Digitális frontvonal

avagy túlélési praktikák változó biztonsági környezetben

2022. november 4.

HÍRKÖZLÉSI ÉS INFORMATIKAI TUDOMÁNYOS EGYESÜLET

ALAPÍTVA 1949

EIVOK-30. Tudományos - Szakmai Konferencia

Building a better working world

TOP 3 üzleti kockázat

Allianz Risk Barometer 2022

Melyek a vezető üzleti kockázatok egy szervezet életében 2022-ben?

1 **Cyber incidents**
(e.g. cyber crime, IT failure/ outage, data breaches, fines and penalties)

2 **Business interruption**
(incl. supply chain disruption)

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

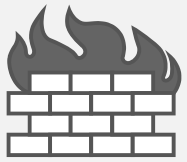
Source: Allianz Risk Barometer 2022

A COVID19 öröksége | Fenyegetettségek

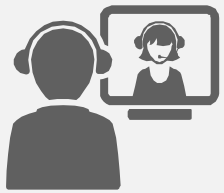
Szektorokon átívelő fenyegetések

Minden szektor érintett, de a **jelentős publikus felülettel** és a **nagy munkavállalói létszámmal** rendelkező szervezetek különösen kitettek a támadásoknak.

Drasztikusan megnövekedett az összekapcsolt eszközök, hálózatok és kollaborációs platformok száma, amiken nagy mennyiségű **bizalmas vállalati információ** kerül megosztásra.



Az új helyzetben a **felhasználók** megkísérlik **megkerülni** azokat a **biztonsági intézkedéseket**, amik hátráltatják őket a napi tevékenységük elvégzésében, ami miatt **bizalmas vállalati információk kerülhetnek ki** a védett, kontrollált környezetből.



A távoli munkavégzésre történő gyors átállás **nyomást gyakorol a biztonsági csapatokra**, hogy megértsék és azonosítsák a potenciális biztonsági kockázatokat.

A COVID19 öröksége | Támadási formák

Kiemelt támadási formák

1

Adathalászat, rosszindulatú tartalmak és céges email fiókokat érintő veszélyek

- A kiberbűnözők kihasználják az emberek érdeklődését a világméretű járvánnyal kapcsolatban.

2

Információ lopás és reputációs veszteség

- Egyes ágazatok esetében megnövekedett a hacktivisták által elkövetett támadások valószínűsége (egészségügy, energetikai szektor, létfontosságú infrastruktúrák, pénzügyi szektor, stb.)

3

Üzletmenet folytonosságot érintő támadások

- A koronavírus témájú zsarolóvírusok jó esetben váltságdíj fejében oldják fel a szerverek, tárolóeszközök titkosítását, vagy nem hajtják végre a DDoS támadást

4

IT üzemeltetési tevékenységek és folyamatok átalakulása

- Távoli munkavégzés kiberbiztonságának kialakítására nem maradt ideje és kapacitása a szervezeteknek, ezt használják ki a támadók

Új geopolitikai helyzet | Támadási formák

Kiemelt támadási formák

Jelentős növekedés a támadási műveletek számában a kibertérben

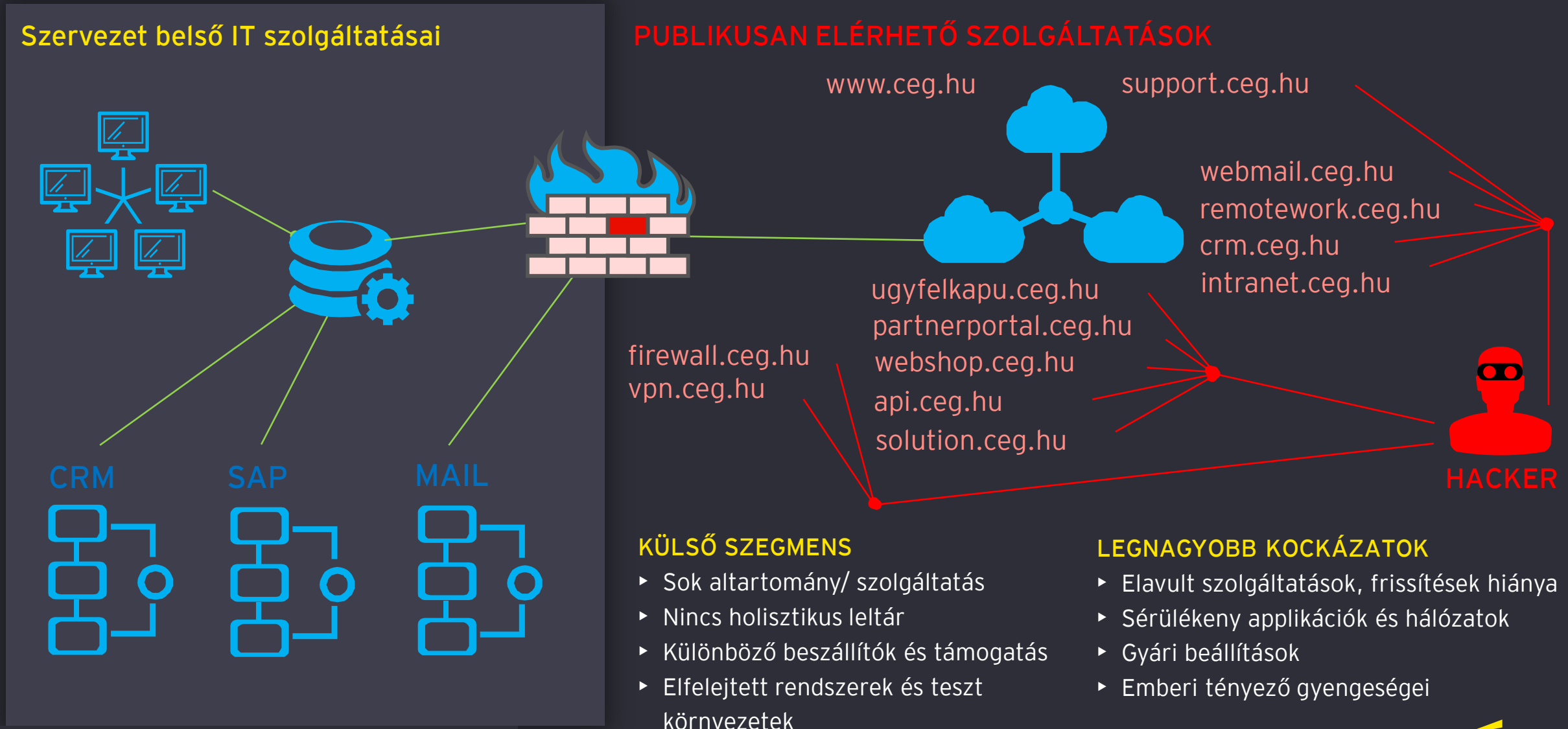
A támadások előkészületi szakaszának 90%-ban adathalász technikákat alkalmaznak

Megnőtt az ellátási láncok elleni támadások száma

Tovább erősödött a zsarolóvírusok használata

Túlterheléses (DoS, DDoS) támadások

Technikai Környezet | Általános IT Infrastruktúra



KÜLSŐ SZEGMENS

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

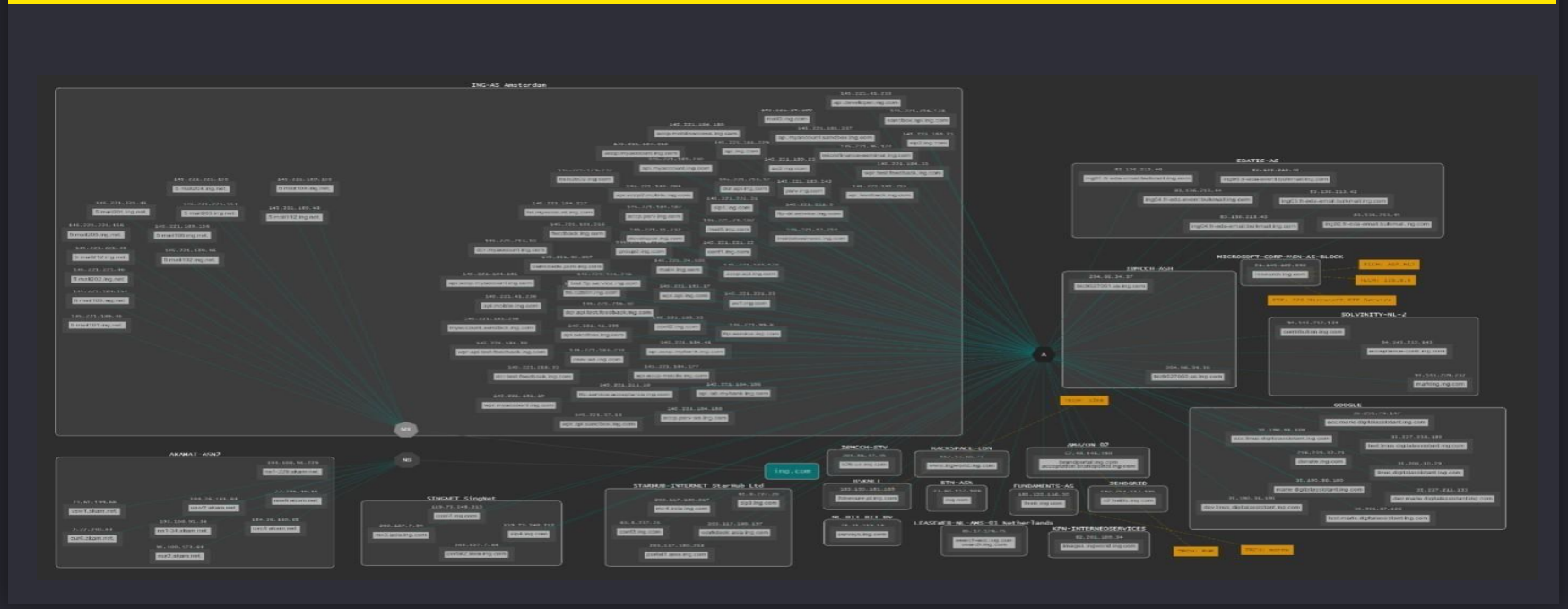
LEGNAGYOBB KOCKÁZATOK

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

Javaslataink | Külső kitettségek csökkentése

- 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.



Aktuális biztonsági kérdések

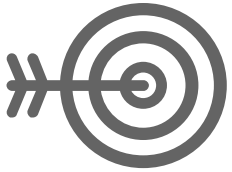
1. Ismeri-e a szervezet teljes külső kitettségét, lehetséges betörési pontokat?
2. A biztonságtudatossági képzések intenzitása/hatékonysága megfelelő-e?
3. Adathalászat megelőzése, mint kiemelt támadási kockázatai?
4. Banki összeolvadások, felvásárlások kockázatai?
5. Szektorspecifikus biztonsági kérdések (AFR, PSD2, számlavezető rendszerek)?
6. Az ágazati certek ajánlásait figyelik, alkalmazzák?
7. Központi védelmi rendszer kialakítása (pl.: SOC) megtörtént?

Javaslataink - Fókuszterületek

Minőségbiztosítás

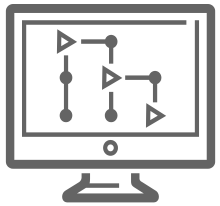
- Külső/belső fejlesztések
- Beszállítók
- Technológiai megoldások bevezetése

Biztonsági vizsgálatok



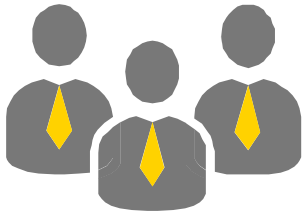
- Sérülékenység vizsgálatok
- Célzott betörési tesztek
- Forráskód vizsgálatok
- Technológiai tesztek

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.