# Fejlődő támadási formák szigorodó kiberbiztonsági környezetben

Zala Mihály, partner
Ernst & Young Tanácsadó kft.

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

Building a better working world

# Tartalomjegyzék

# 1. Bevezetés

# TOP 3 üzleti kockázat 2023

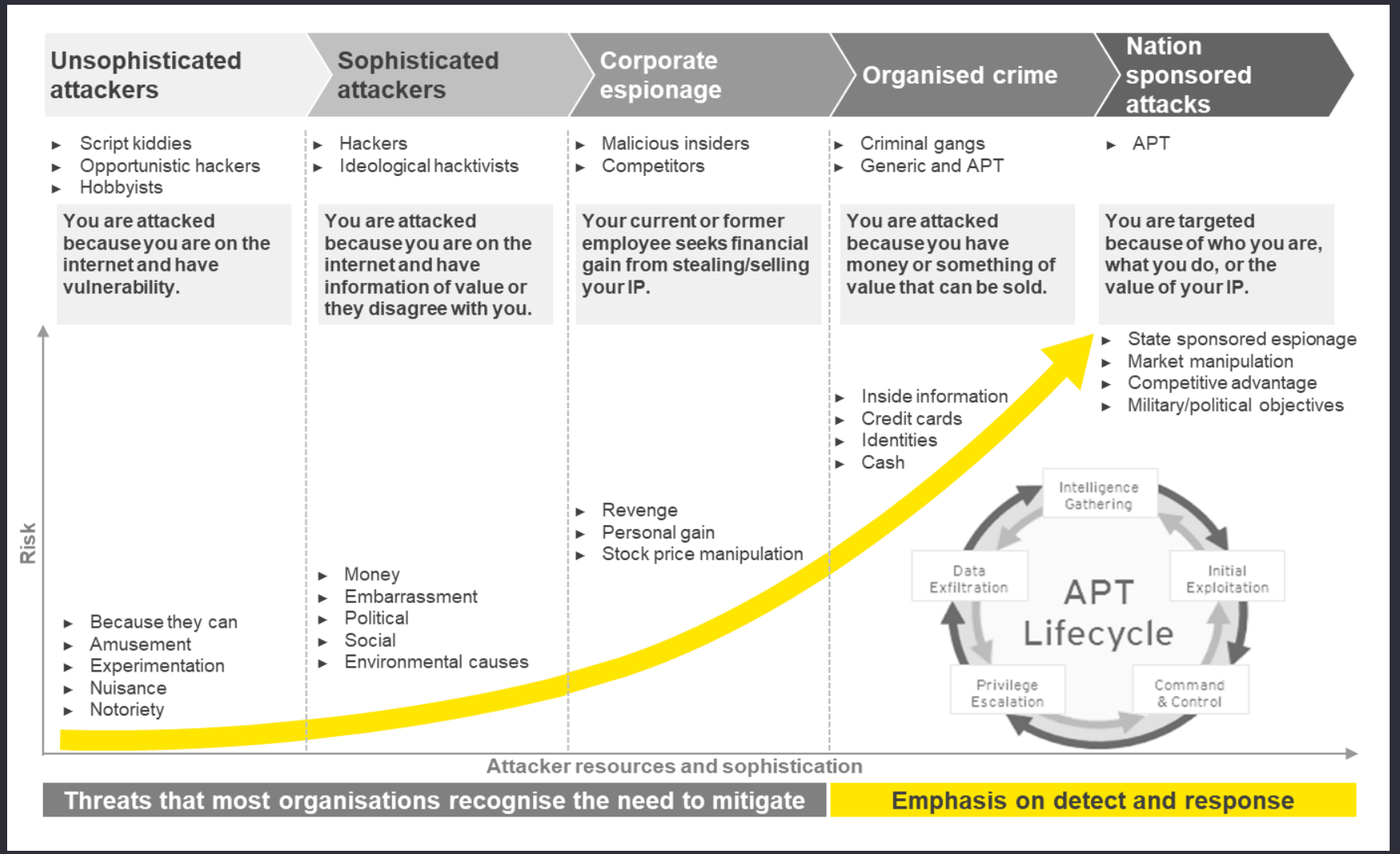
Allianz Risk Barometer 2023


*Source: Allianz Risk Barometer 2023*

# II. Kibertámadások anatómiája

# Kibertámadások evolúciója

## Kibertámadások evolúciója



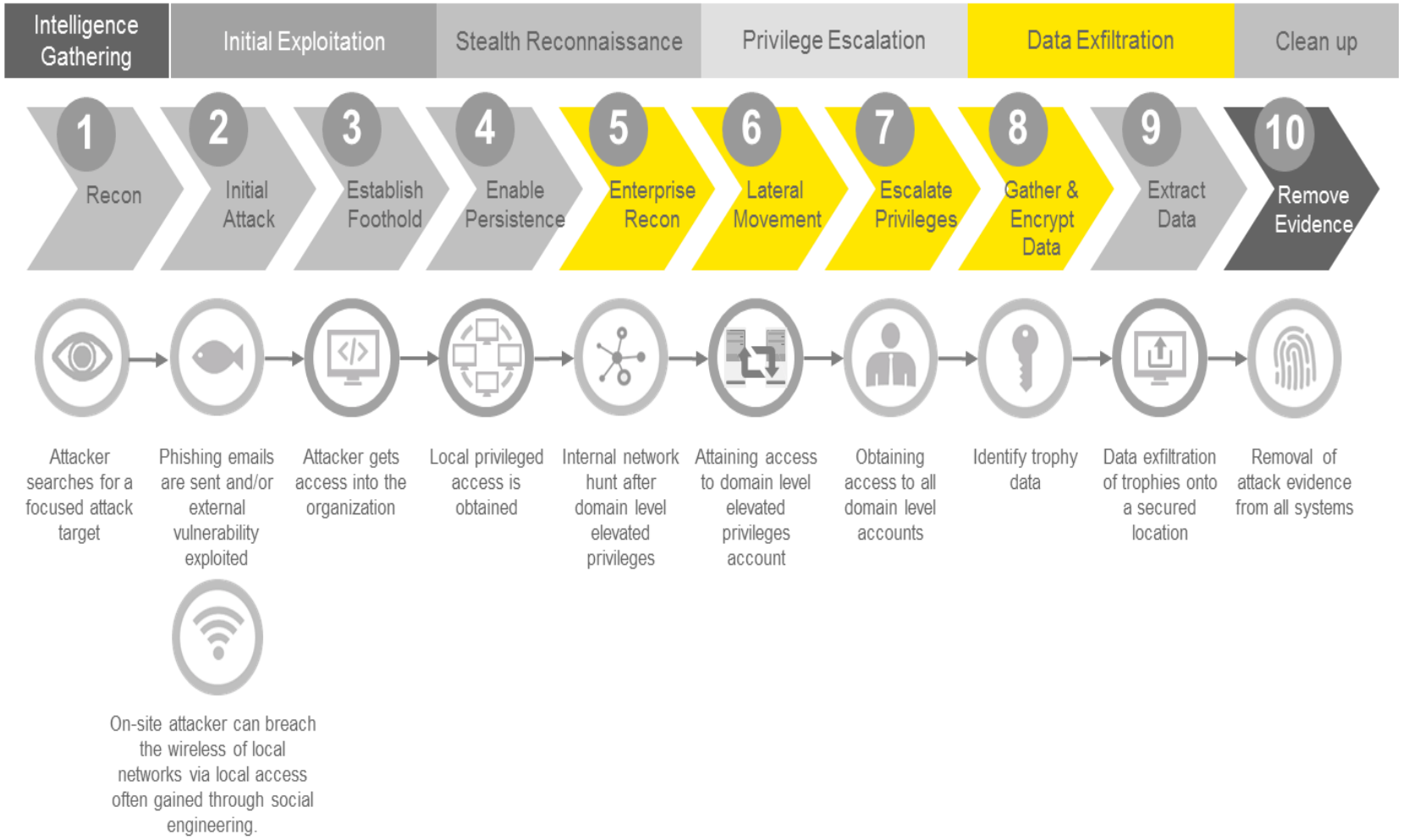
# Támadók és motivációik

## Támadók és motivációik

| Type of Hacker | Definition | Motivation Includes: |
|---|---|---|
| Script Kiddies | A hacker that does not possess technical expertise and relies on pre-developed scripts and programs to perform attacks. | • Thrill of the Challenge<br>• Malicious Intent<br>• Financial Gain |
| Thrill-Seeker | A hacker that break into systems/network for entertainment value (non-malicious intent) | • Thrill of the Challenge<br>• Admiration of fellow hackers |
| Insider Hacker | An employee/consultant that performs security exploits within their firm's system/network utilizing organizational knowledge. Typically this type of hacker is a disgruntled/departing employee, contractor or whistleblower. | • Revenge<br>• Exposing firm weaknesses<br>• Deception/fraud |
| Hacktivists | A socially or politically motivated hacker with the intention of fulfilling a social or political agenda. | • Promotion of political or social beliefs<br>• Website and Social Media Defacement |
| Cyberterrorists | A hacker with threatening objectives such as harming people or destroying critical systems and/or information. | • Invoke Terror/Fear/Panic<br>• Disruption<br>• Cause chaos |
| Cyber Warriors/State Sponsored | A hacker that works for a specific governments to serve their military/economic objectives via cyberspace. These hackers have limitless time and funding to target civilians, corporations, and enemies of the state. | • Promote governmental beliefs<br>• Damage economies<br>• Invoke Terror/Fear/Panic<br>• Exert Dominance<br>• Cause chaos |

# Támadások lefolytatása

**Hogyan visznek véghez a támadók egy kibertámadást?**

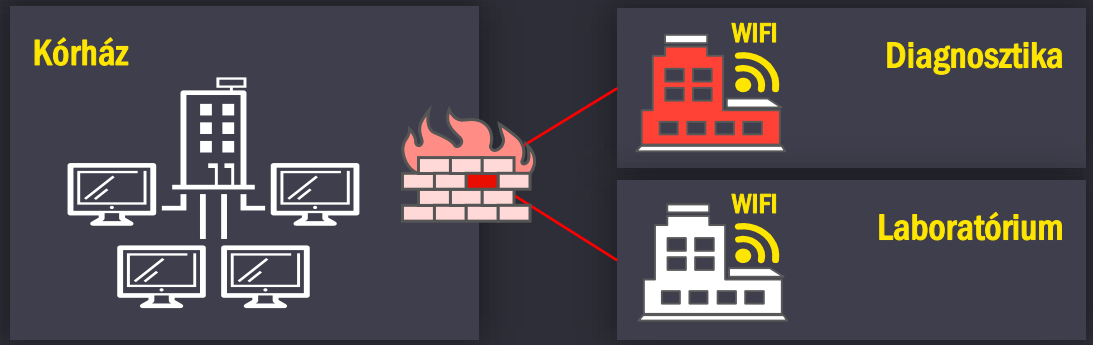


# Magyar kórházakban előfordult zsarolóvírus támadás

**Megyei kórház**

- *Teljes megye ellátása (1,5m fő)*
- *800 aktív ágy*
- *6 dolgozó az IT osztályon*

**Kiváltó ok:** kórházi beszállítók egy routeren keresztül össze voltak kötve a kórház IT rendszerével, beszállító titkársági gépén zsarolóvírus fertőzés




***Zsaroló vírus terjedése***

- *A beszállító szerverén tárolt adatok titkosítása az első gép megfertőzését követően kb. 6 perc elteltével kezdődött meg.*

**Fertőzés lefolyása**

a) Beszállító jelezte a kórház felé az IT rendszere lassulását
b) Kivizsgálás közben zsarolóvírust detektáltak
c) Beszállító leállította a teljes IT rendszerét
d) Azonnali fizikai leválasztás a kórház hálózatáról
e) Hatóságok értesítése (OKF, ÁEEK, NKI)
f) Vírusellenőrzés a teljes kórházi rendszeren

**Általános tanulságok**

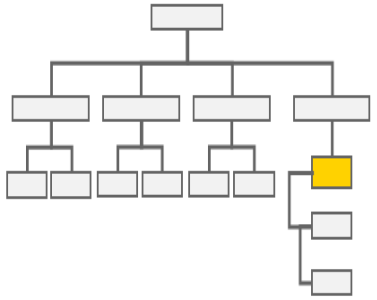
a) A kórház vezetésének tisztában kell lenni, hogy a Kiberbiztonság a kórházi működés és a betegbiztonság szempontjából kritikus tényező.
b) Az informatika és az információbiztonsági képzettségét naprakészen kell tartani (munkavállaló, IT, döntéshozók)
c) Az informatikai beszállítók megbízhatósága felértékelődöt
d) Az IT szinten kapcsolódó beszállítók illetve az ellátási lánc jelentős biztonsági kockázatot hordozhatnak
e) A biztonság növelése érdekében szükség esetén támogatókat, külső cégeket, tanácsadókat is szükséges alkalmazni.
f) Mentések, naplózás, végpontvédelem, kártékony kódok elleni védelem, tűzfalak, gyakorlatban tesztelt BCP/DRP tervek!

Forrás: http://real.mtak.hu/132133/1/fa3312dbda1220b77b7dbe62700a997f.pdf

# III. Kibertámadásokhoz vezető okok

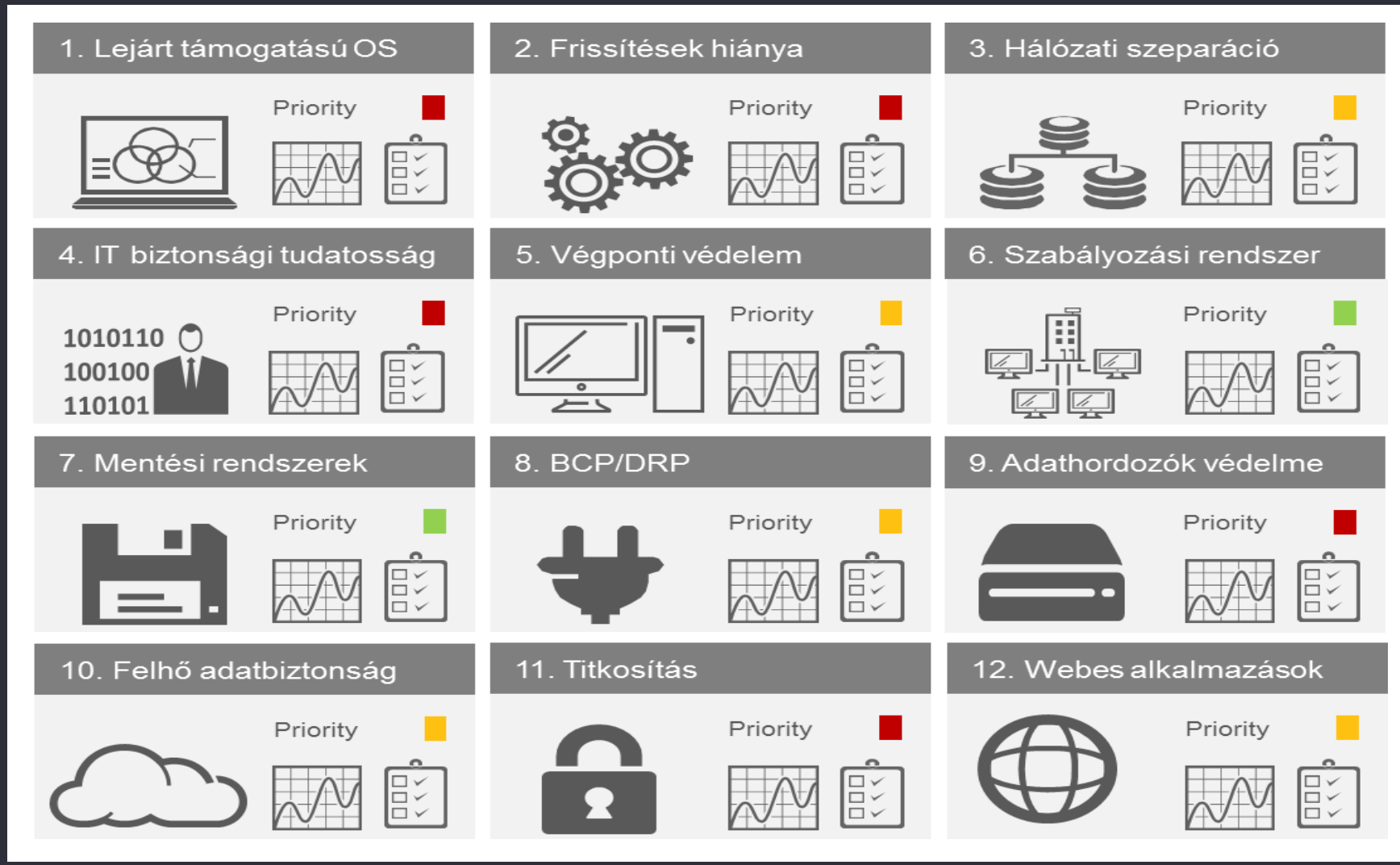
# Belső problémák szervezeti szinten

**Milyen problémákkal küzd általában az IT biztonsági terület?**

| | | |
|---|---|---|
| Szervezeti hierarchia | Költségvetés | Szakértői csapat |
|  |  |  |
| Korszerű rendszerek | Belső szabályozások | Külső szabályzói megfelelések |
|  |  |  |

# Belső problémák technológiai szinten

**Milyen problémákkal küzd az IT biztonsági terület technikai szinten?**

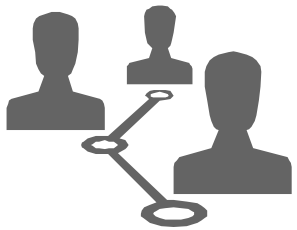


# Motivációs különbségek

**Motivációs tényezők a támadó, védekező és vizsgálati oldalon**

## A helyi üzemeltetés miért nem tárja fel a problémát?

### Fejlesztők, üzemeltetők



### Vizsgálatot végzők

### Támadók

# IV. Jellemző kibertámadási formák

# Gyakori támadási formák

**Gyakori támadási formák**

1. **Emberi megtévesztésen alapuló támadások**

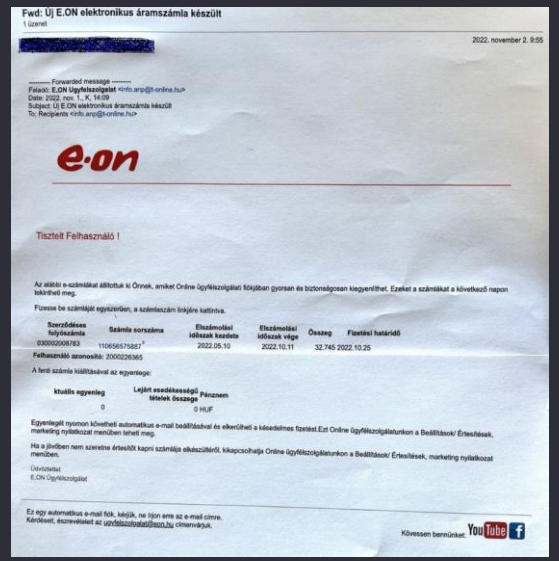
2. **Mobil eszközök** elleni támadások
   - Hamis banki applikációk, „Wallet” szoftverek (amik lehetnek rosszindulatúak)
   - Mobiltelefonra specializált banki malware-ek
   - Hamisított SMS üzenetek (sms spoofing, a két faktor megkerülésére)
   - Phishing támadás mobil alkalmazás szinten (overlay attack)
   - Klónozott sim kártyák
   - Magas szintű supply chain támadások

3. **Botnetekkel elvégezhető támadások**
   - Keylogging
   - Email spamming (malware / phishing)
   - Payperinstall szolgáltatás (telepítésért cserébe fizet az egyébként malware alkalmazás)
   - (D)DOS
   - Bruteforcing

4. **Third party alkalmazások/szolgáltatók** kapnak korlátozott hozzáférést a bankoki rendszerekhez

# Leggyengébb láncszem

**A leggyengébb láncszem továbbra is a felhasználó**


Fwd: Új E.ON elektronikus áramszámla készült

1 üzenet

[redacted] 2022. november 2. 9:55

---------- Forwarded message ---------
Feladó: E.ON Ügyfélszolgálat <info.anp@t-online.hu>
Date: 2022. nov. 1., K, 14:09
Subject: Új E.ON elektronikus áramszámla készült
To: Recipients <info.anp@t-online.hu>

e·on

Tisztelt Felhasználó !

Az alábbi e-számlákat állítottuk ki Önnek, amiket Online ügyfélszolgálati fiókjában gyorsan és biztonságosan kiegyenlíthet. Ezeket a számlákat a következő napon tekintheti meg.

Fizesse be számláját egyszerűen, a számlaszám linkjére kattintva.

| Szerződéses folyószámla | Számla sorszáma | Elszámolási időszak kezdete | Elszámolási időszak vége | Összeg | Fizetési határidő |
|---|---|---|---|---|---|
| 030002008783 | 11065657587 | 2022.05.10 | 2022.10.11 | 32.745 | 2022.10.25 |

Felhasználó azonosító: 2000226365

A fenti számla kiállításával az egyenleg:

| Kiadás egyenleg | Lejárt esedékességű tételek összege | Pénznem |
|---|---|---|
| 0 | | 0 HUF |

Egyenlegét nyomon követheti automatikus e-mail beállításával és elkerülheti a késedelmes fizetést.Ezt Online ügyfélszolgálatunkon a Beállítások/ Értesítések, marketing nyilatkozat menüben lehet meg.

Ha a jövőben nem szeretne értesítőt kapni számlája elkészültéről, kikapcsolhatja Online ügyfélszolgálatunkon a Beállítások/ Értesítések, marketing nyilatkozat menüben.

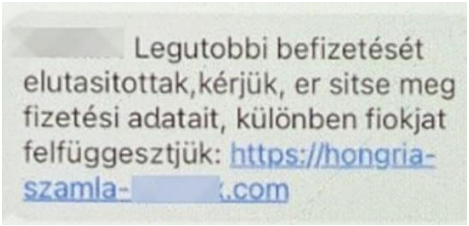
Üdvözlettel
E.ON Ügyfélszolgálat

Ez egy automatikus e-mail fiók, kérjük, ne írjon erre az e-mail címre.
Kérdéseit, észrevételeit az ugyfelszolgalat@eon.hu címenvárjuk.

Kövessen bennünket: YouTube f

## A felhasználók egyre nehezebb helyzetbe kerülnek, mert:

- új, ismeretlen megoldások érkeznek, melyeket nem ismernek
- A csalók folyamatosan fejlesztik a támadási technikájukat, amihez a védelmi képességek lassan tudnak felfejlődni


[redacted] Legutobbi befizetését elutasitottak,kérjük, er sitse meg fizetési adatait, különben fiokjat felfüggesztjük: https://hongria-szamla-[redacted].com

## Leggyakoribb támadási technikák felhasználók ellen:

- A banki ügyintézős csalás
- Hamis linket alkalmaznak email-es vagy SMS-es megkeresés során
- Apróhirdetéssel összekapcsolható csalások lebonyolítása
- Nyereményjáték
- „Ráijesztéses” módszer

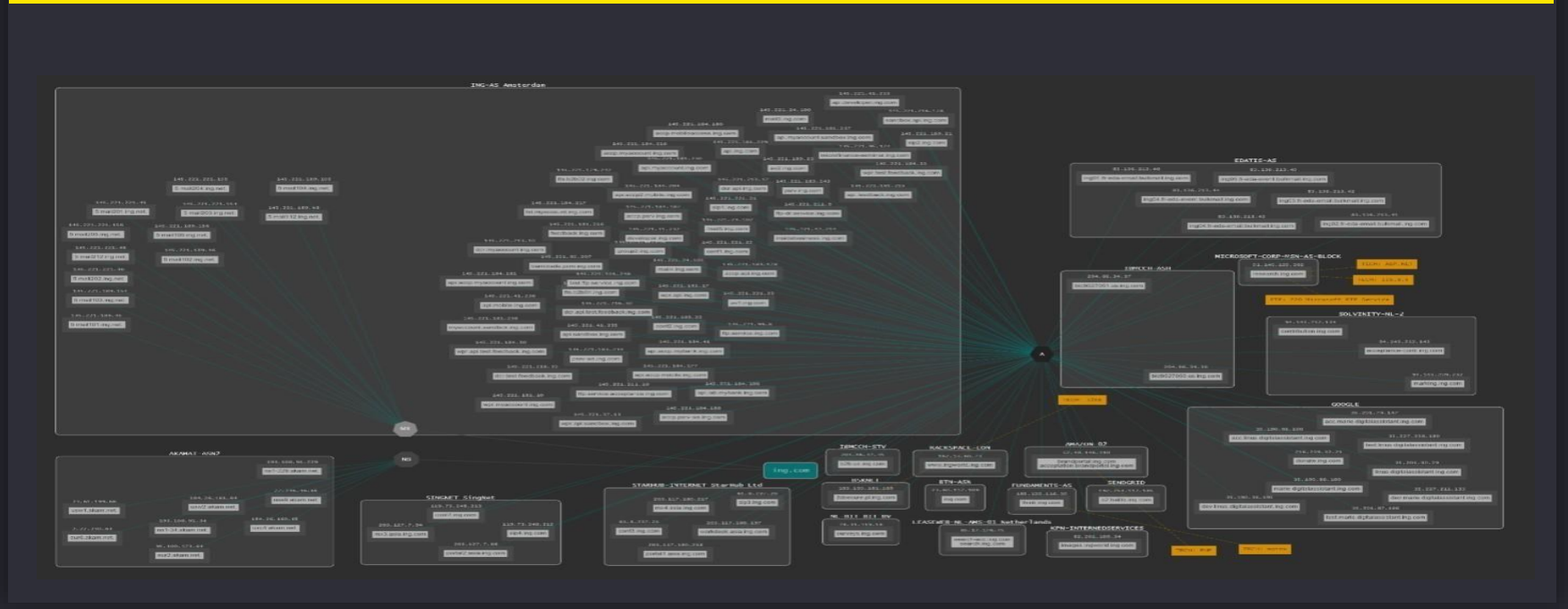
***Aki a saját pénzét önként elutalja, vagy banki hozzáférési adatait önként kiadja, azt semmilyen hatóság és bank sem tudja megvédeni – „Bankszövetség főtitkára”***

# V. Védekezési lehetőségek

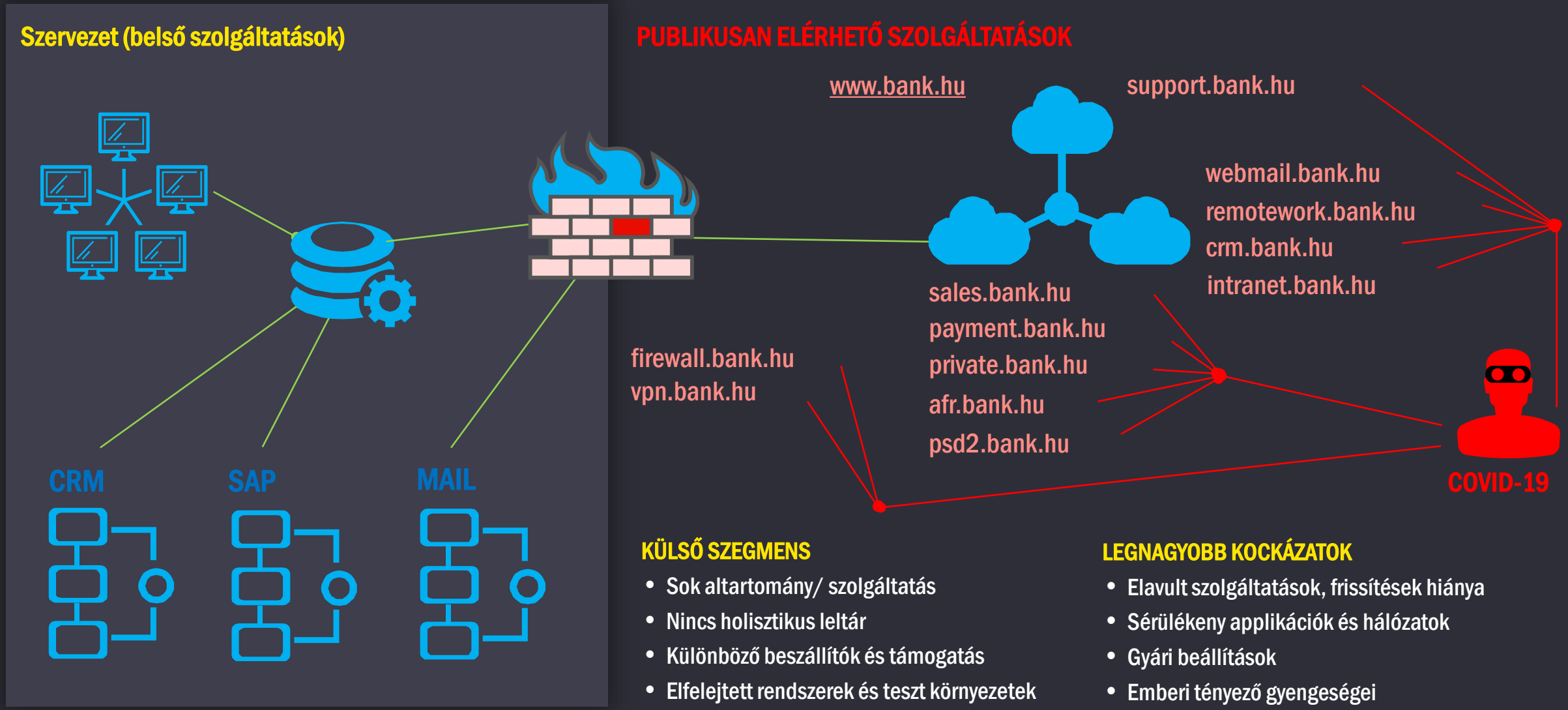
# Külső technológiai kitettségek kontrollálása

- Külső kitettségek horizontális azonosítása
- Korábban feltárt sérülékenységek felülvizsgálata

**A legrosszabb forgatókönyvre kell számítani, javasolt a biztonsági rések haladéktalan feltárása és javítása a szervezet internet irányból elérhető eszközein és határvédelmi rendszerein, akár külső szolgáltató igénybevételével.**



# Külső technológiai kitettségek kontrollálása




**KÜLSŐ SZEGMENS**

- Sok altartomány/ szolgáltatás
- Nincs holisztikus leltár
- Különböző beszállítók és támogatás
- Elfelejtett rendszerek és teszt környezetek

**LEGNAGYOBB KOCKÁZATOK**

- Elavult szolgáltatások, frissítések hiánya
- Sérülékeny applikációk és hálózatok
- Gyári beállítások
- Emberi tényező gyengeségei

# Harmadik feles kockázatok kezelése

**Beszállítói auditok elvégzése a harmadik feles/ellátási lánchoz köthető kockázatok kontrollálása érdekében**

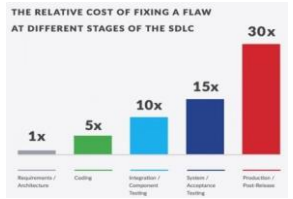
## Miért fontos ellenőriznünk a beszállítóinkat?

- Megbízható kapcsolatokban való megbízás
- Gyengébb védelmi intézkedések

## Milyen szabványokat alkalmazzunk a beszállítók ellenőrzése során?

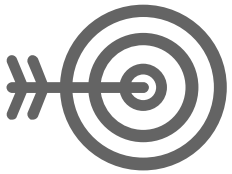
- Nagyon széles a választék (saját policy, NIST, COBIT, GDPR, IBTV+BM VHR)

## Minőségbiztosítás



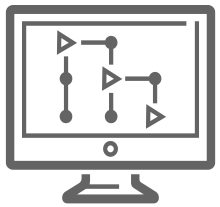

- Külső/belső fejlesztések
- Beszállítók
- Technológiai megoldások bevezetése

## Biztonsági vizsgálatok



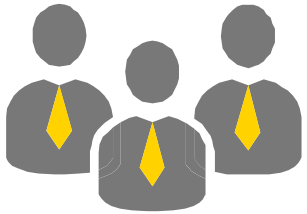
- Sérülékenység vizsgálatok
- Célzott betörési tesztek
- Forráskód vizsgálatok
- Technológiai tesztek

## IT audit



- IT Biztonsági keretrendszer GAP elemzése (GDPR, NIS, NIST, IBTV, ISO27k)
- IT biztonsági auditok
- IT technológiai auditok

## Felkészítés



- Adminisztratív szabályzók felülvizsgálata, elkészítése
- Teljes IT biztonsági keretrendszer felülvizsgálata, elkészítése
- Oktatások elvégzése

# Köszönjük a figyelmet

**Minden harmadik válaszadó (36%) arra számít, hogy** olyan sikeres támadás fogja érni**, amelyet jobb költségallokációval** el lehetett volna kerülni**.**
**76% szerint a kollégák csak** akkor vonják be **az IT biztonságot a projektekbe, ha a** tervezési szakasz befejeződött**.**


Mihály Zala

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