NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023. 30. hét

HÍREK

- Nulladik napi sebezhetőséggel törtek fel egy tucat norvég kormányzati IT rendszert
- Sürgősen patchelendő a Citrix ADC kritikus sérülékenysége
- Így védhetjük az ESXi virtuális környezeteket egy új, egyre gyakoribb ransomware taktikával szemben
- Távoli kódfuttatási hiba (RCE) került javításra az OpenSSH továbbított ssh-agentjében
- A Lazarus APT csoport kiemelt célpontjai a Microsoft IIS webszerverek

Heti IT biztonsági tipp

Helymeghatározás - használjuk, de csak okosan!

STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint
- Események eloszlása csapdatípusok alapján
- Támadott port szerinti eloszlás

KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD
E078 ABD3 E75D

NEWS

IT biztonsági
HÍREK

Nulladik napi sebezhetőséggel törtek fel egy tucat norvég kormányzati IT rendszert

(bleepingcomputer.com)

A norvég nemzetbiztonsági hatóság (NSM) megerősítette, hogy az Ivanti Endpoint Manager Mobile (korábbi nevén: MobileIron Core) nulladik napi sebezhetőségét felhasználva illetéktelenek hozzáfértek az ország 12 minisztériuma által használt szoftverplatformhoz. **Bővebben...**

Sürgősen patchelendő a Citrix ADC kritikus sérülékenysége

(cisa.gov)

Múlt hét során biztonsági frissítés vált elérhetővé a Citrix Application Delivery Controller (ADC) és NetScaler Gateway rendszerekhez. A sérülékenység többféle módon is kihasználható, valós incidens is ismert, miközben továbbra is több ezer sérülékeny verzió érhető el az Interneten keresztül. **Bővebben...**

A Lazarus APT csoport kiemelt célpontjai a Microsoft IIS webszerverek

(bleepingcomputer.com)

Az észak-koreai állami támogatású Lazarus hackercsoport előszeretettel intéz támadásokat Windows Internet Information Service (IIS) webszerverek ellen, például rosszindulatú szoftverek terjesztéséhez. **Bővebben...**

Távoli kódfuttatási hiba (RCE) került javításra az OpenSSH továbbított ssh-agentjében

(securityaffairs.com)

A Qualys Threat Research Unit (TRU) kutatói távoli kódfuttatási sebezhetőséget (RCE) fedeztek fel az OpenSSH továbbított ssh agentjében. **Bővebben...**

IT biztonsági
TIPP

Így védhetjük az ESXi virtuális környezeteket egy új, egyre gyakoribb ransomware taktikával szemben

(truesec.com)

Kiberbiztonsági szakértők arra figyelmeztetnek, hogy megemelkedtek a **VMware vSphere ESXi** virtuális szerverkörnyezetek elleni ransomware támadások — sajnos már hazai cég is szerepel az áldozatok között. A Truesec ajánlása szerint az ESXi hosztokat ellenállóbbá tehetjük a ransomware támadásokkal szemben egy kevésbé ismert beállítással. **Bővebben...**

IT biztonsági Tipp

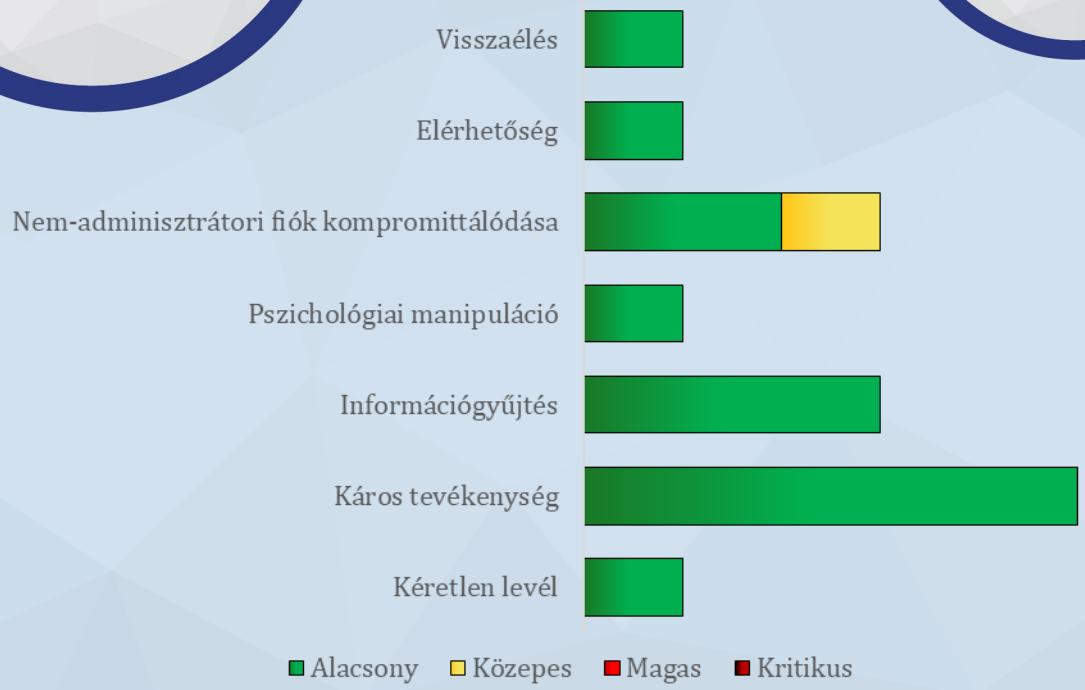
E heti tippünkben a helymeghatározással kapcsolatban szeretnénk megosztani néhány tanácsot. Ha okosan használjuk ezeket a technológiákat, biztonságosan hozhatjuk ki belőlük a legtöbbet a nyaralás idején és a hétköznapok során.

Statisztikai adatok

2023.07.21.-2023.07.27.

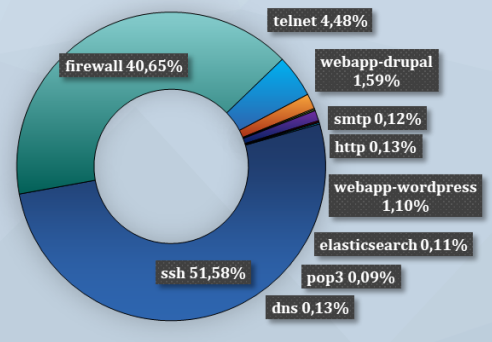
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

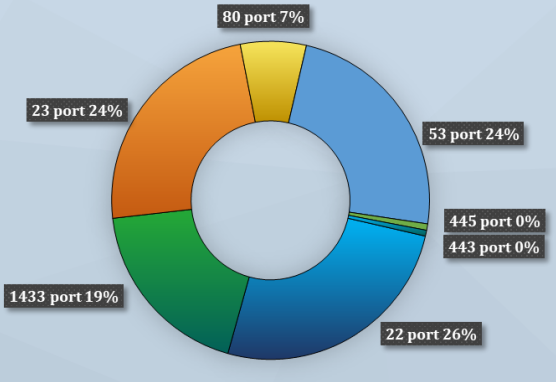
Fenyegetettségi szint: közepes



Incidensek eloszlása típus és kockázati besorolás szerint

Az elosztott kormányzati IT-biztonsági csapdarendszerből (Gov1probe) származó adatok:





További információkért, látogasson el **weboldalunkra**!