NEMZETI KÖZSZOLGÁLATI EGYETEM
LUDOVIKA

Ellátási láncok információbiztonsági vetülete

Magyar Sándor

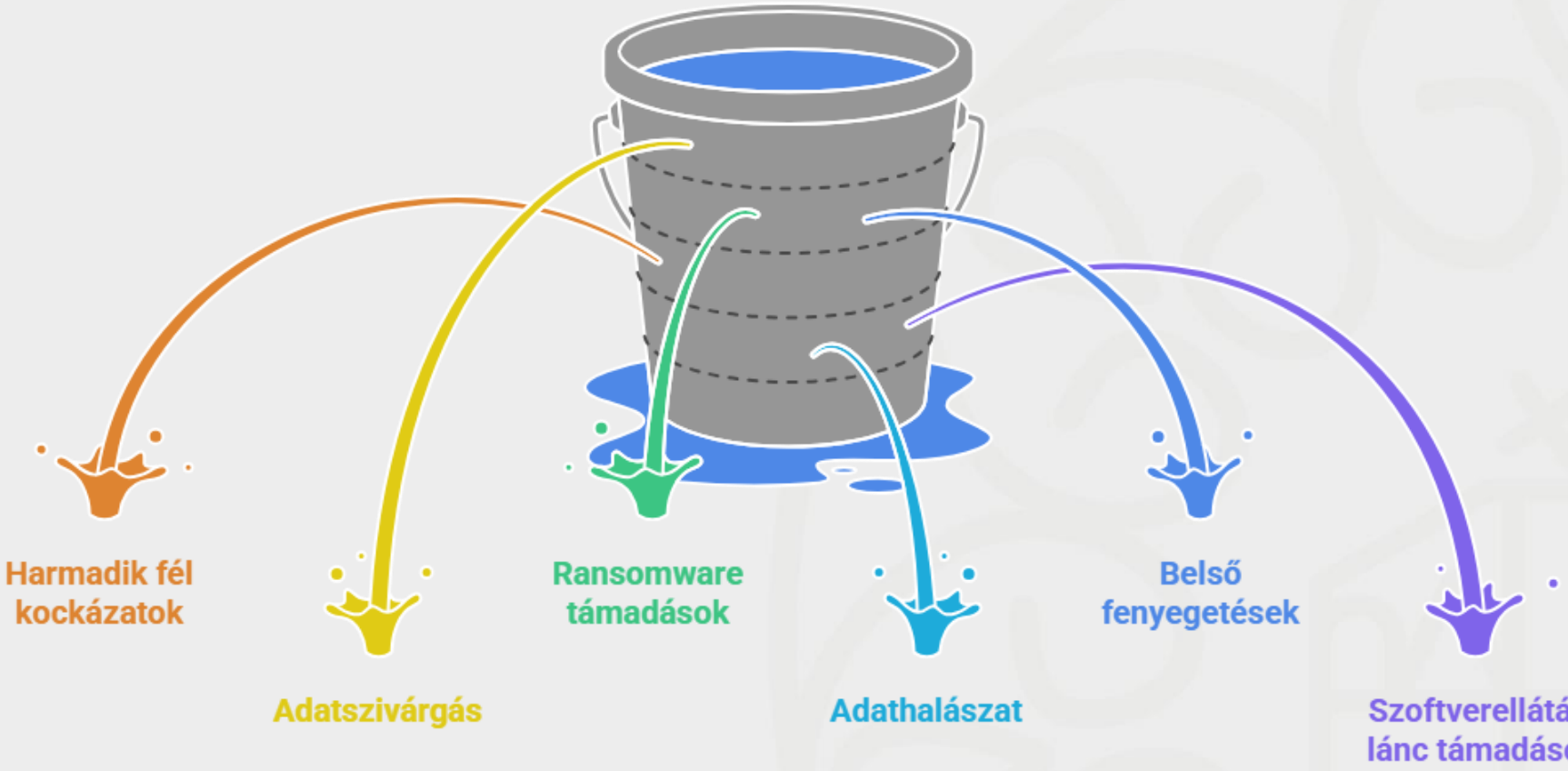
Bevezetés

- Az ellátási láncok digitalizációja.
- A beszállítói hálózatok összetettsége miatt a leggyengébb láncszem elve különösen érvényesül.
- Adatmegosztás és integráció kulcsfontosságú, ugyanakkor sérülékeny pont a partnerek közötti együttműködésben.
- Kibertámadások következményei már nemcsak informatikai, hanem logisztikai, gazdasági és reputációs szinten is megjelennek.
- Nemzetközi szabályozások (pl. NIS2, ISO 28000) új követelményeket támasztanak az ellátási láncok biztonságával szemben.
- A reziliencia fenntartása.

Információbiztonság az ellátási láncban

- Három alappillér: bizalmasság, sértetlenség, rendelkezésre állás.
- Kockázatok: adatlopás, rendszerleállás, jogosulatlan hozzáférés.
- A lánc minden szereplője potenciális célpont.

Példák az ellátási láncok információbiztonsági kockázatára



Kritikus sebezhetőségek

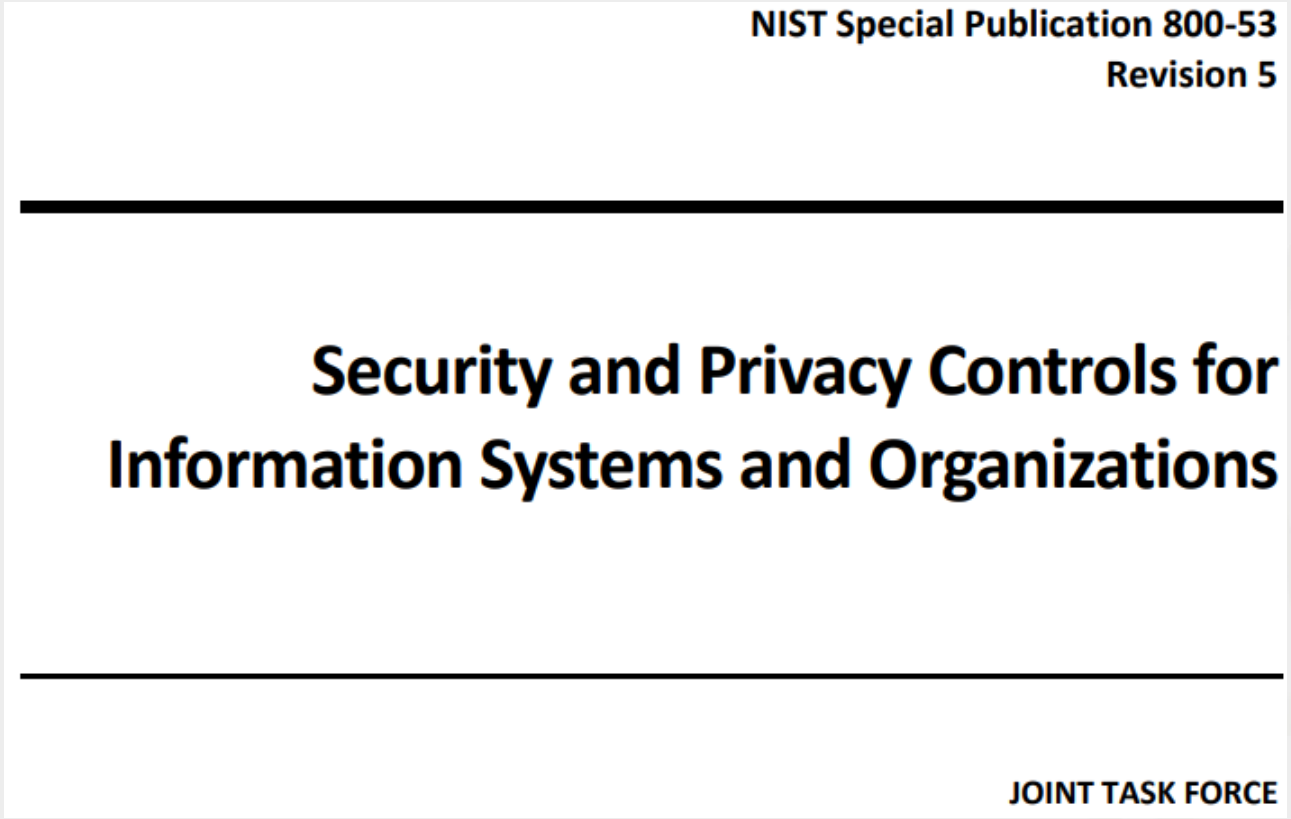
- Harmadik fél kockázatok (beszállítók, alvállalkozók).
- Ipari vezérlőrendszerek (ICS), IoT eszközök.
- SolarWinds, Log4j – globális hatások.

Szabályozási környezet

- NIS2 irányelv: kötelezettségek és hatókör.
- ISO/IEC 27001 szabvány (Information Security Management Systems – ISMS).
- ISO/IEC 28000 szabvány (Supply Chain Security Management Systems - SCSMS).

- GDPR és adatvédelmi megfelelés.

NIST 800-53 rev5



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for
Information Systems and Organizations

JOINT TASK FORCE

supply chain 243/10

Magyarország Kiberbiztonsági Stratégiája

- **Ellátási láncok** megzavarása: Az ellátási láncok fenyegetettsége az elmúlt években kiemelt veszélyforrássá vált, mivel az azokhoz kapcsolódó, többnyire előre nem látható események kölcsönhatásai súlyos társadalmi, gazdasági és politikai következményekkel járhatnak.
- Intézkedéseket szükséges hozni a kis- és középvállalkozások **ellátási láncaiban** felmerülő kihívások kezeléséhez
- A stratégiai időszakban célkitűzés a kiberbiztonsági kötelezettségek hatálya alá tartozó szervezetek egészére kiterjedő szabályozás kialakítása, amely az EIR-ek és IKT termékek és szolgáltatások, rendszerelemek és rendszerszolgáltatások fejlesztésével, beszerzésével, karbantartásával, üzemeltetésével és selejtezésével kapcsolatosan közreműködő **ellátási lánc** kockázatainak és esetlegesen bekövetkező biztonsági eseményei elemzésére és kezelésére vonatkozóan előírja a tervezési dokumentumrendszer készítését és aktuálisan tartását.
- Az űrszektorhoz köthető kibervédelmi aspektusoknak meg kell akadályozniuk az űrtevékenységekkel kapcsolatos érték láncok felderítését, támadóképességek kifejlesztését, a rendszerekhez való hozzáférését, a támadó tevékenység végrehajtását, hosszú idejű fenntartását, a védelmi rendszerek elkerülését és az alrendszerek közötti rosszindulatú átjárást annak érdekében, hogy az **ellátási láncok** biztonságát biztosítani tudjuk

7/2024. (VI. 24.) MK rendelet

- 1.21. Ellátási lánc kockázatmenedzsment stratégiája
- 1.22. Ellátási lánc kockázatmenedzsment stratégia – Üzletmenet (ügymenet) szempontjából kritikus termékek beszállítói
- 9.19. Biztonsági események kezelése – Ellátási lánc koordinációja
- 9.30. A biztonsági események jelentése – Ellátási lánc koordinációja
- 15.5. Kockázatelemzés – Ellátási lánc

19. Ellátási lánc kockázatkezelése

- 19.1. Szabályzat és eljárásrendek
- 19.2. Ellátási láncra vonatkozó kockázatmenedzsment szabályzat
- 19.4. Ellátási láncra vonatkozó követelmények és folyamatok
- 19.7. Ellátási lánc ellenőrzések és folyamatok – Alvállalkozók
- 19.13. Beszerzési stratégiák, eszközök és módszerek
- 19.16. Beszállítók értékelése és felülvizsgálata
- 19.19. Értesítési megállapodások
- …

Szabályzat a felmerülő ellátási lánccal kapcsolatos kockázatok kezelésére.

Technológiai megoldások

- Zero Trust modell.
- Blockchain az átláthatóságért.
- SIEM, SOAR, XDR rendszerek.

Kockázatkezelési gyakorlatok

- Beszállítói auditálás és értékelés.
- Incidenskezelési terv.
- Tudatosságnövelés és képzések.

Jövőbeli kihívások

- Mesterséges intelligencia a prediktív biztonságban.
- Kvantumszámítógépek és a kriptográfia jövője.
- Globális együttműködés és szabványosítás szükségessége.

Összegzés

- A logisztikai vállalatok hatalmas mennyiségű érzékeny adatot kezelnek, beleértve az ügyféladatokat, a szállítási részleteket és a fizetési adatokat.
- A „fejlesztések” folyamatosak a támadó oldalon, ami versenyt generál a védekező oldalon.
- A kiberbiztonságra fordított kiadások nem járnak közvetlen haszonnal az üzlet számára. De ezek nélkül a kockázat jelentős.

Következtetések

- Komplex és kritikus terület, ami több szinten jelent kihívást
- Átfogó biztonsági stratégia szükséges az egész ellátási láncra
  - harmadik fél kockázatkezelés
  - szoftverellátási lánc biztonsága
  - hozzáférés-szabályozás és titkosítás
  - monitoring és incidenskezelés
- Kockázatértékelés, auditok, oktatás.
- Proaktív megközelítés: támadások kockázatának csökkentése, adatok védelme

KÖSZÖNÖM A FIGYELMET!

uni-nke.hu