Adatmentési stratégiák a NIS2 tükrében (is)

SZÉCHENYI ISTVÁN EGYETEM, GYŐR
Dr. Kovács Ákos
EIVOK-52
2024.11.13

NIS2

- A társadalom digitális átalakulása kibővítette a kiberfenyegetettségi környezetet. Új kihívások jelentek meg, amelyek alkalmazkodó és innovatív válaszokat igényelnek. Erre reagálva az Európai Parlament és az Európai Unió Tanácsa **2022. december 27**-én közzétette a NIS2 irányelvet, ami **2023. január 16**-án lépett hatályba.

- A NIS2 direktíva számos követelményt fogalmaz meg az EU-tagállamok kiber- és információbiztonságára vonatkozóan. Magyarországon a „2023. évi XXIII. törvény a kiberbiztonsági tanúsításról és a kiberbiztonsági felügyeletről” tisztázza a nemzeti kiberbiztonsági tanúsítás és felügyelet alapvető kérdéseit, illetve implementálja az EU-s NIS2 direktíva rendelkezéseit.

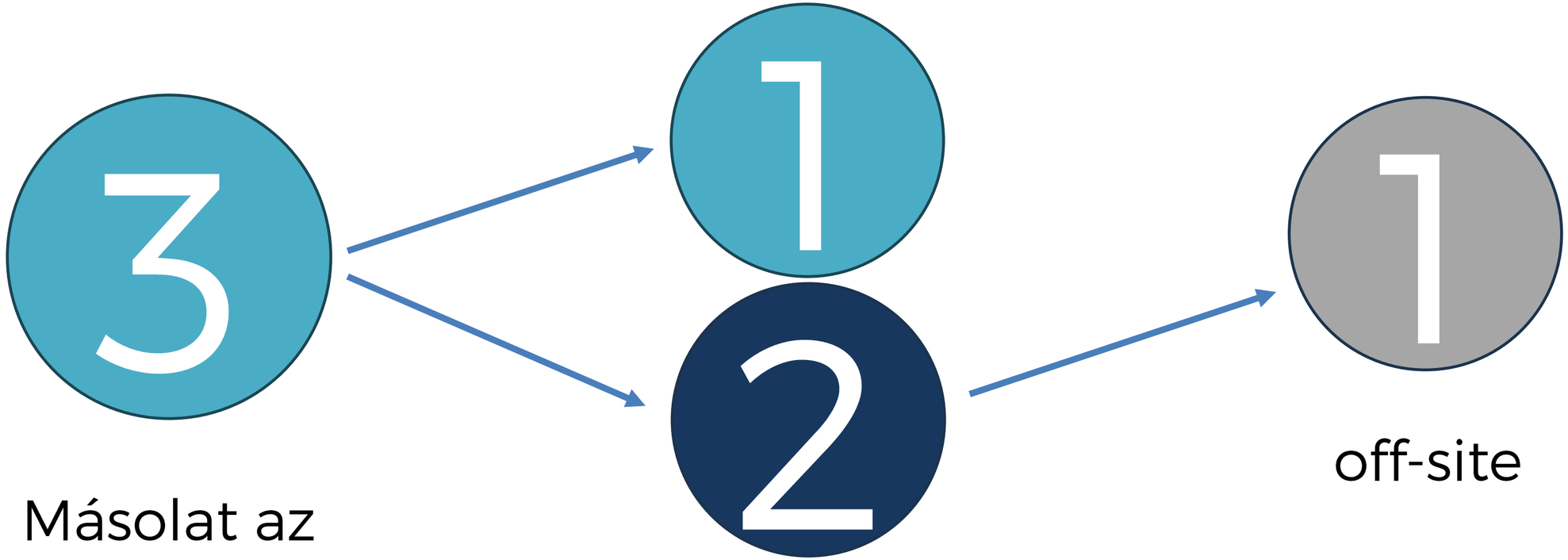
NIS2 - a gyakorlatban

- incidens esetén, 24 órán belüli első értesítési kötelezettség a hatóságok felé
- 72 órán belül esemény-bejelentési kötelezettség
- **informatikai biztonsági szabályzat kidolgozása (IBSZ)**
- ellátási lánc biztonságának biztosítása
- incidensekre való reagálási terv kidolgozása
- 1 hónapon belüli zárójelentés kötelezettség
- információbiztonságért felelős személyt kell kijelölni
- **katasztrófa utáni helyreállítási terv kidolgozása**

- stb stb...

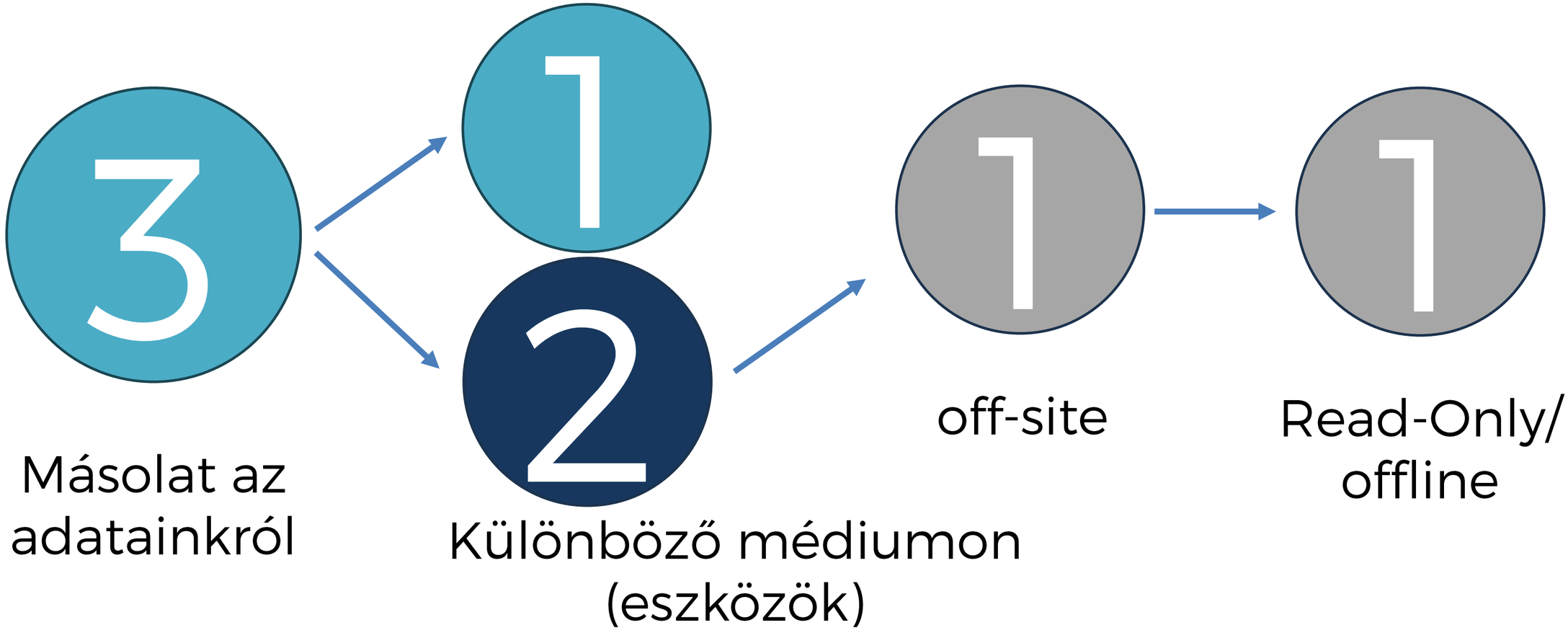
NIS2 – Mentési stratégiák

- Vicces módon nem IT iparból jött alapelvek
- Peter Krogh amerikai fotós nevéhez fűződik a 3-2-1 szabály, mely azóta az alapja a mentési stratégiáknak. (2005)



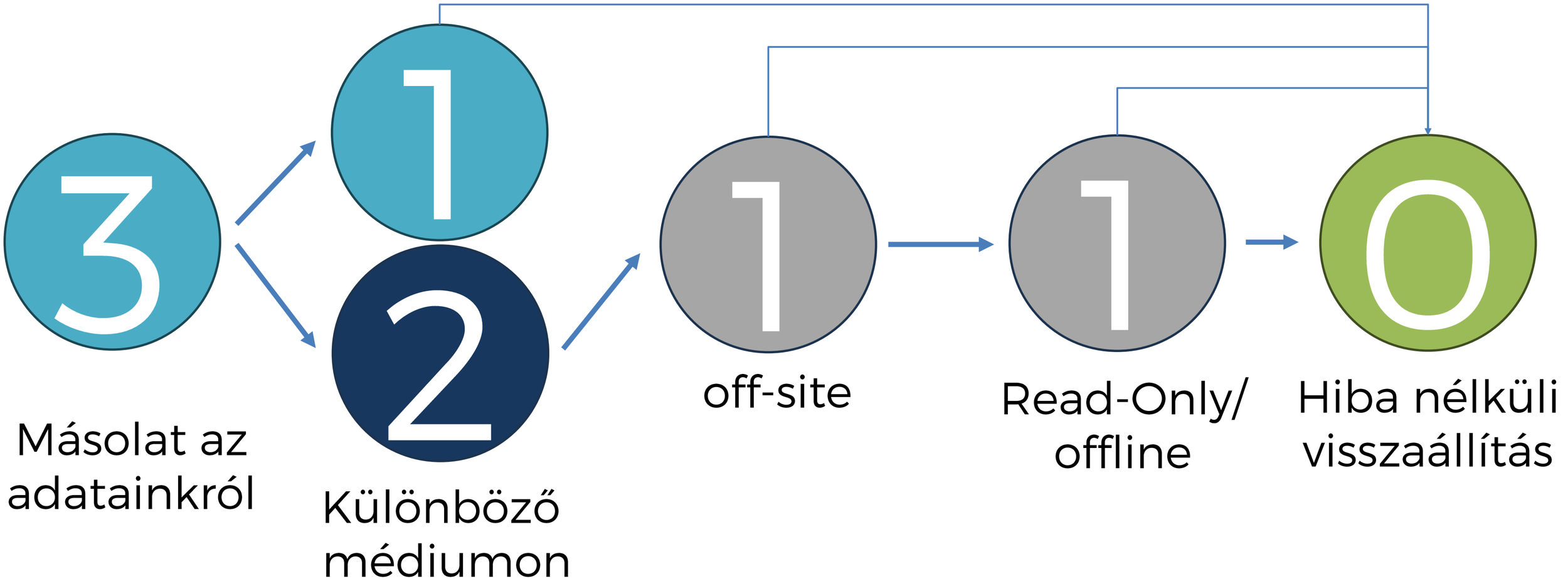
NIS2 – Mentési stratégiák 2

- Ransomware-ek betörésével ki kellett egészíteni
- Egy olyan másolattal, mely nem módosítható így nem támadható
- Az IDC ajánlása a felhőben tárolt – Magyarországon tipikusan egy USB Winchester



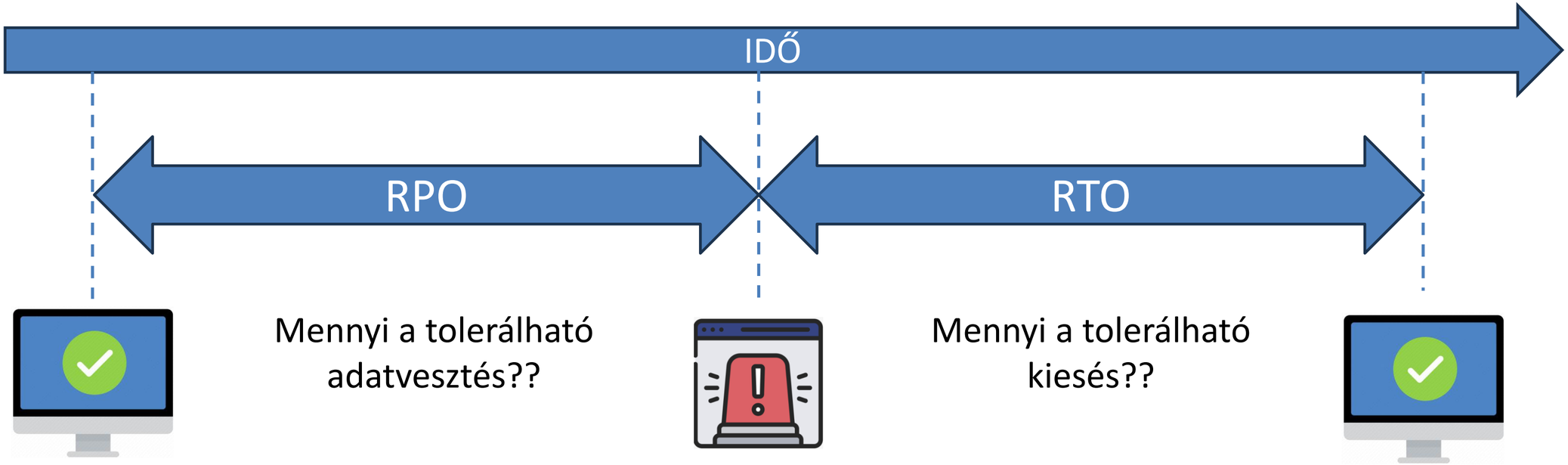
NIS2 – Mentési stratégiák 3

- A adatok integritása érdekében plusz egy lépés (3-2-1-1-0 Golden Rule)
- Visszaellenőrzés - > 0 hibával



NIS2 – Mentési stratégiák 4

- RTO és RPO meghatározása
  - RPO: Recovery Point Objective - azaz mennyi adatvesztést engedünk meg
  - RTO: Recovery Time Objective - azaz mennyi idő alatt tudjuk helyreállítani a rendszert



NIS2 – GFS

- GFS Grandfather – Father – Son
- Időszakos hosszútávú mentések kidolgozása
- Automatizálás – értesítések definiálása

Son	Father	Grandfather
napi (inkrementális)	Heti (teljes)	Havi (teljes)

NIS2 – a mentések fontossága

- **Incidensjelentés:** A NIS2 előírja a szervezetek számára, hogy a jelentős incidenseket 24 órán belül jelenteniük kell. Ha megbízható biztonsági mentési rendszerrel rendelkezik, gyorsan felmérheti az incidens hatását, és pontos jelentéseket készíthet.

- **Kockázatkezelés:** A rendszeres biztonsági mentések a kockázatcsökkentés kulcsfontosságú részét képezik. Ezek biztosítják, hogy a legrosszabb forgatókönyvek esetén is vissza tudja állítani adatait és rendszereit.

NIS2 – a mentések kapcsolata

•**Üzletmenet-folytonosság:** Kibertámadás esetén a rendszerek és adatok gyors helyreállításának képessége jelentheti a különbséget egy kisebb fennakadás és egy nagyobb válság között.

•**Ellátási lánc biztonsága:** A NIS2 hangsúlyozza a biztonság fontosságát az ellátási lánc egészében. A biztonsági mentési stratégiájának tartalmaznia kell a harmadik fél szolgáltatókkal megosztott vagy általuk kezelt adatok védelmére vonatkozó terveket.

Az irányelv kifejezetten előírja a szervezeteknek, hogy gondoskodjanak a teljes adatellátási lánc biztonságáról, beleértve az adatmentési szolgáltatók gondos átvilágítását is.

NIS2 – Elégséges

- Minél több mentés annál jobb ☺
- Legalább 2 mentés az élő adatról (3)
- Ennek egyike legalább másik épületben (felhő előfizetés) (2)
- Havonta 1x és Évente 1x offline mentés (1-1-0)
  - (lehetőség szerint külön adathordozón)

- Dokumentálás!!

Köszönöm a figyelmet!

Dr. Kovács Ákos
kovacs.akos@ddc.sze.hu