



NMHH

Nemzeti Média- és Hírközlési Hatóság

Cyber Threat Intelligence
(CTI) aktuális kérdései

NMHH - HTE –EIVOK Konferencia
2024. május 2.

eivok

HÍRKÖZLÉSI ÉS INFORMATIKAI
TUDOMÁNYOS EGYESÜLET
INFORMÁCIÓBIZTONSÁGI
SZAKOSZTÁLY

Hogyan használja a CTI-t a Hatóság a
szakfeladatai ellátáshoz?

Dr. Orbán József
Szakértő

NMHH Védelmi és Rendészeti
Frekvenciagazdálkodási
Igazgatóság

Mottó

Az informatika

- *nem foghatja mindig a felhasználók kezét*
- *nem láthatja előre a felhasználók cselekvéseit és*
- *nem lesz hatékony vezetői elkötelezettség nélkül!*



A kiber játszma fehér oldala:

A megelőzés a legfontosabb szereplői:

- *a felhasználók*
- *a vezetők és*
- *az informatika*

A Kiber Fenyegetettség Felderítésében (CTI) a munkatársak és a vezetés elkötelezettsége kulcstényező lehet!

Milyen kiberbiztonsági fenyegetettsége lehet a Hatóságnak?

- Kémkedés (nem polgári oldalon)
- Ipari kémkedés (polgári oldalon)
- Ransomware támadások
- Phishing
-

Források

- Nyílt Forrású Felderítés (OSINT, nyilvános forrásokból)
- **Zárt Forrású Felderítés**
 - *Saját, vagy*
 - *partneri adatbázis*
 - *Folyamatos partneri információcsere*
- [Emberi Felderítés (HUMINT: hálózati csatlakozás, beépülés)]
- Technikai Felderítés (műszaki információk, IT)

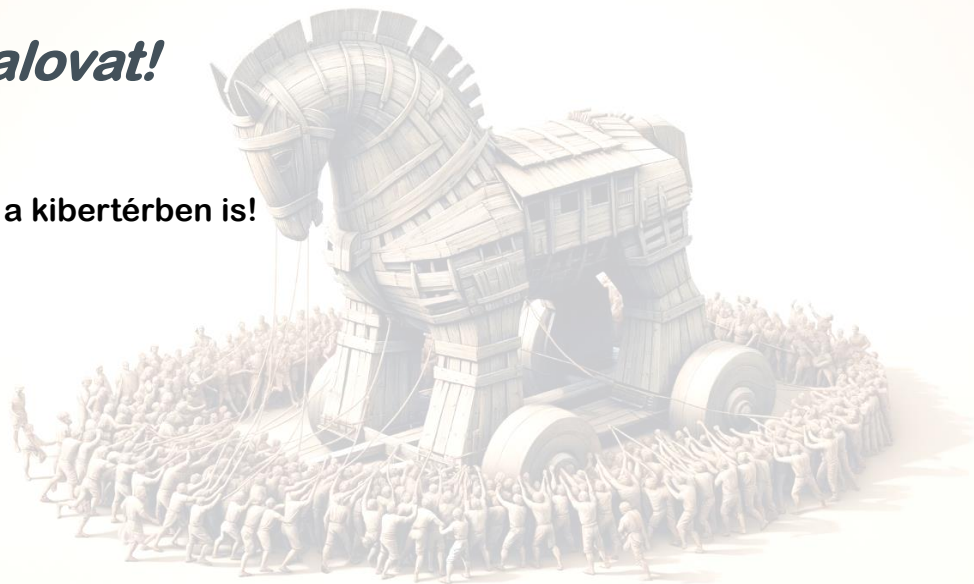


Zárt forrású felderítés

- Partner szervezetekkel kapcsolattartás
- Partner szervezeteket ért támadás elemzése, értékelése
- A megfelelő válaszlépések kidolgozása és alkalmazása

Megelőzés minden szinten:

- Proaktív védelem :
Ne vonszoljuk be a trójai falovat!
 - Fenyegtettség felismerése
 - ***Ne akarjuk a védelmet megkerülni!***
 - Tartózkodjunk a kockázatos helyektől a kibertérben is!
 - ***Vezetőként se legyünk kivételek!***
- Informált döntéshozatal
 - Fontos, és
 - Elengedhetlen
- Munkatársi támogatás (nem csak IT!)
 - Kiberveszély felismerésének képessége
 - Veszély észlelése esetén felettes és IT haladéktalan értesítése
- Adekvát vezetői kockázatkezelés
 - Szoftverfrissítések kötelező és rendszeres letöltése



Nem polgári példa:

- *Információcsere biztonságos felületen és korlátozott módon*
 - *Hozzáférés hatóságok közötti magas szintű megállapodással!*
 - *Nem publikus tárhely használata*
 - *Információ frissítéskor csak annak tényét kapják meg az érintettek*
 - *Kapcsolattartási vonalak rendszeres ellenőrzése*
 - *Kapcsolattartók személyének rendszeres ellenőrzése*



NMHH

Nemzeti Média- és Hírközlési Hatóság

Thank you

Köszönöm a figyelmet!



Dr. Orbán József

Szakértő

NMHH Védelmi és Rendészeti
Frekvenciagazdálkodási
Igazgatóság