javasoljuk új beruházként.

4.5 Hogyan biztosítható a zsarolóvírus elleni védelem?

4.5.1 A támadás a mentést célozza

A Veeam 2025-ös jelentése szerint a támadások 89 százaléka a mentéseket is célba vette.¹⁴ A Sophos adatai szerint, ahol a mentés is sérült, a váltságdíjat fizetők aránya 67 százalék volt az ép mentésű szervezetek 36 százalékával szemben, a helyreállítás költsége pedig nyolcszoros.¹⁵ A Verizon szerint az ezer főnél kisebb szervezeteket érintő, megerősített adatbiztonsági incidensek 88 százalékában jelen volt zsarolóvírus.¹⁶ A kis cégeknél a mentés gyakran a napi munkához használt jelszóval elérhető, meghajtóbetűjellel csatolt hálózati mappába készül, ilyenkor a zsarolóvírus azt is titkosítja.

4.5.2 Megváltoztathatatlanság és légrés

A megváltoztathatatlan (immutable, WORM) tárolásnál a mentést a megőrzési idő alatt még a rendszergazda sem törölheti. A légrés (air gap) azt jelenti, hogy legalább egy példány fizikailag vagy logikailag nem érhető el a hálózatról. A Nemzeti Kibervédelmi Intézet a fizikailag leválasztható meghajtóra készített rendszeres mentést tartja a legfontosabb intézkedésnek, az amerikai CISA és a brit NCSC ajánlásai ugyanerre az offline, titkosított és tesztelt példányra épülnek.¹⁷ A zárolást legalább 14, de inkább 30 napra érdemes beállítani, mert a kártevő a titkosítás előtt gyakran hetekig lappang.

4.5.3 Hozzáférés és hardening

¹⁴ Veeam, From Risk to Resilience, 2025 Ransomware Trends and Proactive Strategies Report (2025)

¹⁵ Sophos, The impact of compromised backups on ransomware outcomes (2024. április)

¹⁶ Verizon, 2025 Data Breach Investigations Report, SMB Snapshot

¹⁷ Nemzeti Kibervédelmi Intézet, Zsarolóvírus (Ransomware) (2019); CISA, #StopRansomware Guide (2023. október); NCSC, Ransomware-resistant backups gyűjtemény (2024. november 22.)

A mentési infrastruktúra védelmét az alábbi intézkedésekkel javasoljuk biztosítani.

- a) A mentőrendszernek külön, többfaktoros hitelesítéssel védett adminisztrátori fiókja legyen, amely nem azonos a napi munkára használt fiókkal.
- b) A mentési tárolót ne csatolják meghajtóbetűjellel a gépekre, a mentés ügynökön keresztül vagy a NAS által kezdeményezve készüljön.
- c) A NAS és a mentőkonzol ne legyen elérhető az internetről, távoli eléréshez VPN-t kell használni, a QuickConnect, az UPnP és a porttovábbítás funkciót ki kell kapcsolni.
- d) A mentőszoftvert és a NAS rendszerét automatikusan frissíteni kell, mert a NAS-eszközök elleni tömeges támadások ismert hibákra épültek.
- e) A titkosító kulcs papíron, széfben elzárva is legyen meg, és riasztás jelezze a sikertelen mentést és a tömeges törlést.

4.5.4 Helyreállítás és próba

A Sophos 2026-os felmérése szerint a 100-5000 fős szervezetek körében a titkosított adatokat az érintettek 66 százaléka mentésből állította helyre, szemben az előző évi 54 százalékkal.¹⁸ A helyreállítást tiszta, újrategyűjtött rendszerre kell végezni, a mentés fertőzőttségének ellenőrzése után. A CISA legalább évenkénti, az ENISA rendszeres, lehetőleg teljes próba-visszaállítást javasol.¹⁹ A minimum mindkét méretben az évenkénti próba, az optimális szint mikrovállalkozásnál a félévenkénti, kisvállalkozásnál a negyedéves. A jegyzőkönyv a GDPR szerinti rendszeres tesztelést is igazolja.

5. FELHASZNÁLT FORRÁSOK

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (GDPR): <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
- 2024. évi LXIX. törvény Magyarország kiberbiztonságáról: <https://njt.hu/jogszabaly/2024-69-00-00>
- 2004. évi XXXIV. törvény a kis- és középvállalkozásokról: <https://njt.hu/jogszabaly/2004-34-00-00>
- MKIK Iránymutatások (pl. 2026/14 Biztonságos törlési megoldások): <https://nis2.mkik.hu/iranymutatasok>
- Európai Adatvédelmi Testület (EDPB) 01/2021. számú iránymutatás: https://edpb.europa.eu/system/files/2022-01/edpb_guidelines_012021_adb_notification_adopted_hu.pdf
- Nemzeti Kibervédelmi Intézet (NKI): <https://nki.gov.hu/>
- Külföldi intézmények ajánlásai: CISA (USA), NCSC (Egyesült Királyság), ENISA (EU), Eurostat.

¹⁸ Sophos, The State of Ransomware 2026 (2026. június)

¹⁹ CISA, Cross-Sector Cybersecurity Performance Goals, 2.R cél (2023); ENISA, Cybersecurity guide for SMEs (2021), 9. lépés

- Iparági statisztikák: Veeam, Sophos és Verizon felmérések; a gyártók és szolgáltatók nyilvános termékleírásai és árlistái (2026. szeptember 30.)

6. FELELŐSSÉGGKIZÁRÓ NYILATKOZAT