NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023. 38. hét

HÍREK

- A Fehér Ház arra kötelezné a CRI-tag országokat, hogy ne fizessenek váltságdíjat a kiberbűnözőknek
- 12 000 Juniper tűzfal vált sebezhetővé egy RCE sebezhetőséggel szemben
- Már aktívan használják a deepfake technikát a kibertámadások során
- Új funkció érkezett a Windows 11-be az NTLM-alapú támadások kiküszöbölésére
- Kubernetes sebezhetőségek kerültek javításra

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

A Fehér Ház arra kötelezné a CRI-tag országokat, hogy ne fizessenek váltságdíjat a kiberbűnözőknek

(therecord.media)

Az Egyesült Államok Nemzetbiztonsági Tanácsa (NSC) közös nyilatkozat kiadására sürgeti a nemzetközi zsarolóvírus elleni kezd eményezésben (International Counter Ransomware Initiative — CRI) résztvevő országok kormányait, amelyben kijelentik, hogy nem fizetnek váltságdíjat a kiberbűnözőknek. **Bővebben...**

12 000 Juniper tűzfal vált sebezhetővé egy RCE sebezhetőséggel szemben

(thehackernews.com)

Egy új kutatás szerint közel 12 000 Internetre kitett Juniper tűzfal eszköz sebezhető egy nemrég nyilvánosságra hozott távoli kódfuttatási hibával (RCE) szemben. **Bővebben...**

Már aktívan használják a deepfake technikát a kibertámadások során

(securityaffairs.com)

A Retool szoftverfejlesztői vállalatot deepfake és smishing technikát is felhasználó kibertámadás érte, amelynek következtében több mint két tucat felhőalapú ügyfélfiókuk kompromittálódott. **Bővebben...**

Kubernetes sebezhetőségek kerültek javításra

(thehackernews.com)

A Kubernetes-ben felfedezett három magas kockázati besorolású sérülékenység (CVE-2023-3676, CVE-2023-3893, CVE-2023-3955, CVSS 8,8) kihasználásával az egy klaszteren belüli Windows végpontokon emelt jogosultságokkal történő távoli kódfuttatás (RCE) érhető el. **Bővebben...**

Windows 11

Új funkció érkezett a Windows 11-be az NTLM-alapú támadások kiküszöbölésére

(bleepingcomputer.com)

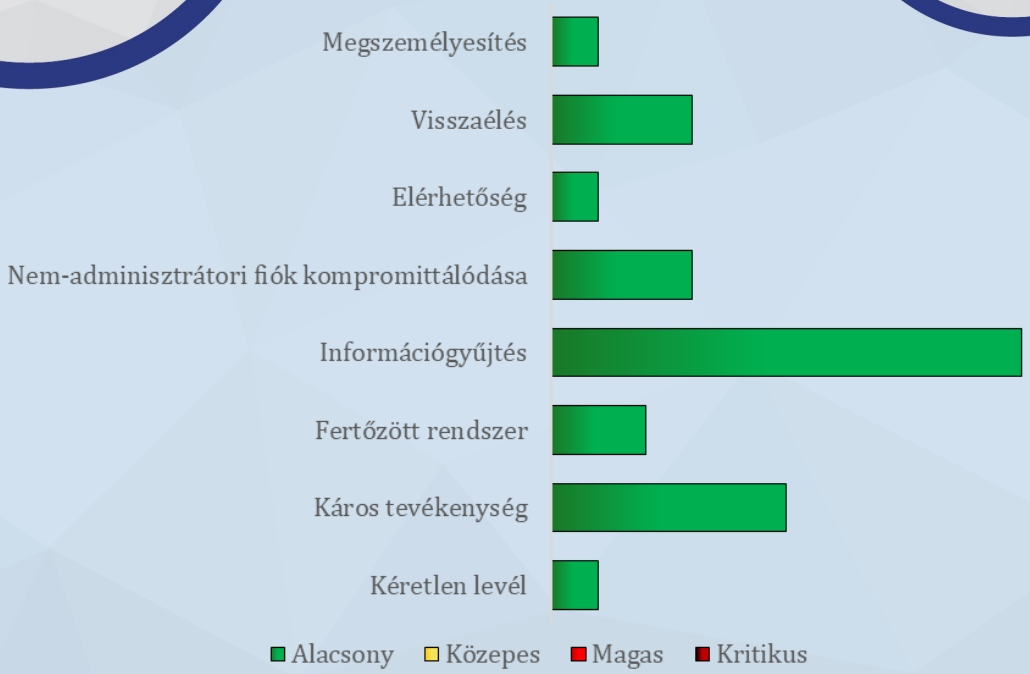
A Microsoft egy új biztonsági funkcióval egészítette ki a Windows 11-et, amellyel a rendszergazdák blokkolhatják az NTLM-et az SMB-n keresztül a pass-the-hash, NTLM relay vagy jelszófeltörő támadások megakadályozása érdekében.
Ez módosítja a hagyományos megközelítést, ahol a Kerberos és az NTLM hitelesítés a célkiszolgálókkal a Windows SPNEGO segítségével működött.
Bővebben...

Statisztikai adatok

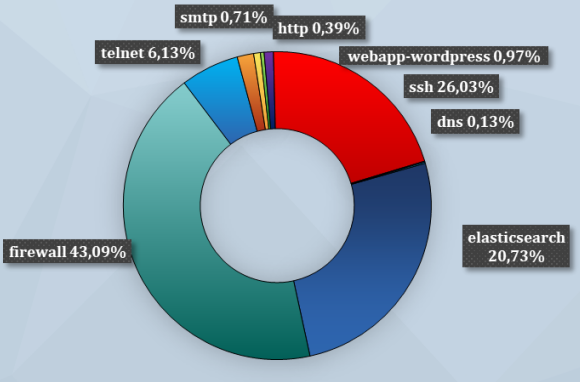
2023.09.15.-2023.09.21.

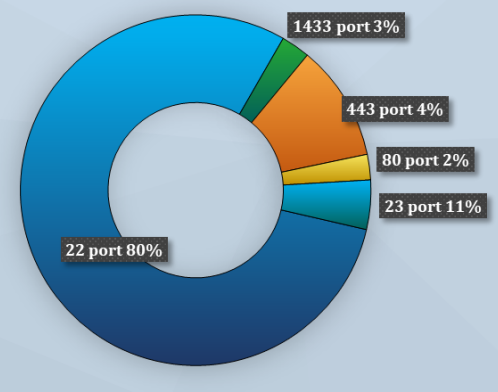
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint
Az elosztott kormányzati IT-biztonsági csapdarendszerből (Gov1probe) származó adatok:





További információkért, látogasson el **weboldalunkra**!