# Információbiztonsági aktualitások 2023.

Siket Csaba 2023. május 26.

# Információbiztonsági kihívások

- Az új sérülékenységek száma rohamosan növekszik (0 day / CVE )
- Egyre hamarabb képesek kihasználni a sérülékenységeket
- Work from Home elterjedése - COVID
- Orosz- ukrán háború és hatásai
- Megnövekedett erőforrás és időigény, szakemberhiány, megtartás
- ChatGPT – óvatosan!

# Sérülékenységek alakulása

- Ismert sérülékenységek száma (CVE/ év)
  - 2004- 1300 db
  - 2014- 9465 db
  - 2020- 30 680 db
  - 2021- 28 506 db
  - 2022- 34 553 db

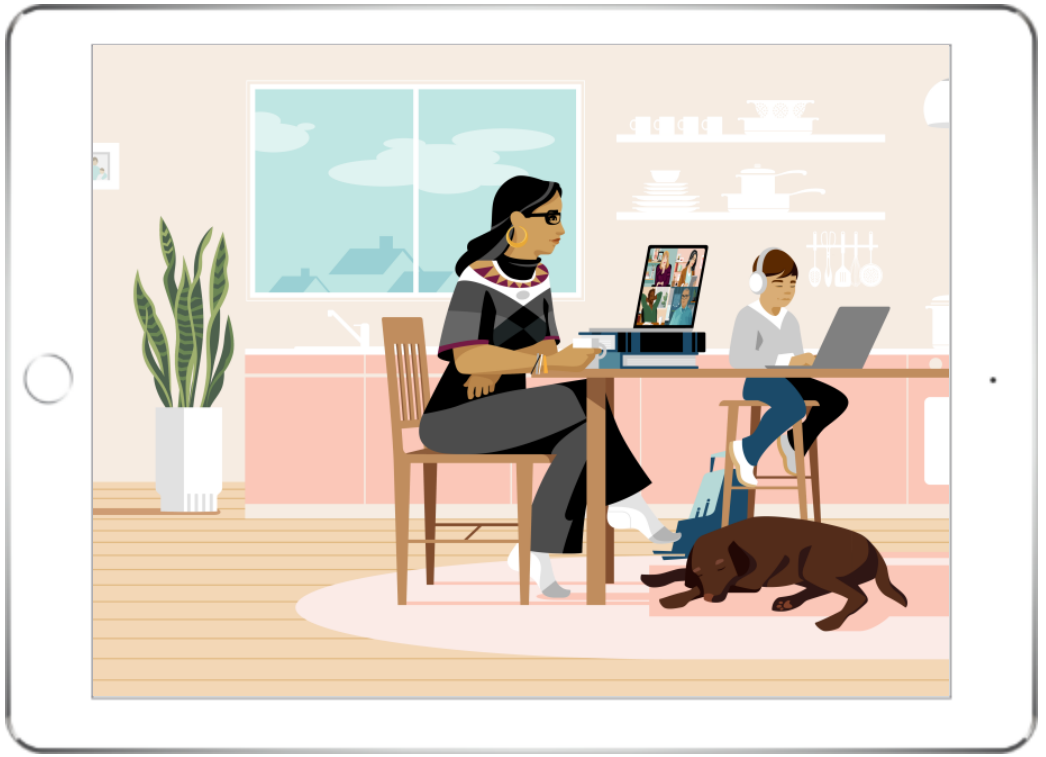
A megjelenő sérülékenységre átlagban 15 percen belül reagálnak

Exploitok készítésének ideje folyamatosan csökken, 2022-ben

Zero day sérülékenységek száma

# Work from Home

- Megnövekedett kiberbiztonsági kockázat az alacsonyabb szintű, otthoni kontrol környezet miatt
  - Fizikai biztonsági korlátai
  - Hozzáférés ellenőrzés kihívásai
  - Adatszivárgás, adatvesztés lehetősége
  - Nyilvános hálózat vs. belső védett környezet
  - Nem „hardenelt” helyi hálózati környezet
- Új technikai megoldások kiépítésének költsége, a lojalitás és a munkavállalók megtartásának kihívásai.



# Orosz – ukrán háború hatása

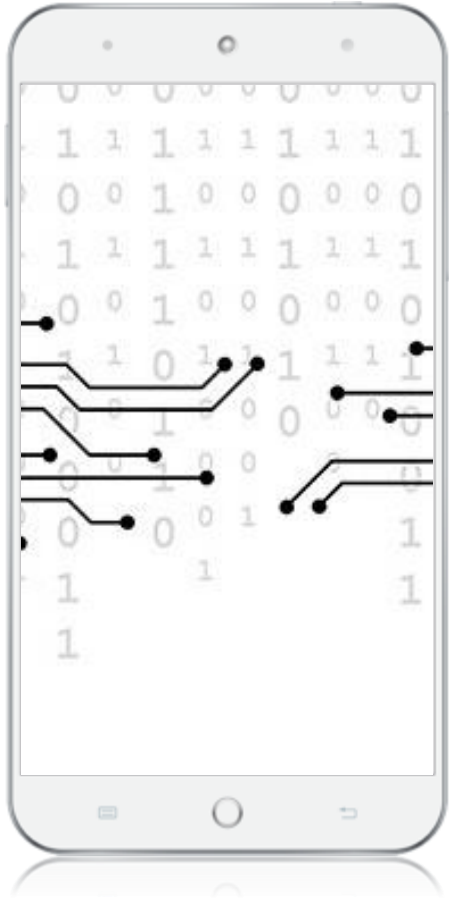
Kiberháború az orosz –ukrán felek és támogatóik között

Ukrajna infrastruktúra elemei és az állami intézmények elleni digitális támadás már a háború előtt megkezdődött.

Elsődleges célpontok az energia, a közlekedés, a vízügy, az egészségügy, másodlagosan a pénzügyi szolgáltatók és a média.

A háború nem csak a kibertérben található adatok, digitális infrastruktúra degradálását vagy megszűntetését célozzák, hanem információgyűjtés, hírszerzés illetve dezinformációs, befolyásolási céljuk is van –deepfake.

Ezekben a támadásokban nem csak az egyes országok katonai és hírszerzéssel foglalkozó szervezetek vesznek részt, hanem az azokkal szimpatizáló, támogató „civil” csoportok is. A támadások ezekre a szervezetkre országokra is eszkalálódott.



# Az ENISA - Fenyegetettségi trendek 2022-ben

A támadások egyre szofisztikáltabbak és az MI felhasználása is erőteljesebb!

- Zsarolóvírusok
- Rosszindulatú programok (malware-ek)
- Megtévesztésen alapuló támadások
- Az adatokkal szembeni fenyegetések
- A rendelkezésre állás elleni fenyegetések: DDoS
- A rendelkezésre állás elleni fenyegetések: internetes fenyegetések
- Dezinformáció
- Ellátási láncok elleni fenyegetések

# Mit tehetünk?

- Automatizált/ Komplex információbiztonsági megoldások – MI megbízható
- Security Operational Services – saját vagy szolgáltatói
- EU szabályozói kezdeményezések – pl. DORA rendelet, DFP
- Tudatosság - ismeretlen szerző – „Tanulni – tanulni – tanulni”
  - (Folyamatos oktatás – magas felhasználói biztonsági tudatosság elérése)
- Zero Trust – „a bizalomnál csak az ellenőrzés fontosabb”
- Magyarországi szakmai közösségekkel történő információ és tapasztalat csere
  - Lessons learned

# Köszönöm szépen a figyelmet!

***Segítünk az embereknek anyagi biztonságot teremteni egy életen át***

# Mit tehetünk?

- 2023 Q1 Ukrajna volt a fő célpont az orosz APT támadásoknál (60%)
- A adathalászkampányok fő célja a védelmi és az energiaszektorban
  - a kampányok elsődleges célja a hírszerzés, a zavarás és az érzékeny adatok kiszivárogtatása volt Ukrajnával szemben.
  - 2023 első három hónapjában Ukrajnát célzó tevékenységek
  - a Sandworm, az APT28és egy fehérorosz csoport, amelyet Pushcha néven tevékenykedett.