Kibervédelem a frontvonalból

Szemtől szemben az ellenséggel

Mihály Zala
Partner | Head of Technology Consulting and Cybersecurity

2025
Ernst & Young Consulting Ltd.

The better the question. The better the answer.
The better the world works.

Building a better working world

Az IT biztonságra költeni luxus, vagy üzleti kényszer?

1
38%
→
2024: 1 (36%)

Cyber incidents

(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)

The most important global business risks for 2025

2
31%
→
2024: 2 (31%)

Business interruption
(incl. supply chain disruption)

3
29%
→
2024: 3 (26%)

Natural catastrophes
(e.g., storm, flood, earthquake, wildfire, extreme weather events)

4
25%
→
2024: 4 (19%)

Changes in legislation and regulation
(e.g., new directives, protectionism, environmental, social, and governance, and sustainability requirements)

5
19%
↑
2024: 7 (18%)

Climate change
(e.g., physical, operational and financial risks as a result of global warming)

6
17%
→
2024: 6 (19%)

Fire, explosion

7
15%
↓
2024: 5 (19%)

Macroeconomic developments
(e.g., inflation, deflation, monetary policies, austerity programs)

8
14%
↑
2024: 9 (13%)

Market developments[1]
(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)

9
14%
↓
2024: 8 (14%)

Political risks and violence
(e.g., political instability, war, terrorism, coup d'état, civil unrest, strikes, riots, looting)

10
10%
↑
NEW

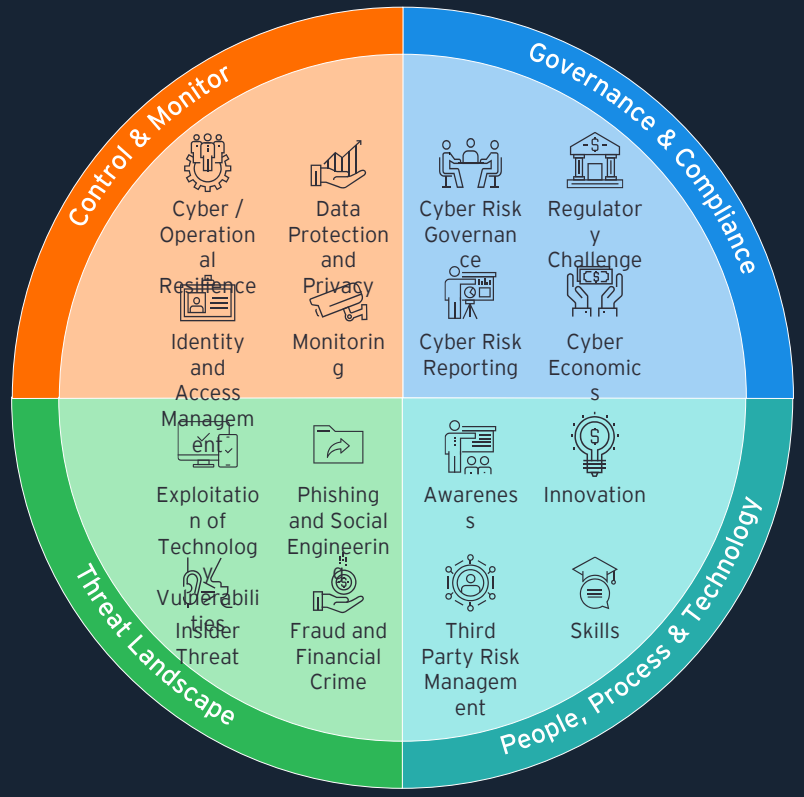
New technologies
(e.g., risk impact of artificial intelligence, connected / autonomous machines)

Mi a kiberbiztonság és miért fontos?

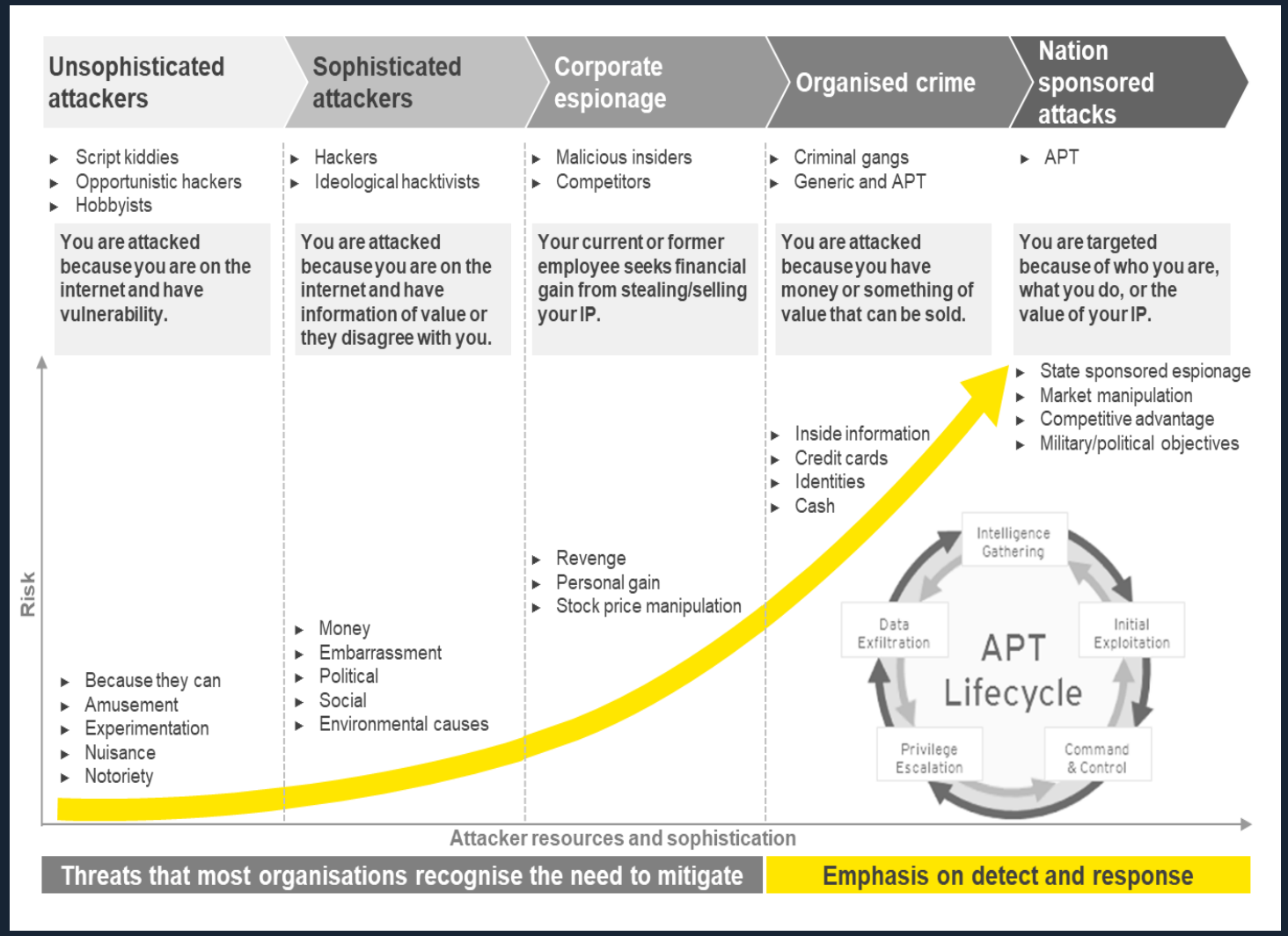
Csak két típusú szervezet létezik: az, amelyiket már megtámadtak, és az, amelyik még nem tudja, hogy megtámadták. A kiber ma már nem csak technológiai kérdés, hanem üzleti kérdés is.

Mihaly Zala
Head of Technology Consulting and Cybersecurity

A kiberbiztonság már nem technológiai kérdés, hanem üzleti kérdés.



A digitális forradalom hogyan változtatta meg a támadási trendeket?



IT fejlődés és digitalizáció

- Internet elterjedése
- Cloud, SaaS megjelenése
- E-kereskedelem, online bankolás
- **Új támadási trendek**

Új típusú támadások és motivációk

- Szervezett bűnözői csoportok
- Hacktivisták
- Nemzetállami támadások
- Zsaroló vírusok
- AI által vezértelt kibertámadások

Hogyan fogják megtámadni a szervezetemet a támadók?

Mi a legnépszerűbb támadás?

- A sikeres támadások 85%-a továbbra is az emberi hibára, megtévesztésre épül
- Ezek ellen a legfejlettebb tűzfalak se védenek meg

Miért nem működnek a klasszikusvédekezési módszerek?

- Zero-day támadások és APT-k
- Az emberi tényezőt nagyon nehéz kiiktatni
- 7/24 támadói aktivitás

Támadók motivációi

Mi a támadók motivációja?

Adatgyűjtés

A támadó elsődleges motivációja az adatgyűjtés

Technikai adatok

- elérhető eszközök
- elérhető szolgáltatások
- ismert sérülékenységek
- felhasznált technológiák

Személyes adatok

- felhasználónevek
- jelszavak
- e-mail címek
- közösségi profilok

Technológiai fókuszú támadás

Social Engineering fókuszú támadás

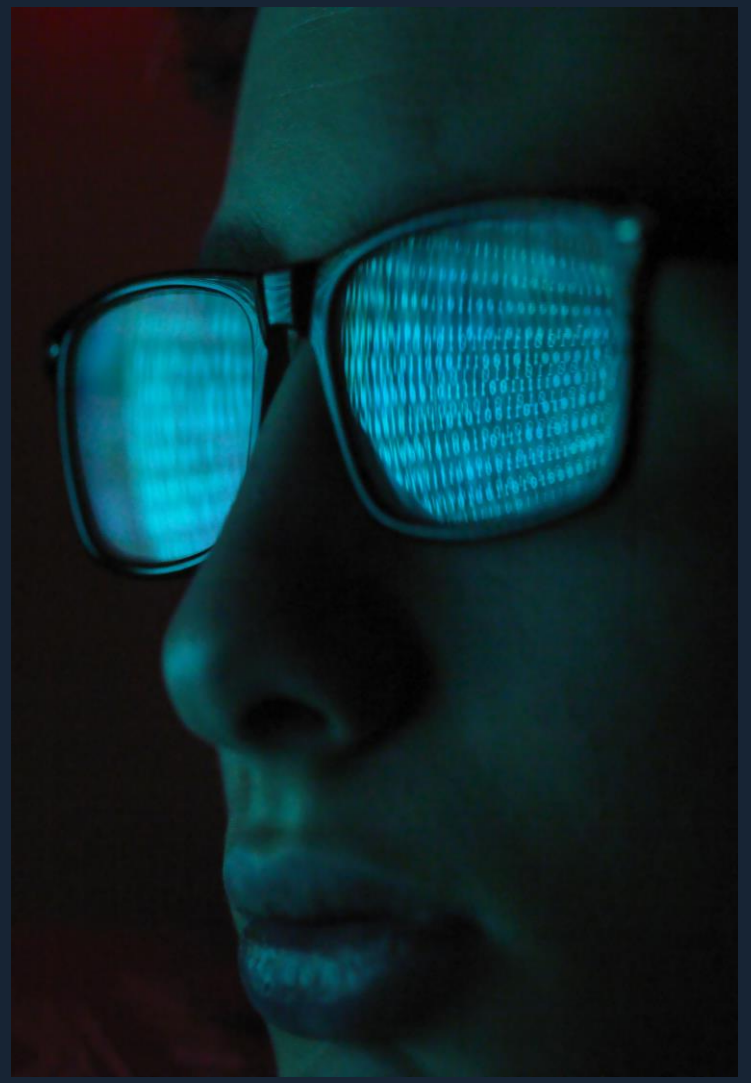
Testre szabott támadások

- ipari kémkedés
- versenytárs lejáratása
- személyes bosszú
- szellemi tulajdon megszerzése

Mesterséges intelligencia alkalmazása a támadások során I.

Hogyan használható az MI az emberi megtévesztésen alapuló támadások során?

1. MI alapú profilkészítés közösségi-média, saját webhelyek vagy nyilvános adatbázisok alapján
2. Személyre szabott, célzott megkeresések
3. Nyelvi akadályok már nincsenek
4. Olyan domain-ek keresése, melyek legjobban hasonlítanak az adott intézményére (xyzbank.hu -> xyz-bank.hu)
5. Weboldal/profil generálás



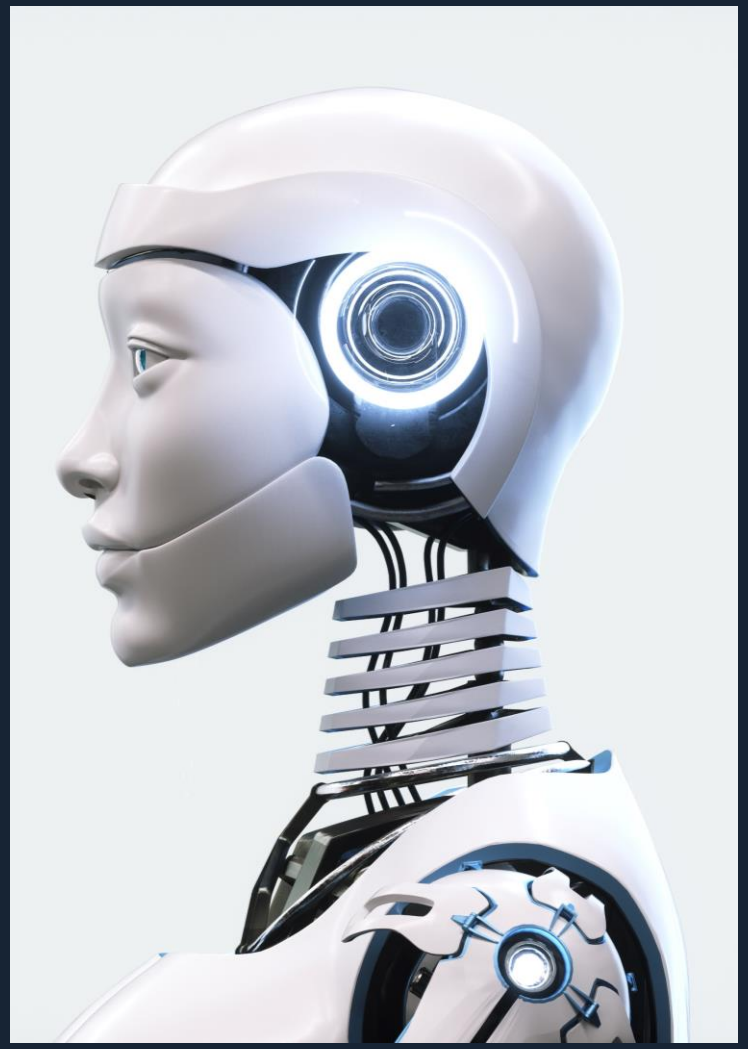
Mesterséges intelligencia alkalmazása a támadások során II.

Hogyan használható az Deepfake technológia a támadások kivitelezése során?

1. Social Engineering támadások: Deepfake technológiát alkalmaznak arra, hogy manipulálják az embereket, bizalmas információkat szerezzenek, vagy a támadás áldozatait cselekvésre késztessék.

2. Információs hadviselés és reputációs támadások: Deepfake technológiával készült tartalmakat használnak dezinformáció terjesztésére vagy egy személy/szervezet hírnevének rontására.

3. Technikai és pénzügyi támadások: Deepfake technológiát közvetlenül technológiai rendszerek vagy pénzügyi tranzakciók manipulálására használnak.



Mesterséges intelligencia alkalmazása a védekezés területén

Hogyan használható az MI a támadások korai fázisában?

1. **Az MI által támogatott rendszerek gyorsan reagálnak a kiberbiztonsági támadásokra.**
2. **Automatizált válaszreakciók lehetővé teszik a hatékony reakciót a fenyegetésekre.**
3. **Az MI segítségével minimalizálhatók a potenciális károk és veszteségek.**
4. **Az automatikus korlátozások/válaszlépések segítik a támadók visszatartását.**
5. **A gyors reakcióidő és rugalmas válaszok biztosítják a nagyobb ellenálló képességet a kiberbiztonsági fenyegetésekkel szemben.**

Fejlett védekezési technológiák - SOC

24/7 Monitoring és gyors reagálás

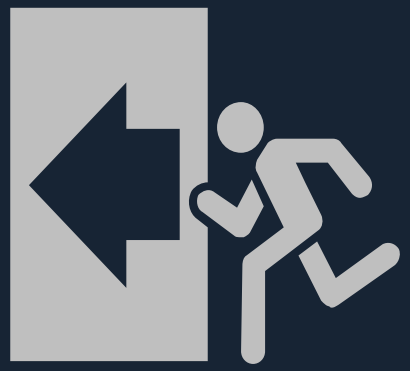
- azonnali reagálás
- nem csak riasztásokat küld, hanem aktívan kezeli is az incidenseket

Központosított fenyegetésfigyelés

- a SOC integrálja az összes IT biztonsági adatot
- támadási minták automatikus, proaktív keresése, felismerése és kezelése

Karrier lehetőség?

Jelenleg a CISO-k nagyon nehéz helyzetben vannak



Köszönjük a figyelmet!

A mesterséges intelligencia használata **rendkívül hatékony eszköz** a **támadók kezében**, mely radikálisan **növeli a támadások hatékonyságát** és jelentősen csökkenti a szükséges felkészülési időt.
Kiemelt jelentősége van a szervezetek **kiberbiztonságában** az ilyen jellegű támadások hatékony felismerésének és elhárításának.

Mihály Zala

Partner | Head of Technology Consulting and Cybersecurity
Ernst & Young Tanácsadó Kft.