Incidenskezelés?
Mire észbe kap, már késő!

A probléma égető valósága

Date of the Event	Victim	Incident
2024. jan.. 2.	Blockchain platform Orbit Chain	Orbit Chain loses $86 million in fintech hack
2024. jan.. 4.	KyivStar Telecommunication	Russian hackers wipe thousands of systems in KyivStar attack
2024. jan.. 8.	loanDepot	US mortgage lender loanDepot confirms ransomware attack
2024. jan.. 21.	Majorca city Calvià	Majorca city Calvià hit by ransomware attack
2024. jan.. 29.	Energy company Schneider	Energy giant Schneider Electric hit by Cactus ransomware attack. Cactus ransomware claim to steal 1.5 TB of data
2024. febr.. 1.	Lurie Children's Hospital	Rhysida ransomware demands $3.6 million for children's stolen data
2024. febr.. 22.	AT & T	Cell Phone outage hits AT&T customers nationwide; Verizon and T-Mobile users also affected
Marc 30. 2024		AT&T confirms data of 73 million customers leaked on hacker forum
Marc 05, 2024	Duvel Moortgat Brewery	Duvel says it has "more than enough" beer after ransomware attack
Mar 12, and 22, 2024	Boat Dealer MarineMax	Boat Dealer MarineMax hit by cyber attack
Marc 15, 2024	NHS Dumfries and Galloway	Ransomware group allegedly leaks stolen data from the Scottish health service
Apr 04 and 11, 2024	Hoya Corporation	Hoya's optics production and orders disrupted by ransomware attack with a demand of $10 million
2024. máj.. 8.	Dell	Dell warns of data breach, 49 million customers allegedly affected
2024. jún.. 3.	American Radio Relay League (ARRL)	ARRL says it was hacked by an "international cyber group"
June 24, 2024	Neiman Marcus	Neiman Marcus confirms data breach after Snowflake account hack
July 15, 2024	Rite Aid Pharmacy	Rite Aid says June data breach impacted 2.2 million people
July 18, 2024	Indian crypto platform WazirX	Indian crypto platform WazirX confirms $230 million stolen during cyber attack
2024. aug.. 4.	Keytronic	Keytronic reports losses of over $17 million after ransomware attack
2024. aug.. 8.	ADT Alarm	Home alarm company ADT says hackers obtained 'limited' customer data
Aug. 23-29, 2024	Halliburton	Halliburton forced to take systems offline to contain cyber attack
2024 okt 10.	Casio	Casio confirms customer data stolen in a ransomware attack
2024. nov.. 1.	Los Angeles Housing Agency	Los Angeles Housing Agency confirms another cyber attack after 2023 ransomware incident
2024. nov.. 3.	Schneider Electric	Schneider Electric says hackers accessed internal project execution tracking platform
2024. nov.. 21.	Blue Yonder	Retailers struggle after ransomware attack on supply chain tech provider Blue Yonder
2024. dec.. 3.	BT	BT unit took servers offline after Black Basta ransomware breach
2024. dec.. 16.	Texas Tech University	Texas Tech University System data breach impacts 1.4 million patients
2024. dec.. 30.	Cisco	Cisco confirms authenticity of data after second leak

A jellemző megközelítés: **„Majd reagálunk”**

Először jön a támadás, aztán a pánik.

Miért **kezeljük** az incidenseket, ha

megelőzhetnénk őket?

Az incidenseket nem csak **túlélni**, hanem

elkerülni is lehet!

A megszokott megközelítések kudarca

Túl későn kezdődik

- A támadás megtörtént, mire észrevesszük.
- Az átlagos észlelési idő: 6-9 hónap (!), a támadók addig észrevétlenül mozognak.

Túl reakcióközpontú

- tüzet oltunk, nem megelőzünk.
- időnként csak logokat nézegetünk és riasztásokat kapcsolgatunk ki.

Túlzottan a technológiára épít

- Egy újabb biztonsági eszköz NEM oldja meg a problémát.
- Az IT biztonság nem egy termék!

Az incidens MEGELŐZÉSE, nem csak kezelése:
"Mi lenne, ha az incidens meg sem történne?"

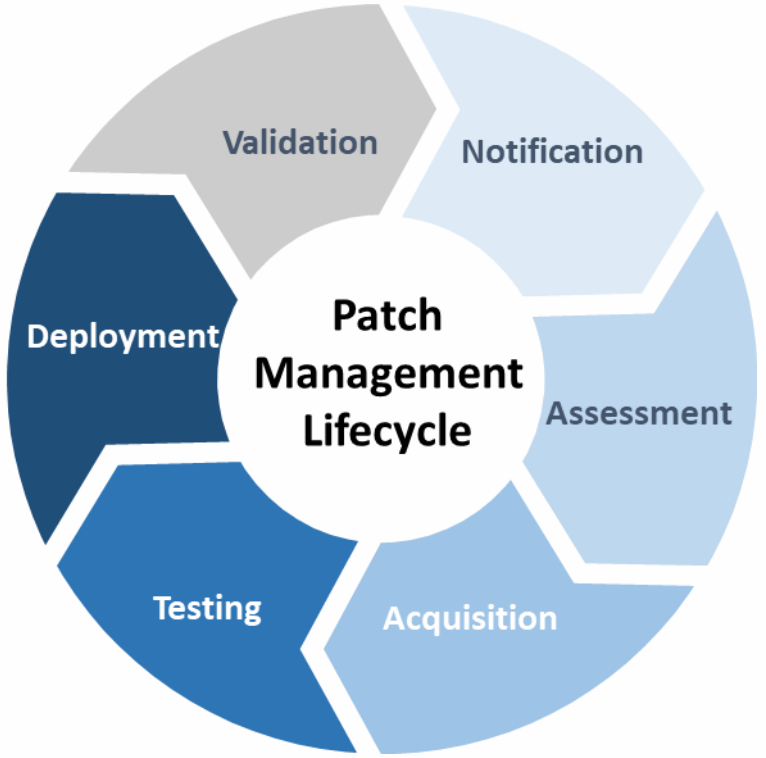
- **Proaktív megközelítés – gondolkodjunk a támadó fejével!**
- **Threat hunting** – folyamatos keresés, nem csak riasztások figyelése.
- **Anomália-alapú felderítés** – ne a múltbeli támadások után nyomozzunk, hanem az új fenyegetéseket ismerjük fel!
- **Honeypot és deception technology** – állítsunk csapdákat a támadóknak.
- **Zero Trust architektúra – Ne bízzunk senkiben**
- Az alapelv: **"Minden rendszer feltört, amíg az ellenkezője be nem bizonyosodik."**
- **Mikroszegmentáció, minimális jogosultságok, folyamatos hitelesítés**.
- **Red Teaming és folyamatos támadásszimulációk**
- Az éves pentest nem elég! **Folyamatos támadásszimulációk kellenek.**
- **Automatizált tesztelés + humán intelligencia**– így szűrjük ki a potenciálisan támadható sérülékenységeket

A biztonság nem állapot, hanem folyamatos harc.

neti

Patch Management: **az incidensek kriptonitja**

- **Mi az a Patch Management?**
  - A szoftverekhez kiadott hibajavítások és biztonsági frissítések **rendszerezett** kezelése és telepítése.
  - Magában foglalja a frissítések **nyomon követését, tesztelését és bevezetését**.
- **Miért fontos?**
  - **Sérülékenységek**: Az elavult szoftverek komoly biztonsági réseket tartalmazhatnak.
  - **Automatizált támadások**: A hackerek célzottan használják ki a közismert hibákat.
  - **Jogszabályi megfelelés**: Számos szabvány és előírás előírja a rendszeres frissítést (NIS2, ISO 27001, GDPR stb.).
- **Előnyök**
  - **Kockázatcsökkentés** – Megelőzhetők a támadások és adatvesztések.
  - **Rendszerbiztonság** – Folyamatosan csökkenti a támadási felületet.
  - **Megbízhatóság** – Javítja a rendszer stabilitását és teljesítményét.

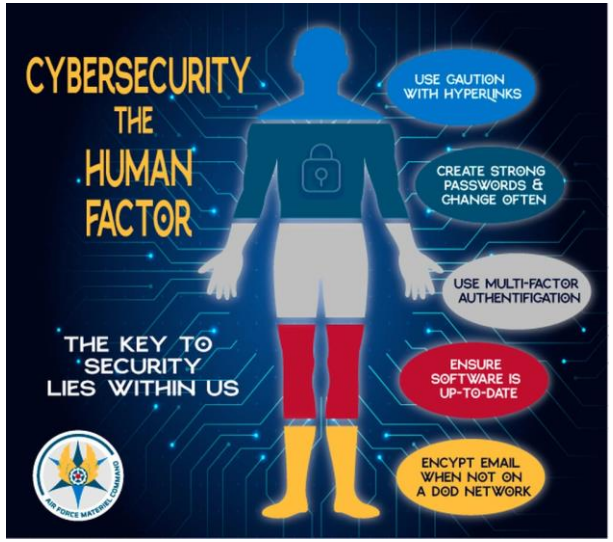


A biztonság nem állapot, hanem folyamatos harc.

neti

Az emberi tényező: **A támadók elsődleges célpontja**

- **A támadók gyakran nem a rendszereket támadják először, hanem az embereket!**
- **Social engineering és phishing – A belépőjegy a rendszerbe**
  - A legtöbb támadás **egyetlen rossz kattintással** kezdődik.
  - Egy jól célzott adathalász e-mail képes megkerülni a legjobb technológiai védelmeket.
- **Zero Trust nem csak a rendszerekre, hanem az emberekre is vonatkozik**
- **Folyamatos biztonságtudatossági tréningek** – nem elég évente egyszer egy unalmas e-learning!
- **Valós szimulációk** – teszteljük le, hogy a munkatársak felismerik-e a támadási kísérleteket!



neti

A beszállítói lánc: **A leggyengébb láncszem**

A támadások jelentős része külső partneren vagy alvállalkozón keresztül történik!

- **Third-party risk management – Kit engedünk be a rendszerünkbe?**
  - Egyetlen feltört beszállító kompromittálhatja az egész vállalatot.
- **Szigorúbb beszállítói biztonsági követelmények**
  - A partnereinknek **ugyanúgy kell védekezniük, mint nekünk!**
- **Folyamatos monitoring és auditálás**
  - Nem elég egyszer ellenőrizni, **a veszély folyamatosan változik**!

Az AI és az automatizáció szerepe a támadások megelőzésében

- **A támadók is mesterséges intelligenciát használnak – sárkány ellen sárkány(fű)!**
- **AI-alapú viselkedéselemzés és anomáliaérzékelés**
  - Az AI felismerhet **gyanús mintázatokat**, amiket egy ember nem venne észre.
- **Automatizált incidensreakció – Ne várjunk a manuális beavatkozásra!**
  - Az AI és az automatizáció **másodpercek alatt** képes reagálni, míg egy embernek percek vagy órák kellenek.
- **AI vs. AI – A jövő támadásai és védelmi stratégiái**
  - A támadók egyre kifinomultabb módszerekkel dolgoznak, **ezért a védelmünknek is fejlődnie kell!**

Az offline rendszerek és fizikai biztonság szerepe

- **A kibertámadások nem mindig csak virtuálisak – a fizikai támadások is valós veszélyt jelentenek!**
- **Baiting, belső támadók, kompromittált hardverek**
  - Egyetlen rossz helyre dugott pendrive **elég lehet egy rendszer feltöréséhez**.
- **Fizikai hozzáférés korlátozása és ellenőrzése**
  - **Zero Trust nemcsak digitálisan, hanem fizikailag is!**
- **Red Team fizikai behatolási tesztek**
  - Vajon **bemenne-e egy idegen az irodába egy hamis belépőkártyával**?

Az üzleti szemlélet: **A megelőzés olcsóbb, mint a katasztrófa**

A támadás utáni károk:

- Anyagi kár, adatvesztés, jogi következmények.
- **A legnagyobb kár: az ÜGYFELEK BIZALMA elveszik!**

A megelőzés költsége:

- A korai észlelés és védekezés **a töredékébe kerül**, mint egy éles támadás kezelése.
- A "megtakarított támadások" értékelése a vezetőség számára – **mennyibe kerülne, ha nem lennének incidensek?**

Jogszabályi megfelelés és a kockázatok minimalizálása

A szabályozások nem csak kötelező feladatok, hanem versenyelőnyt is jelenthetnek!

GDPR, NIS2, ISO 27001 – Csak papírmunka vagy valós védelem?

- A megfelelés nem helyettesíti a biztonságot, de segíthet kialakítani a megfelelő szemléletet

A jogi felelősség kérdése

- Egy incidens **nem csak üzleti, hanem jogi kockázat is**.

Biztonság, mint üzleti érték

- Egy jól működő IT biztonsági rendszer **ügyfélelőnyt és versenyelőnyt jelenthet**!

Konklúzió és call-to-action

Az incidenskezelési képesség kialakítása elengedhetetlen...

...de legalább ilyen fontos a megelőzés!

"Az incidensek nem elkerülhetetlenek. Csak azok számára, akik nem készülnek fel!"

neti

Köszönöm a figyelmet!