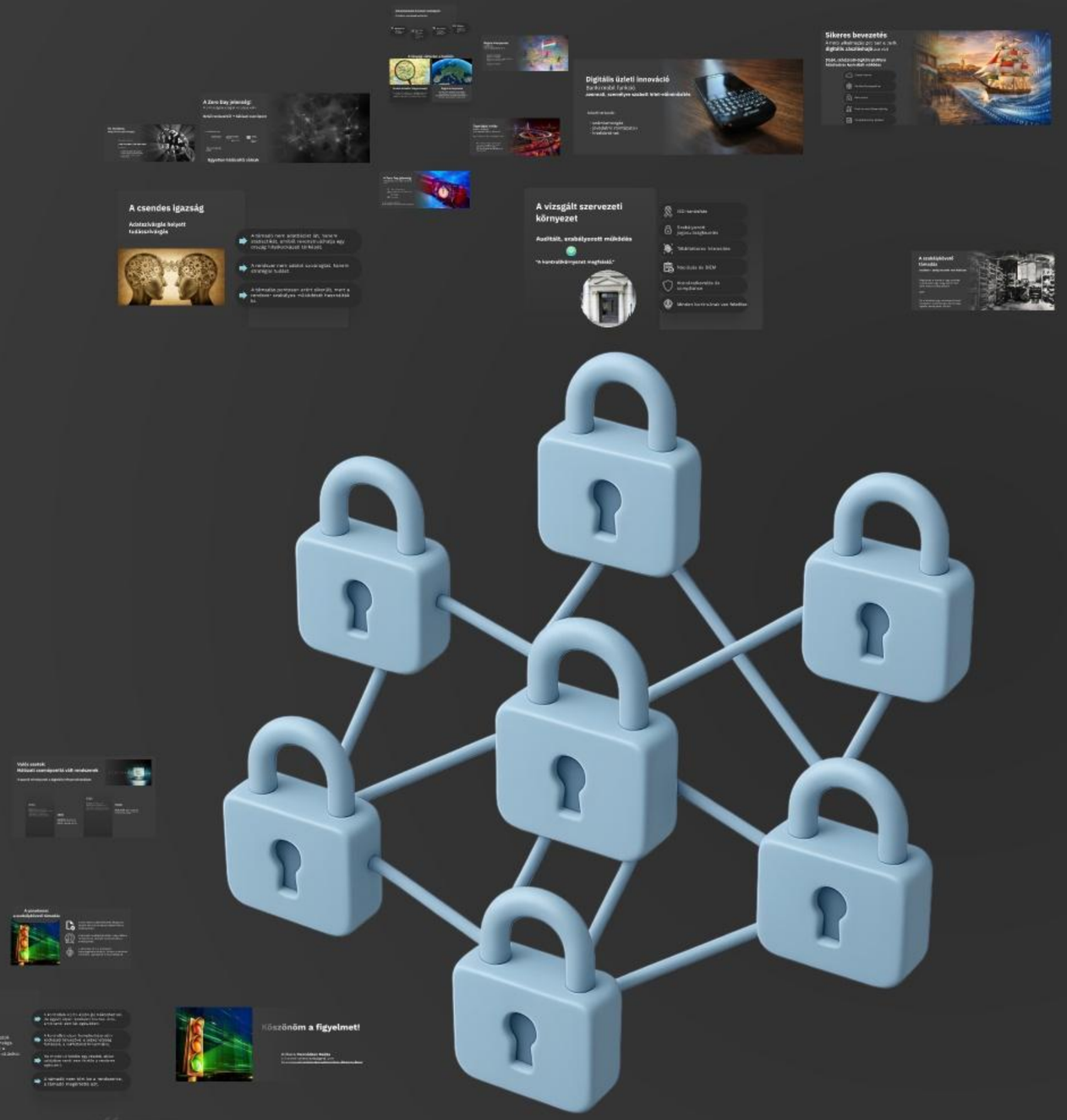

EIVOK-74. Információbiztonsági Szakmai Fórum

A szabálykövető támadás – hogyan hackelhető egy auditált szervezet?

Amikor a szabályok betartása vezet a sebezhetőséghez

Szikora Mercédesz Beáta
intézménytámogatási szakreferens
Budavári Polgármesteri Hivatal

Nemzeti Közszolgálati Egyetem
2026. március 19.

A szabálykövető támadás

Incidens - pedig itt senki nem hibázott

Meg lehet-e hackelni egy auditált szervezetet úgy, hogy senki nem sérti meg a szabályokat?

Igen.

Ez a történet egy mintázatról szól, amelyben a látszólagos biztonság rejtett veszélyeket hordoz.

A vizsgált szervezeti környezet

Auditált, szabályozott működés

"A kontrollkörnyezet megfelelő."

- ISO-tanúsítás
- Szabályozott jogosultságkezelés
- Többfaktoros hitelesítés
- Naplózás és SIEM
- Kockázatkezelés és compliance
- Minden kontrollnak van felelőse

Digitális üzleti innováció

Banki mobil funkció

azonnali, személyre szabott hitel-előminősítés

Adatforrások:

- számlamozgás
- jövedelmi mintázatok
- hiteltörténet

Sikeres bevezetés

A mobilalkalmazás gyorsan a bank
digitális zászlóshajójává vált

Stabil, skálázható digitális platform
Átlátható és kontrollált működés

- Cloud-native
- DevSecOps/pipeline
- Zero trust
- End-to-end Observability
- Compliance by default

Régiós kiterjesztés

Skálázódás

Több ország ügyfélállománya

- Ugyanaz a rendszer
- Ugyazaz a modell
- Ugyanazok a jogosultsági szerepek
- Ugyanazok a kontrollok

Nagyobb hatókör

A lényegi változás: a hatókör

Eredeti működés (Magyarország)

Az alkalmazás egyetlen ország ügyféladataival dolgozott, a hozzáférés mértéke ehhez a léptékhez igazodott. Kockázati profil: lokális.

Régiós kiterjesztés

Ugyanaz az alkalmazás, ugyanazzal a jogosultsággal, már több ország teljes ügyfélállományának mintázataival dolgozik. A kitettség nagyságrendje megváltozott.

Alkalmazásból hálózati csomópont

A rendszer szerepének evolúciója

Mobilalkalmazás

Egy belső, országspecifikus szolgáltatás.

Régiós Pénzügyi Elem

Több ország pénzügyi felügyelete alá tartozik.

Hálózati Csomópont

Más bankokkal, külső scoring szolgáltatásokkal kommunikál.

Kritikus Infrastruktúra

Rendszerszintű elemmé válik, adatokat ad és kap.

Topológiai váltás

Belső rendszerből
csomóponttá válás a hálózatban

Egy 'mellékutca' hirtelen 'autópályává' válik.

Mi történik, amikor egy rendszer
már nem önmagában működik,
hanem már infrastruktúra,
ami más rendszerek működését is
befolyásolja?

A Zero Day jelenség:

A biztonság topológiai kérdéssé válik.

- Modern infrastruktúra
- Egymásba kapcsolódó hálózatok
- Komplexitás
- Új kihívások

A rendszereket auditáljuk.
De ki auditálja a rendszerek kölcsönhatásait?

Az incidens:
Modell-kivonatoló támadás

Támadási módszer:

model extraction / inference attack

A támadó:

- legitim kérdéseket használ
- mesterséges profilokat gyárt
- statisztikai mintázatokat rekonstruál

A csendes igazság

Adatszivárgás helyett tudásszivárgás

- A támadó nem adatbázist lát, hanem statisztikát, amiből rekonstruálhatja egy ország hitelkockázati térképét.
- A rendszer nem adatot szivárogtat, hanem stratégiai tudást.
- A támadás pontosan azért sikerült, mert a rendszer szabályos működését használták ki.

A paradoxon: a szabálykövető támadás

A szervezet szabálykövető állapotot tartott fenn (a rendszer betartotta a szabályokat).

A támadó szabálykövetően használta a rendszert (a támadó is betartotta a szabályokat).

A támadás nem a szabályok megszegésével történt, hanem a rendszer működési logikájának kihasználásával.

Valós esetek:
Hálózati csomóponttá vált rendszerek

Hasonló mintázatok a digitális infrastruktúrában

2020

SolarWinds támadás: Egy szoftverfrissítésen keresztül kaptak hozzáférést kormányzati hálózatokhoz. A támadó egy szoftverellátási láncot tört fel.

2021

Log4Shell: Egy naplózó, digitális könyvtárból lett globális támadási felület.

2023

MOVEit támadás: Egy fájltranszfer rendszer vált nemzetközi adatcsatornává, több ezer szervezetet érintve.

Trend

Közös minta: adminisztrációs eszközökből kritikus hálózati csomópontok lettek.

A tanulság:

A komplexitás sebezhetőségi tényező

A modern hálózatok topológiai biztonsága kulcsfontosságú a csomópontokká váláskor.

- A kontrollok külön-külön jól működhetnek, de együtt olyan rendszert hoznak létre, amit senki sem lát egészében.
- A kontrollrendszer komplexitása válik kockázati tényezővé: a sebezhetőség forrásává, a vakfoltokat kihasználva.
- Ha mindenki felelős egy részért, akkor valójában senki sem felelős a rendszer egészéért.
- A támadó nem tört be a rendszerbe, a támadó megértette azt.

Egy rendszer nem a részek összessége, hanem a kölcsönhatások eredménye.

Russel L. Ackoff

Köszönöm a figyelmet!

Szikora Mercédesz Beáta
szikoramercedeszbeata@gmail.com
https://www.linkedin.com/in/mercedesz-beata-szikora/