Mit veszíthetünk? Valós incidensek elemzése, tanácsok az elkerülésükre

VFP2 KiberVéd - NIS2 Audit felkészítés jogi állásfoglalás 2026/20

VERZIÓKÖVETÉS

Verziószám	Dátum	Módosította	Módosítások leírása
1.0	2026.02.21	Kálmán és Társai Ügyvédi Iroda	Első kiadott verzió

1. VEZETŐI ÖSSZEFOGLALÓ

A közelmúlt hazai kiberbiztonsági incidensei azt mutatják, hogy ezek az esetek nem csupán adatvesztést, illetve adatszivárgást okozhatnak, hanem eredményezhetnek több napos vagy akár több hetes szolgáltatás-kiesést, teljes működésleállást (zsarolóvírus), illetve akár ipari folyamatok biztonságát érintő kockázatokat is (OT/ICS).

A bemutatott incidensek alapján látható, hogy a támadók gyakran hitelesítő adatok megszerzésével, internetre kitett rendszereken keresztül jutnak be. A hatást súlyosbítja, ha nincs felügyeleti (monitoring / napló elemző), illetve riasztó rendszer, valamint ha nem megfelelően szegmentált a hálózat. A szervezetek veszteségei jellemzően a következő területeken jelentkeznek:

- Üzletmenet-folytonosság: szolgáltatáskiesés, termelés/logisztika leállása, elmaradt bevétel.
- Adatvédelem: személyes (és különösen egészségügyi), illetve üzleti / pénzügyi adatok kiszivárgása, elérhetetlensége; hatósági vizsgálat, jogi kockázat.
- Bizalom és reputáció: ügyfél- és partnerbizalom megingása; ügyfelek elvesztése; kommunikációs nyomás
- Közvetlen költségek: incidens kivizsgálás és kezelés; rendszer helyreállítás; külső szakértők (IT, jog, kommunikáció); új védelmi, illetve IT eszközök beszerzése; adott esetben hatósági büntetés, valamint esetleg kártérítések

Az alábbi összefoglalók célja, hogy a „Mit veszíthetünk?” kérdést konkrét példákon keresztül megválaszolja, és rámutasson azokra az alapvető megelőző intézkedésekre, amelyek az esetek többségében mérhetően csökkentik a bekövetkezés valószínűségét vagy a hatás súlyosságát.

2. INCIDENSEK ELEMZÉSE

Minden incidensnél egységes szerkezetben ismertetjük az eseményt, a típust, a veszteségeket, a megelőzési lehetőségeket és a legfontosabb tanulságokat.

3. SECTOR 16 – MAGYAR GEOTERMIKUS TERMELŐRENDSZER ELLENI TÁMADÁS (2025. JÚLIUS)

3.1 Az incidens bemutatása

Incidens leírása: A beszámolók szerint a SECTOR 16 nevű hackercsoport 2025 júliusában jogosulatlan hozzáférést szerzett egy magyar geotermikus termelőrendszer kritikus irányítói felületéhez. A támadók részletes képet kaptak a rendszer működéséről és a biztonsági beállításokról, majd bizonyítékokat tettek közzé. Közvetlen beállítás-módosítást vagy szabotázst nem jeleztek, ugyanakkor képesek lettek volna olyan zavarokat okozni, mint például ventilátorok-leállása vagy túlmelegedésének okozása, vagy nyomásingadozás előidézése, amelyek súlyos üzemzavarhoz vezettek volna.

Incidens típusa: OT/ICS rendszer elleni behatolás (jogosulatlan hozzáférés)

Lehetséges veszteségek:

Fizikai és üzembiztonsági kockázat: a túlmelegedés/nyomásingadozás berendezéskárosodáshoz és termeléskieséshez vezethet.

Helyreállítási és vizsgálati költségek: incidens forensics vizsgálata, rendszeraudit, hozzáférések újraszervezése, hardening.

Reputációs és szabályozói kockázat: kritikus infrastruktúrához közeli rendszerek esetén fokozott figyelem.

Potenciális további károk kockázata: a támadók helyismerete növeli egy későbbi támadás valószínűségét.

Hogyan lett volna megelőzhető az incidens:

A termelésirányítási környezetet (OT) hálózatilag el kellett volna választani az irodai IT-től és az internettől, minimálisra csökkentve a távoli elérések számát.

Minden távoli adminisztrációt, hozzáférést többtényezős hitelesítéssel és szigorú jogosultságkezeléssel kellett volna védeni.

Rendszeres kiberbiztonsági felülvizsgálatot és sérülékenységkezelést kellett volna végezni a teljes rendszer tekintetében

OT-környezetre szabott behatolásészlelést esetleg naplógyűjtést kellett volna bevezetni, hogy a gyanús műveletek gyorsan észlelhetők legyenek.

A személyzetet célzottan kellett volna képezni a kiberbiztonsági incidensek felismerésére és kezelésére.

> ***Tanulságok:*** *Az OT/ICS rendszerek elleni támadások már nem elméleti kockázatok: egy „nem romboló" behatolás is komoly figyelmeztetés, mert bizonyítja a hozzáférést és a folyamatismeretet. A kritikus üzemei folyamatoknál a kiberbiztonsági kontrollok hiánya gyorsan fizikai és üzletmeneti kockázattá alakulhat.*

3.2 Javasolt 7/2024 MK követelmények

1. **Hálózati szegmentáció / információáramlás-szabályozás**

> *„2.28. A szervezet a meghatározott információáramlási szabályokkal összhangban érvényesíti a jóváhagyott jogosultságokat a rendszeren belüli és a kapcsolódó rendszerek közötti információáramlás ellenőrzése során."*

Miért? IT–OT logikai szétválasztás, csak szükséges forgalom engedése az OT irányítórendszer felé, internet / irodai hálózat felől érkező kapcsolatok minimalizálása.

2. **Távoli hozzáférés egységes szabályozása**

> *„2.100. A szervezet:*
> *2.100.1. Kidolgozza és dokumentálja az engedélyezett távoli hozzáférés minden egyes típusára vonatkozóan a használati korlátozásokat, a konfigurációs vagy csatlakozási követelményeket és az alkalmazási útmutatókat.*

2.100.2. Engedélyezési eljárást folytat le a rendszerhez való távoli hozzáférés minden egyes típusára, az ilyen kapcsolatok lehetővé tételét megelőzően"

Miért? OT-felületek távoli adminisztrációja csak formalizált, engedélyezett csatornákon, kontrollált módon valósulhatna meg.

3. **Távoli hozzáférés titkosítása és kontrollált pontokon keresztül vezetése**

„2.102. A szervezet kriptográfiai mechanizmusokat alkalmaz a távoli hozzáférés biztonságának és sértetlenségének biztosítása érdekében."
„2.103. A szervezet a távoli hozzáféréseket engedélyezett és menedzselt hálózati hozzáférés-felügyeleti pontokon keresztül irányítja."

Miért? OT-iranyítói felület csak biztonságos, titkosított, központilag menedzselt ugrópontokon / VPN-en keresztül lenne elérhető.

4. **Privilegizált fiókok védelme, PAM-szemlélet**

„2.9. A szervezet:
2.9.1. Létrehozza és kezeli a privilegizált fiókokat egy szerepköralapú vagy tulajdonságalapú hozzáférési rendszerrel összhangban.
2.9.2. Felügyeli a privilegizált szerepkörök vagy tulajdonságok hozzárendeléseit.
2.9.3. Felügyeli a szerepkörök vagy tulajdonságok változásait.
2.9.4. Visszavonja a hozzáférést, amikor a privilegizált szerepkörök vagy tulajdonságok hozzárendelése többé már nem releváns."

Miért? Az OT-irányításhoz használt admin fiókok szigorú kezelése (RBAC, rendszeres review) csökkenti a kompromittálható, túl-széles jogosultságú fiókok számát.

5. **Többtényezős hitelesítés kritikus fiókokra**

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

Miért? Az OT-admin hozzáférések MFA nélkül könnyen kompromittálhatók (jelszólopás, brute force stb.).

6. **Eszközök azonosítása és hitelesítése az OT-zónában**

„8.10. A szervezet egyedileg azonosítja és hitelesíti a meghatározott eszközöket, vagy eszköztípusokat, mielőtt helyi, távoli, hálózati vagy egyéb kapcsolatot létesítene velük."
Miért? Ismeretlen / nem hitelesített eszközről ne lehessen az OT környezethez kapcsolódni (pl. „rogue" laptopról).

7. **Folyamatos technikai felügyelet / monitoring**

„5.15. A szervezet kidolgozza a rendszerszintű folyamatos felügyeleti stratégiát és megvalósítja a folyamatos felügyeletet a szervezeti szintű stratégiával összhangban, amely magában foglalja a következőket:
5.15.1. A rendszerszintű metrikák meghatározását.
5.15.2. Rendszeres felügyelet biztosítását a védelmi intézkedések hatékonyságának értékelésére.
5.15.3. A védelmi intézkedések folyamatos értékelését.
5.15.4. Az EIR és a szervezet által meghatározott mutatók folyamatos nyomon követését.
5.15.5. A védelmi intézkedésekről gyűjtött és feldolgozott információ összegzését és kiértékelését.
5.15.6. A védelmi intézkedések értékelése és elemzése alapján végrehajtott válaszintézkedéseket.
5.15.7. az EIR biztonsági állapotáról rendszeres időközönként történő jelentés a kijelölt személyeknek.”

Miért? OT-specifikus loggyűjtés és behatolásészlelés – a gyanús műveletek, hozzáférésminták korai detektálására.

8. **Rendszeres biztonsági értékelés (audit / pentest)**

„5.2. A szervezet:
5.2.1. Kiválasztja az elvégzendő értékelés típusának megfelelő értékelő személyt vagy csoportot.
5.2.2. Biztonságértékelési tervet készít, …
5.2.4. Meghatározott gyakorisággal értékeli az EIR és működési környezete védelmi intézkedéseit, kontrollálja a bevezetett intézkedések működőképességét, valamint a tervezettnek megfelelő működését.
5.2.5. Elkészíti a biztonságértékelés eredményét összefoglaló jelentést.”

Miért? Az OT-rendszer sérülékenységeinek és rossz konfigurációinak (internet felé nyitott felületek) feltárása, még a támadók előtt.

9. **Kockázatelemzés és kockázatok kezelése OT-fókuszban**

„5.1.1. A szervezet értékeli az elektronikus információs rendszerrel, az általa kezelt adatokkal kapcsolatosan felmerülő kockázatokat, amelynek keretében:
5.1.1.1. Azonosítja és dokumentálja az elektronikus információs rendszer és az általa feldolgozott adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából értelmezhető fenyegetéseket. …
5.1.1.5. Meghatározza a fenyegetések káros hatásainak és azok bekövetkezésének valószínűsége alapján az eredő kockázatokat, valamint legalább négy fokozatú skálán („alacsony”, „közepes”, „magas”, „kritikus”) azok mértékét (kockázati kategória).”

Miért? Az OT-folyamatok rendelkezésre állási és biztonsági kockázatai alapján magasabb osztályba sorolás és erősebb kontrollok kijelölése.

10. **Biztonságtudatossági és szerepkör-alapú képzés az OT-személyzetnek**

„3.2. A szervezet:
3.2.1. Biztonságtudatossági képzést biztosít a rendszer felhasználói számára …
3.2.3. Frissíti a képzési és tudatossági tananyagot …
3.2.4. Integrálja a belső és külső biztonsági eseményekből levont tanulságokat a képzési anyagokba…"
„3.9. A szervezet:
3.9.1. Szerepkör alapú biztonsági képzést nyújt a felhasználóknak…
3.9.3. Beépíti a belső vagy külső biztonsági eseményekből levont tanulságokat a szerepköralapú biztonsági képzésekbe."

Miért? OT-mérnökök, üzemeltetők célzott képzése a kiberkockázatok felismerésére, helyes adminisztrátori gyakorlatokra.

4. ROSSMANN MAGYARORSZÁG – WEBSHOP ÉS APP KUPONKÖZPONT LEÁLLÁSA (2025. DECEMBER)

4.1 Az incidens bemutatása

Incidens leírása: A Rossmann egyik informatikai rendszerét kibertámadás érte, amelyet a vállalat közlése szerint rövid időn belül észleltek. A vásárlói adatok védelme érdekében elővigyázatosságból több rendszert – köztük a webshopot és az applikáció kuponközpontját – ideiglenesen elérhetetlenné tettek. A leállás napokig tartó fennakadásokat okozott az online vásárlásokban, rendelésekben, kiszállításban, valamint a kupon- és ajándékkártya-használatban.

Incidens típusa: kiberbiztonsági incidens miatt szolgáltatás-kiesés

Okozott veszteségek:

- Bevételkiesés a webshop leállása és a rendeléskezelési fennakadások, valamint a kuponok és ajándékkártya használat leállítása miatt.
- Ügyfélélmény-romlás és reputációs kár (főként a kuponok, ajándékkártyák használhatatlansága, valamint a kiszállítások akadozása miatt).
- Lehetséges adatszivárgás (egyelőre nem bizonyított)
- Megnövekedett ügyfélszolgálati és üzleti terhelés (panaszkezelés, manuális kompenzáció, kuponok hosszabbítása, kártyák hosszabbítása).
- Kivizsgálási és helyreállítási költségek (Rosmann saját híre szerint: külső nemzetközi IT-biztonsági szakértők igénybevétele, illetve extra üzemeltetési költségek).

Hogyan lett volna megelőzhető az incidens:

- A híradásokból csak igen keveset lehet megtudni az incidensről, így a pontos megelőző intézkedésekre csak ezekből tudunk következtetni: Az adatok alapján vélhetően gyakrabban

kellett volna professzionális sérülékenységvizsgálatot végezni az internet irányába nyújtott szolgáltatások tekintetében (például webalkalmazás, API-k, VPN).

- Az üzletmenet-folytonossági terv és helyreállítási terv tekintetében vélhetően voltak hiányosságok, mivel a webshop december 13. és 30. között nem volt elérhető.
- Gyakorolt incidenskezelési és kommunikációs forgatókönyvet kellett volna fenntartani, hogy a helyreállítás gyorsabb legyen, illetve e közben is kiszámítható legyen a tájékoztatás.

Tanulságok: *A kereskedelmi rendszerekben a „biztonság vs. elérhetőség" döntés azonnali bevétel- és bizalomvesztéssel járhat. A jól kialakított szegmentáció, monitoring és üzletmenet-folytonosság lehetővé teszi, hogy a védekezés célzott legyen, és lehetőség szerint ne járjon teljes szolgáltatás-leállással.*

4.2 Javasolt 7/2024 MK követelmények

1. **Sérülékenységkezelés**

„15.9. A szervezet:
15.9.1. Meghatározott folyamat szerint rendszeresen vagy eseti jelleggel ellenőrzi az EIR sérülékenységeit, illetve minden olyan esetben, amikor új, az EIR-t potenciálisan érintő sérülékenységeket azonosítanak és jelentenek.
15.9.2. Kijavítja a valós sérülékenységeket a meghatározott válaszidőn belül, a kockázatkezelési eljárásoknak megfelelően."

Miért? Webshop, API-k, VPN-ek rendszeres sérülékenységvizsgálata, gyors patch-elés – kevesebb sikeres kompromittálás.

2. **Sérülékenységmenedzsment eszközökkel**

„15.10. A szervezet:
15.10.1. Meghatározott folyamat szerint rendszeresen vagy eseti jelleggel szkenneli az EIR sérülékenységeit…
15.10.2. Olyan sérülékenységmenedzsment eszközöket és technikákat alkalmaz, amelyek … automatizálják a sérülékenységkezelési folyamat egyes lépéseit…
15.10.4. Kijavítja a valós sérülékenységeket a meghatározott válaszidőn belül…"

Miért? Folyamatos scanning az internetre néző komponenseken, így a gyenge pontok még a támadás előtt kiderülnek.

3. **Üzletmenet-folytonossági terv (BCP)**

„7.2. A szervezet:
7.2.1. Kidolgozza az EIR-re vonatkozó üzletmenet-folytonossági tervet, amely:
7.2.1.2. tartalmazza a helyreállítási célokat, a helyreállítási prioritásokat és metrikákat;
7.2.1.4. meghatározza az EIR összeomlása, kompromittálódása vagy hibája ellené-

re is biztosítandó szolgáltatásokat;
7.2.4. Meghatározott gyakorisággal felülvizsgálja az EIR-hez kapcsolódó üzletmenet-folytonossági tervet."

Miért? Webshop és kuponrendszer kritikus üzleti funkció – BCP nélkül hosszú, decemberi kiesés keletkezik.

4. **BCP tesztelése**

„7.13. A szervezet:
7.13.1. meghatározott gyakorisággal és meghatározott teszteken keresztül vizsgálja az EIR-re vonatkozó üzletmenet-folytonossági tervet …; értékeli az üzletmenet-folytonossági terv tesztelési eredményeit;
7.13.3. a felülvizsgálat eredményei alapján, szükség esetén javítja a tervet."

Miért? Gyakorlott visszaállítás – gyorsabb szolgáltatás helyreállítás, kisebb bevételkiesés.

5. **Biztonsági mentések és helyreállítás**

„7.35. A szervezet:
7.35.1. Meghatározott gyakorisággal mentést készít az EIR-ben tárolt felhasználói szintű információkról, összhangban a helyreállítási időre és a helyreállítási pontokra vonatkozó célokkal.
7.35.2. Meghatározott gyakorisággal mentést készít az EIR-ben tárolt rendszerszintű információkról…
7.35.4. Megvédi a mentett információk bizalmasságát, sértetlenségét és rendelkezésre állását…"

Miért? Ha az érintett rendszerek jó mentésből, gyakorolt módon visszaállíthatók, a leállás hossza számottevően csökken.

6. **Mentések visszaállításának tesztelése**

„7.36. A szervezet meghatározott gyakorisággal teszteli a mentett információkat, az adathordozók megbízhatóságának és az információ sértetlenségének garantálása érdekében."

Miért? A tesztelt mentések biztosítják, hogy incidenskor valóban működőképes visszaállítási útvonal álljon rendelkezésre.

7. **Biztonsági események kezelése – formalizált IR**

„9.9.1. A szervezet:
9.9.2. Biztonsági eseménykezelési képességet alakít ki, amely … magában foglalja a felkészülést, az észlelést és elemzést, az elszigetelést, a felszámolást és a helyreállítást.

9.9.3. A szervezet összehangolja a biztonsági eseménykezelési tevékenységeket az üzletmenet-folytonossági tervezési tevékenységekkel."

Miért? Gyorsabb, strukturált reagálás, célzott izoláció – elkerülhető a teljes webshop- és app-leállás.

8. **Incidenskezelési terv**

„9.34. A szervezet:
9.34.1. A hatályos jogszabályoknak megfelelően kidolgozza a biztonsági esemény-kezelési tervet, amely:
9.34.1.1. A szervezet számára iránymutatást ad a biztonsági események kezelési módjaira.
9.34.1.6. Metrikákat alkalmaz a biztonsági eseménykezelési folyamatok működésének belső mérésére.
9.34.1.9. Meghatározott gyakorisággal felülvizsgálja a biztonsági eseménykezelési tervet…"

Miért? Kommunikációs és technikai forgatókönyvek előkészítése – kisebb reputációs kár, átlátható tájékoztatás.

9. **Rendszer és kommunikációvédelem – webes szolgáltatások**

„17.12. A szervezet:
17.12.1. védekezik a meghatározott szolgáltatásmegtagadással járó támadások ellen, vagy korlátozza azok hatásait; és
17.12.2. alkalmazza azokat a védelmi intézkedéseket, amelyek segítségével elérheti a szolgáltatásmegtagadással járó támadások elleni védekezés célját."

Miért? Online szolgáltatásoknál (webshop) kulcsfontosságú a szolgáltatás-kiesés elleni védelem (DDoS, alkalmazásszintű támadások).

10. **Hálózati határvédelem, publikus szolgáltatások kontrollja**

„17.17. A szervezet:
17.17.1. Ellenőrzi a kommunikációt a menedzselt külső interfészein, valamint a rendszer kulcsfontosságú menedzselt belső interfészein.
17.17.2. A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól.
17.17.3. Csak a szervezet biztonsági architektúrájával összhangban lévő határvédelmi eszközökön keresztül, menedzselt interfészek segítségével kapcsolódik külső hálózatokhoz vagy külső EIR-ekhez."

Miért? Webshop és app backend védelmére, a belső rendszerek védett szeparációjára szolgál.

5. FŐVÁROSI TÖRVÉNYSZÉK – BELSŐ FELHASZNÁLÓI SZABÁLYSZEGÉS (2025. DECEMBER)

5.1 Az incidens bemutatása

Incidens leírása: A Fővárosi Törvényszék tájékoztatása szerint az informatikai rendszerben észlelt biztonsági jelzések nem külső, célzott kibertámadásból eredtek, hanem egy belső felhasználói szintű szabályszegési kísérletből. A jogosulatlan eszközhasználatra utaló próbálkozást a védelmi rendszerek azonnal észlelték és blokkolták, és a közlés szerint sem az adatok, sem a rendszerintegritás nem sérült.

Incidens típusa: Belső fenyegetés / szabályszegés / jogosulatlan hozzáférési vagy eszközhasználati kísérlet.

Okozott veszteségek:

- Vizsgálati és adminisztratív teher (biztonsági kivizsgálás, dokumentálás, HR/felelősségre vonás).
- Bizalmi kockázat és fokozott figyelem a szervezeti kiberbiztonsági felkészültsége iránt, még tényleges adatvesztés nélkül is.
- A kontrollok finomhangolásának és a szabályozás betartatásának költsége (pl.: hardening, oktatás, eszközcsere).
- Esetleges pótlólagos, nem tervezett IT beszerzések, amelyek szükségességére az incidens rámutathatott

Hogyan lett volna megelőzhető az incidens:

- Az elavult eszköz és szoftver állomány időben történő cseréje
- A belső szabályok megsértéséhez kapcsolódó következményeket és ellenőrzéseket egyértelműen kommunikálni kellett volna, rendszeres tudatosító képzéssel megtámogatva.
- Kiemelt rendszerekben javasolt többtényezős hitelesítést alkalmazni.

Tanulságok: A belső szabályszegésből eredő incidensek ugyanúgy reputációs és megfelelési kockázatot jelentenek, mint a külső támadások. A gyors detektálás és blokkolás jó kontrollérettséget jelez, de az eset rávilágít arra, hogy az eszköz- és hozzáférés-kezelés folyamatosan karbantartandó, másrészt hogy a kiberbiztonsági területen a szabályozás folyamatos naprakészen tartása (pl.: jelszavak kezelése), illetve azoknak az oktatása, ellenőrzése és betartatása kiemelt fontosságú.

5.2 Javasolt 7/2024 MK követelmények

1. **Viselkedési szabályok és kötelező nyilatkozat**

   „13.3.1. A szervezet megfogalmazza és a szervezetre érvényes követelmények szerint dokumentálja, valamint a szervezeten belül kihirdeti az EIR-hez hozzáférési jogosultságot igénylő személyekkel, felhasználókkal szembeni elvárásokat, a rájuk vonatkozó szabályokat, felelősségüket, az adott rendszerhez kapcsolódó kötelezően elvárt vagy tiltott tevékenységet.

13.3.2. A szervezet az EIR-hez való hozzáférés engedélyezése előtt dokumentált nyilatkozattételre kötelezi a hozzáférési jogosultságot igénylő személyt…"

Miért? Egyértelműen rögzíti, mi minősül szabályszegésnek (pl. jogosulatlan eszközhasználat), és erről a felhasználó írásban nyilatkozik.

2. **Személyi biztonsági szabályzat**

„14.1. A szervezet:
14.1.1. Kidolgozza, dokumentálja, kiadja és megismerteti … a személyi biztonságra vonatkozó szabályzatot…"

Miért? A munkavállalók magatartási normáinak, felelősségének, következményeknek kereteit rögzíti.

3. **Munkakörök biztonsági besorolása**

„14.2. A szervezet:
14.2.1. minden szervezeti munkakörhöz hozzárendel egy kockázati besorolást;
14.2.2. átvilágítási kritériumokat állít fel a munkaköröket betöltő egyének számára…"

Miért? Kritikus bírói / adminisztratív munkaköröknél erősebb előzetes ellenőrzés, ha nagy a visszaélési potenciál.

4. **Hozzáférési megállapodások**

„14.9. A szervezet:
14.9.1. Kidolgozza és dokumentálja a szervezeti EIR-ekhez való hozzáférés szabályait.
14.9.3. Ellenőrzi, hogy a szervezeti információkhoz és rendszerekhez hozzáférést igénylő személyek … megismerték és dokumentált módon elfogadták a vonatkozó hozzáférési szabályokat…"
Miért? A felhasználókat szerződésszerűen köti az előírásokhoz, csökkentve a „nem tudtam" típusú kifogásokat.

5. **Legkisebb jogosultság elve**

„2.60. A szervezet a legkisebb jogosultság elvét alkalmazza, és a felhasználók … számára csak a számukra kijelölt feladatok végrehajtásához szükséges hozzáféréseket engedélyezi."

Miért? Ha a szabályszegő fiókja limitált, a károkozási potenciál is csekélyebb.

2.69. Legkisebb jogosultság elve – Privilegizált funkciók használatának naplózása
„2.69. Az EIR naplózza a privilegizált funkciók végrehajtását."

Miért? Részletes audit trail belső visszaélések bizonyítására, gyorsabb reagálásra.

7. **Felelősségek szétválasztása**

   „2.59. A szervezet:
   2.59.1. azonosítja és dokumentálja azokat a meghatározott feladatokat, amelyeket az egyéneknek elkülönített módon kell ellátniuk; és
   2.59.2. meghatározza az EIR hozzáférési jogosultságait annak érdekében, hogy támogassa a feladatok szétválasztását.”

Miért? Ne egyetlen személy kontrolláljon teljes folyamatokat, csökkentve a belső visszaélés kockázatát.

8. **Személyek munkaviszonyának megszűnése – hozzáférés visszavonása**

   „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.”
   Miért? Ha a „szabályszegő” már kilépéshez közeli, a gyors hozzáférés-megszüntetés megelőzheti az incidenset.

9. **Fizikai belépés ellenőrzése**

   „12.6. A szervezet:
   12.6.1. Kizárólag a szervezet által meghatározott be- és kilépési pontokon biztosítja a belépésre jogosultak számára a fizikai belépést.
   12.6.2. Naplózza a fizikai be- illetve kilépéseket.”

Miért? Jogosulatlan eszköz bevitelének / használatának megelőzésére a bírói, irattári, rendszertermekben.

10. **Biztonsági személyzet képzése, tudatosság**

    „3.2. A szervezet:
    3.2.1. Biztonságtudatossági képzést biztosít a rendszer felhasználói számára …
    3.2.4. Integrálja a belső és külső biztonsági eseményekből levont tanulságokat a képzési anyagokba…”

Miért? A szabályszegés kockázatainak ismertetése, következmények tudatosítása.

6. ÖNKORMÁNYZATI ÉS ÁLLAMI CÉLPONTOK, MALWARE-TERJESZTÉS (2024 ŐSZ; RENDŐRSÉGI KÖZLÉS 2025. SZEPTEMBER)

6.1 Az incidens bemutatása

Incidens leírása: A rendőrségi közlés szerint 2024 októberében egy ismeretlen elkövető jogosulatlanul hozzáfért egy polgármesteri hivatal informatikai rendszeréhez, egy alkalmazott hitelesítő adatainak felhasználásával, és a szerveren tárolt adatok egy részét letöltötte. 2024 novemberében egy állami szervezet e-mail rendszerében történt jogosulatlan hozzáférés, majd több száz címzettnek malware-t tartalmazó mellékletet küldtek; a melléklet megnyitásával az elkövető hozzáférhetett a fertőzött gép adataihoz. A nyomozás alapján 2025 szeptemberében egy 15 éves gyanúsítottat fogtak el.

Incidens típusa: Hitelesítőadat-kompromittálás; jogosulatlan hozzáférés; e-mail alapú malware-terjesztés

Okozott, illetve lehetséges veszteségek:

- Önkormányzati adatok kiszivárgása
- Tömeges fertőzési kockázat és lehetséges adatvesztés több száz címzettnél a kártékony kódot tartalmazó melléklet miatt.
- Helyreállítási és incidenskezelési költségek (önkormányzati hálózat vizsgálata, kormányzati szerv hálózatának vizsgálata, kártékony kódok kezelése, incidensek kivizsgálása és kezelése, soron kívüli biztonsági és üzemeltetési feladatok elvégzése).
- Bizalmi és megfelelési kockázat közszférában, nagy nyilvánosság előtt

Hogyan lett volna megelőzhető az incidens:

- Webes szolgáltatások esetében javasolt volna mindenütt (például e-mail és távoli hozzáférések esetén) többtényezős hitelesítést alkalmazni.
- A szerzvezetek hálózaton elérhető erőforrásainak használatát (szerverek, szolgáltatások) javasolt a legkisebb jogosultság elvének figyelembe vételével korlátozni.
- A meg nem nevezett kormányzati szerv esetében nyilvánvaló hiányosság, hogy a e-mail szolgáltatás nem megfelelően volt beállítva, hiszen tömegesen, kártékony kódot tartalmazó levelet lehetett küldeni. Levelező szolgáltatás esetében mind a tömeges küldés, mind a kártékony kódok ellen védekezni szükséges. Ugyanígy vélhetően az adott rendszer végpontvédelmi megoldása is hiányos volt, hiszen az sem szűrte ki a kártékony kódot tartalmazó fájlt.

Tanulságok: Az eset rávilágít, hogy a támadási küszöb alacsony: akár fiatal elkövetők is képesek szervezeteket kompromittálni, ha a például a jelszavas hitelesítés és az e-mail, valamint a végpont védelem gyenge.

6.2 Javasolt 7/2024 MK követelmények

1. **Azonosítás és hitelesítés – MFA kritikus fiókokra**

8.3. Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése
(lásd fent)

Miért? Polgármesteri hivatal / állami szervezet O365/levelezés, VPN, admin fiókok MFA-val védve – jelszólopással nehezebb jogosulatlan hozzáférést szerezni.

2. **Legkisebb jogosultság és jogosultság-felülvizsgálat**

2.60. Legkisebb jogosultság elve
(lásd fent)

> *„2.67. A szervezet:*
> *2.67.1. Meghatározott időközönként felülvizsgálja a szerepkörök vagy felhasználói csoportok által hozzáférhető jogosultságokat…*
> *2.67.2. Amennyiben szükséges, elvégzi a jogosultságok újra osztását vagy megszüntetését…”*

Miért? Egy kompromittált fiók kevesebb rendszerhez fér, így korlátozottabb kárt okoz.

3. **Végpontvédelem, malware elleni védelem**

18.8. Kártékony kódok elleni védelem
(lásd fent)

Miért? A levelek mellékleteinek lokális detektálása, karanténozása csökkenti a fertőzések számát.

4. **Kéretlen üzenetek elleni védelem**

> *„18.56. A szervezet:*
> *18.56.1. olyan levélszemét elleni védelmet valósít meg az EIR belépési és kilépési pontjain, amelyek felismerik és kezelik az ilyen üzeneteket; és*
> *18.56.2. új verziók elérhetővé válásakor frissíti a levélszemét elleni védelmi mechanizmusokat…”*

Miért? Spam/phishing filterekkel szűrni a malware-t tartalmazó e-maileket.

5. **E-mail biztonsági kontrollok – forgalom monitorozása**

> *„18.17. A szervezet:*
> *18.17.1. … kritériumokat állít fel a szokatlan vagy nem engedélyezett tevékenységek és körülmények azonosítására.*
> *18.17.2. Meghatározott időközönként ellenőrzi a bejövő és kimenő kommunikációs forgalmat…”*

Miért? Tömeges, azonos tárgyú/URL-es kimenő levelek észlelése, riasztás.

6. **Sikertelen bejelentkezési kísérletek kezelése**

> *„2.71. A szervezet:*
> *2.71.1. … korlátot alkalmazza a felhasználó … sikertelen bejelentkezési kísérletei-*

re.
2.71.2. EIR-je automatikusan zárolja a felhasználói fiókot…”

Miért? Brute-force jelszótámadások megnehezítése a felhasználói/levelezési fiókok ellen.

7. **Információszivárgás figyelése**

„4.44. A szervezet:
4.44.1. Rendszeresen figyelemmel kíséri a meghatározott nyílt forrású információkat vagy információs oldalakat a szervezeti információk jogosulatlan nyilvánosságra hozatalának bizonyítékaiért.”

Miért? Ha a letöltött önkormányzati adatok megjelennek nyílt forrásban, gyorsabb a reagálás.

8. **Incidenskezelés és jelentés**

„9.27. A szervezet:
9.27.1. Kötelezi a személyzetet arra, hogy jelentse a biztonsági esemény gyanúját vagy bekövetkeztét.
9.27.2. Jogszabályban meghatározottak szerint jelenti a biztonsági eseményekre vonatkozó információkat a jogszabályban meghatározott szervek felé.”

Miért? Hatósági, CSIRT-irányba történő gyors jelzés, koordinált válasz.

9. **Biztonságtudatossági képzés – phishing / social engineering**

„3.5. A szervezet felkészítő képzést nyújt a pszichológiai manipuláció és adatgyűjtés lehetséges és valós jeleinek felismerésére…”

Miért? A mellékletek megnyitása, adathalász üzenetek felismerése elsősorban emberi tényezőn múlik.

10. **Ellátási lánc kockázatkezelése e-mail szolgáltatóknál**

„19.7. A szervezet gondoskodik arról, hogy … információbiztonsági követelményeket a fővállalkozó által igénybe vett alvállalkozók szerződései is tartalmazzák.”

Miért? Ha külső e-mail-szolgáltatót használnak, szerződésben kell rögzíteni a szükséges security funkciókat (spam/malware-szűrés, DMARC, stb.).

---

7. UNIX AUTÓ – ZSAROLÓVÍRUS MIATTI MŰKÖDÉSLEÁLLÁS (2021. MÁRCIUS 30.)

7.1 Az incidens bemutatása

Incidens leírása: A vállalat tájékoztatása szerint 2021. március 30-án zsarolóvírus támadás érte informatikai rendszereiket. A beszámoló alapján a támadás gyorsan terjedt, rövid időn belül nagyszámú szerver és munkaállomás vált használhatatlanná, és a cégcsoport működése napokra teljesen leállt és hetekig voltak zavarok: üzletek és partnerek ellátása, logisztikai problémák

Incidens típusa: Zsarolóvírus (ransomware), adatvesztés (lehetséges adat szivárgás), rendszer leállás

Okozott veszteségek:

- Teljes működés leállás, illetve működési zavarok: rendelésfelvétel, kiszállítás, ügyfélszolgálat és üzletek működésének szünetelése, partnerek kiszolgálása.
- Jelentős bevételkiesés és partneri szerződéses kockázat a szolgáltatások kiesése miatt.
- Helyreállítási és újjáépítési költségek: incidens kivizsgálás és kezelés, jelentős IT beszerzési költségek, belső és külső szakértők jelentős mennyiségű munkája
- Adatvesztés és esetleges adatszivárgás kockázata
- Bizalom sérülése a partnerek és ügyfelek körében, nagy nyilvánosság előtt

Hogyan lett volna megelőzhető az incidens, illetve hatás csökkentése:

- Zsarolóvírus támadások hatásának jelentős csökkentésének alapvető feltétele (az offline) biztonsági mentések megléte (üzleti, pénzügyi adatokról, valamint a szükséges IT rendszer adatokról is), illetve a visszaállítási folyamatok rendszeresen, éles tesztekkel történő validációja.
- A belső hálózaton is javasolt szigorú szegmentálás, a kártékony kód terjedésének akadályozása miatt.
- Vélhetően a végpontvédelem nem volt megfelelő, hiszen nem volt képes hatékonyan megállítani a vírus terjedését. A naprakész, korszerű végpontvédelem (szerver oldalon is) manapság alapszükséglet.
- Tekintettel arra, hogy a zsarolóvírusok sokszor ismert, de nem javított sérülékenységeket használnak ki a rendszerek kompromittálásra, így kiemelten figyelmet kell fordítani az rendszerek karbantartására: a sérülékenység- és patch menedzsmentet folyamatosan végezni kell, különös tekintettel a távoli elérést biztosító komponensekre.
- Számos hibát fel lehet deríteni és ki lehet küszöbölni rendszeres professzionális internet felőli és belső hálózaton történő sérülékenység vizsgálat elvégzésével. Ezek a vizsgálatok műszakilag megegyeznek egy kibertámadással, így ezzel vizsgálható, hogy a szervezet mennyire kitett egy ilyen helyzetben. Ezen vizsgálatok elvégzése rendszeresen javasolt.

Tanulságok: A zsarolóvírus-incidensek percek alatt teljes vállalati leállást okozhatnak. Az a szervezet, aki úgy ítéli meg a kockázatelemzésében, hogy egy ilyen incidens komoly kárt okozhat neki, annak mindenképpen szükséges komolyan felkészülni egy ilyen helyzetre, természetesen a kockázatarányos védelem elvét figyelembe véve. Ha a szervezet a példához hasonlóan akár 100 millió forintos nagyságrendben veszíthet bevételt, úgy belátható, hogy a védekezésre is komolyabb

erőforrásokat kell rászánnia. Még így is biztos lehet abban, hogy egy valódi incidenssel sokkal többet veszítene.

7.2 Javasolt 7/2024 MK követelmények

1. **Biztonsági mentések**

7.35. Az elektronikus információs rendszer mentései
(lásd fent)

Miért? Offline, elkülönített mentésekből újraépíthető a környezet.

2. **Mentések tesztelése**

7.36. Az elektronikus információs rendszer mentései – Megbízhatóság és sértetlenség tesztelése
(lásd fent)

> *Miért? Rendszeres visszaállítási tesztek nélkül a mentés „feltételezés" marad.*

3. **Hálózati szegmentáció**

> *„17.17.2. A nyilvánosan hozzáférhető rendszerelemeket fizikailag vagy logikailag alhálózatokban helyezi el, elkülönítve a belső szervezeti hálózattól."*

Miért? Belső VLAN-ok, szegmensek, AD-szerepkörök – ne terjedjen végig egyetlen ransomware hullámban.

4. **Zsarolóvírus elleni védelem – malware control**

18.8. Kártékony kódok elleni védelem
(lásd fent)

Miért? Korszerű EDR/XDR, szerveroldali védelem, macro/skript blokkolás.

5. **Sérülékenység- és patch-menedzsment**

> *„18.2. A szervezet:*
> *18.2.3. A biztonsági szempontból releváns szoftver- és firmware-frissítéseket a frissítések kiadását követő meghatározott időtartamon belül telepíti."*

Miért? A ransomware-k nagy része ismert, javított sérülékenységeket használ.

6. **Folyamatos felügyelet / monitoring**

5.15. Folyamatos felügyelet
(lásd fent)

Miért? Szokatlan titkosítási aktivitás, nagyszámú fájl-módosítás korai felismerése.

7. **Behatolásvizsgálat**

„5.21. A szervezet behatolásvizsgálatot végez a szervezet által meghatározott gyakorisággal…”

Miért? Tavasszal végzett pentest rávilágíthatott volna a legkritikusabb bejutási pontokra.

8. **Üzletmenet-folytonosság, DR**

7.2. Üzletmenet-folytonossági terv
(lásd fent)

Miért? Kritikus logisztikai, értékesítési rendszerek BCP nélkül „minden vagy semmi” jelleggel állnak le.

9. **Üzletmenet-folytonossági terv tesztelése**

7.13. Üzletmenet-folytonossági terv tesztelése
(lásd fent)

Miért? Gyakorlott failover/restore = rövidebb kiesési idő.

10. **Kockázatelemzés – ransomware-szcenárió beemelése**

5.1. KOCKÁZATELEMZÉS ÉS A KOCKÁZATOK KEZELÉSE
(lásd fent)

Miért? Ha a kockázat „kritikus” kategóriába kerül, arányos, erős kontroll-portfólió szükséges.

8. SASSZEM KLINIKA – KÜLSŐ KIBERTÁMADÁS ÉS ZSAROLÓVÍRUS-ÁLLÍTÁSOK (2025. ÁPRILIS)

8.1 Az incidens bemutatása

Incidens leírása: A sajtóban 2025 áprilisában jelent meg, hogy egy zsarolóvírus-csoport (Qilin) támadást állított a Sasszemklinika ellen és váltságdíjat követelt. A klinika közlése szerint külső kibertámadás érte őket, és a rendelkezésre álló információk alapján illetéktelenek bizonyos digitális adatfájlokhoz hozzáférhettek (ezek egy jórésze a hírek szerint meg is jelent a dark weben, köztük személyes és egészségügyi adatok). A kivizsgálást kiberbiztonsági szakértőkkel megkezdték. A hírek szerint az incidenst akkor jelentette a szervezet a NAIH felé, amikor az incidens híre kitudódott az interneten, másrészt az érintetek tájékoztatását is ekkor kezdte meg. A betegellátás és az időpontfoglalás működőképes maradt.

Incidens típusa: Feltételezett zsarolóvírus / adatlopás (kettős zsarolás) kockázatával.

Okozott és lehetséges veszteségek:

- Különleges adatok (egészségügyi adatok) érintettségének kockázata, ami kiemelt adatvédelmi következményekkel járhat.
- Zsarolási és nyilvánosságra hozatali kockázat (adatok publikálása) még akkor is, ha az ellátás működőképes marad.
- Kivizsgálási, incidenskezelési és megfelelési költségek
- Reputációs kár és bizalomvesztés a páciensek körében.

Hogyan lett volna megelőzhető az incidens:

- A betegadatokat tartalmazó rendszereket szigorúan szegmentálni szükséges.
- Az adminisztratív, illetve magas jogosultságú (illetve különleges személyes adatokhoz való) hozzáféréseket javasolt többfaktoros hitelesítéssel biztosítani.
- Vélhetően a végpontvédelem nem volt megfelelő, hiszen nem volt képes hatékonyan megállítani a vírus terjedését. A naprakész, korszerű végpontvédelem (szerver oldalon is) manapság alapszükséglet.
- Tekintettel arra, hogy a zsarolóvírusok sokszor ismert, de nem javított sérülékenységeket használnak ki a rendszerek kompromittálásra, így kiemelten figyelmet kell fordítani az rendszerek karbantartására: a sérülékenység- és patch menedzsmentet folyamatosan végezni kell, különös tekintettel a távoli elérést biztosító komponensekre.
- Ebben az esetben is javasolt lett volna rendszeres, professzionális internet felőli és belső hálózaton történő sérülékenység vizsgálat elvégzése és az esetlegesen talált hiányosságok javítása.
- Az szervezetnek alaposabb incidenskezelési eljárást kellett volna készíteni és azt rendszeresen tesztelni, hogy adott helyzetben a károk gyorsabban mérsékelhetők legyenek, illetve a bekövetkezett eseményt a szervezet jobban tudja kezelni, mind IT, mind adatvédelem, mind kommunikációs szempontól.

Tanulságok: Tanulmányok szerint az egészségügyi adatok az egyik legértékesebb célpont a támadók számára, mivel azok értéke mind a szervezetnek, mind az érintettek számára nagy. A zsarolóvírusok esetében nem csak a szolgáltatások, illetve az adatok elérhetőségének az akadályozása a támadási irány, hanem – mivel a támadás során nagy jogosultságot szereznek a rendszer felett – az adatok ellopásából adódóan további zsarolási potenciáljuk keletkezik. A zsarolóvírus támadások elleni megelőző védekezést nagyon komolyan kell venni!

8.2 Javasolt 7/2024 MK követelmények

1. **Adattároló rendszerek szigorú szegmentálása**

17.17. A határok védelme
(lásd fent)

Miért? Betegadatokat tartalmazó EHR/PACS rendszerek elkülönítése a „mezei” kliensektől, internet felé néző zónáktól.

2. **Tárolt adatok védelme (encrypt-at-rest)**

„17.81. A szervezet megóvja a meghatározott tárolt, illetve archivált (at rest) adatok bizalmasságát és sértetlenségét…”
„17.82. A szervezet meghatározott rendszerelemek vagy adathordozók esetében kriptográfiai mechanizmusokat alkalmaz…”

Miért? Lopás esetén is csökkenti az adat kiolvashatóságát (különösen légszoros kulcs-kezeléssel).

3. **MFA az admin / különleges adatokhoz férő fiókokra**

8.3. Azonosítás és hitelesítés (felhasználók) – Privilegizált fiókok többtényezős hitelesítése

Miért? Egészségügyi rendszerek adminfiókjai tipikusan célpontok zsarolóbandáknál.

4. **Kártékony kódok elleni védelem**

18.8. Kártékony kódok elleni védelem

Miért? Klinikai munkaállomások és szerverek védelme zsarolóvírus ellen (makró, RDP-brute, exploit stb.).

5. **Sérülékenység- és patch-menedzsment**

15.9. Sérülékenységek ellenőrzése
18.2. Hibajavítás

Miért? Különösen fontos az internetre kinyitott időpontfoglaló portál, VPN, mail-gateway javítottsága.

6. **Biztonsági mentések (offline is)**

7.35. Az elektronikus információs rendszer mentései

Miért? Betegadatok titkosítása esetén is visszaállítható legyen a rendszer.

7. **Mentések offline/külön helyszínen**

„7.38. A szervezet … mentéseit az elsődleges feldolgozási helyszíntől elkülönített létesítményben vagy egy tűzbiztos tárolóban tárolja.”

Miért? Ransomware ne tudja a mentést is titkosítani.

8. **Incidenskezelés (IT + adatvédelmi fókusz)**

9.9. Biztonsági események kezelése
9.34. Biztonsági eseménykezelési terv

Miért? Időben történő NAIH-bejelentés, érintett-tájékoztatás, kommunikációs terv.

9. **Biztonságtudatossági képzés egészségügyi környezetben**

„3.4. A szervezet felkészítő képzést nyújt a belső fenyegetések potenciális jeleinek felismerésére és jelentésére.”

Miért? Belső visszaélés, social engineering, zsarolóvírusos csatolmányok felismerése.

10. **Kockázatmenedzsment – különleges adatokra fókuszálva**

„1.10. A szervezet:
1.10.1. Kidolgoz egy átfogó stratégiát, amely kezeli:
1.10.1.2. Személyes adatok kezeléséből fakadó kockázatokat.”

Miért? Egészségügyi adatok különlegesen védendők, a stratégia erre külön kockázati súlyt rendel.

9. ÖSSZEFOGLALÓ INTÉZKEDÉSI TÁBLÁZAT

A „✓” jel azt mutatja, hogy az adott kontroll az adott incidens megelőzésében vagy hatáscsökkentésében kiemelten fontos lehetett (volna).

Megjegyzés: a „✓” jel a kiemelt relevanciát jelöli, de a kontrollok egymást erősítik, és rendszerként működnek.

Intézkedés (8–10 pont)	SECTOR 16	Rossmann	Fővárosi Törvényszék	Önkormányzati és állami célpontok, malware-terjesztés	UNIX Autóalkatrész kereskedő	Sasszem klinika
Kötelező többfaktoros autentikáció minden kritikus / fontos fiókra (levelezés, VPN, admin, felhő, különleges adatok).	✓		✓	✓	✓	✓
Zero Trust-alapú hozzáférés: legkisebb jogosultság + rendszeres jogosultság-felülvizsgálat.	✓	✓	✓	✓	✓	✓
Hálózati szegmentáció (különösen OT/ICS környezetben: IT–OT szeparáció, DMZ, ugróhost).	✓	✓	✓	✓	✓	✓
Naprakész végpontvédelem, mind kliens, mind szerver oldalon	✓	✓		✓	✓	✓
Normál és offline biztonsági mentések végzése, rendszeres visszaállítási teszttel.		✓		✓	✓	✓
Sérülékenység-menedzsment: folyamatos patching, internetre néző rendszerek priorizálásával.	✓	✓	✓	✓	✓	✓
Rendszeres penetrációs teszt és biztonsági audit (külön web/app/API rendszerekre).	✓	✓		✓	✓	✓
E-mail biztonsági kontrollok: DKIM, csatolmány- és URL-szűrés.				✓		
Eszköz- és alkalmazáskontroll: whitelist, jogosulatlan eszközhasználat tiltása/riasztása.	✓			✓	✓	
Privileged Access Management (PAM)	✓				✓	
Incidenskezelési terv és gyakorlatok	✓	✓	✓	✓	✓	✓

Üzletmenet-folytonosság és katasztrófa-helyreállítás (BCP/DR). Eljárások és rendszeres tesztelésük		✓	✓	✓
Adatminimalizálás minden adatkezelésnél. *„privacy by design” minden új terméknél/ appnál.*				
Biztonsági alapkonfigurációk (hardening baseline) és megfelelőségi ellenőrzés (CIS benchmark jelleggel) minden szerveren és végponton.	✓		✓	