NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 29. hét

HÍREK

- A Cloudflare Application Security jelentésének összegzése: Proof of Conceptek kihasználása, és DDoS támadások
- APT csoport használt ki egy Windows Zero-day sérülékenységet a letiltott Internet Explorer segítségével
- Kritikus Exim sérülékenység veszélyeztet 1.5 millió levelezőszervert
- Az APT27 újra akcióban Európában
- Egy kritikus Cisco hiba miatt a hackerek root felhasználókat adhattak hozzá SEG eszközökhöz

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 Cloudflare Application Security jelentésének összegzése: Proof of Conceptek kihasználása, és DDoS támadások
(bleepingcomputer.com)

A Cloudflare 2024-es alkalmazásbiztonsági jelentést adott ki, amely a 2023 május és 2024 március közti időszak feltörekvő fenyegetési trendjeiről ad beszámolót. **Bővebben...**

APT csoport használt ki egy Windows Zero-day sérülékenységet a letiltott Internet Explorer segítségével
(securityweek.com)

A Trend Micro állítása szerint a Void Banshee névre keresztelt APT kihasznált egy Windows zero-day sérülékenységet, és így kódot tudott futtatni a letiltott Internet Exploreren keresztül. **Bővebben...**

Kritikus Exim sérülékenység veszélyeztet 1.5 millió levelezőszervert
(bleepingcomputer.com)

A Censys arra figyelmeztet, hogy 1.5 millió Exim mail transfer agent-et (MTA) nem patcheltek egy kritikus sérülékenységgel szemben, amely lehetővé teszi a támadók számára, hogy áthatoljanak a biztonsági szűrőkön. **Bővebben...**

Az APT27 újra akcióban Európában
(x.com)

A német Bundesamt für Verfassungsschutz arra figyelmeztetett, hogy az APT27 hackercsoport ismét támadásokat hajt végre Európa szerte, és a már korábban ismert RSHELL malware új verzióit használják fel a támadások során. **Bővebben...**

Egy kritikus Cisco hiba miatt a hackerek root felhasználókat adhattak hozzá SEG eszközökhöz
(bleepingcomputer.com)

A Cisco javította azt a kritikus sérülékenységet, melyek kihasználásával a hackerek új root felhasználókat adhattak hozzá, illetve egy rövid időre le is kapcsolhattak SEG eszközöket – mindehhez rosszindulatú csatolmányokkal ellátott emaileket használtak fel.
Bővebben...

Aktuális tartalmak

Éves kiberbiztonsági jelentés

az *ENISA Threat Landscape 2023*
című tanulmánya alapján

CTI jelentés

2023 novemberében kiadásra került az *ENISA Threat Landscape 2023* című kiadvány, melynek konkrét célkitűzése, hogy bemutassa a kiberbiztonsági fenyegetések jelenkori állását, leggyakoribb formáit és legújabb részleteit.

Jelen CTI jelentés a fent említett tanulmány feldolgozásával kíván mélyebb betekintést nyújtani a legújabb támadási trendekről.

Elolvasom

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el közösségi oldalainkra!

LinkedIn

Instagram

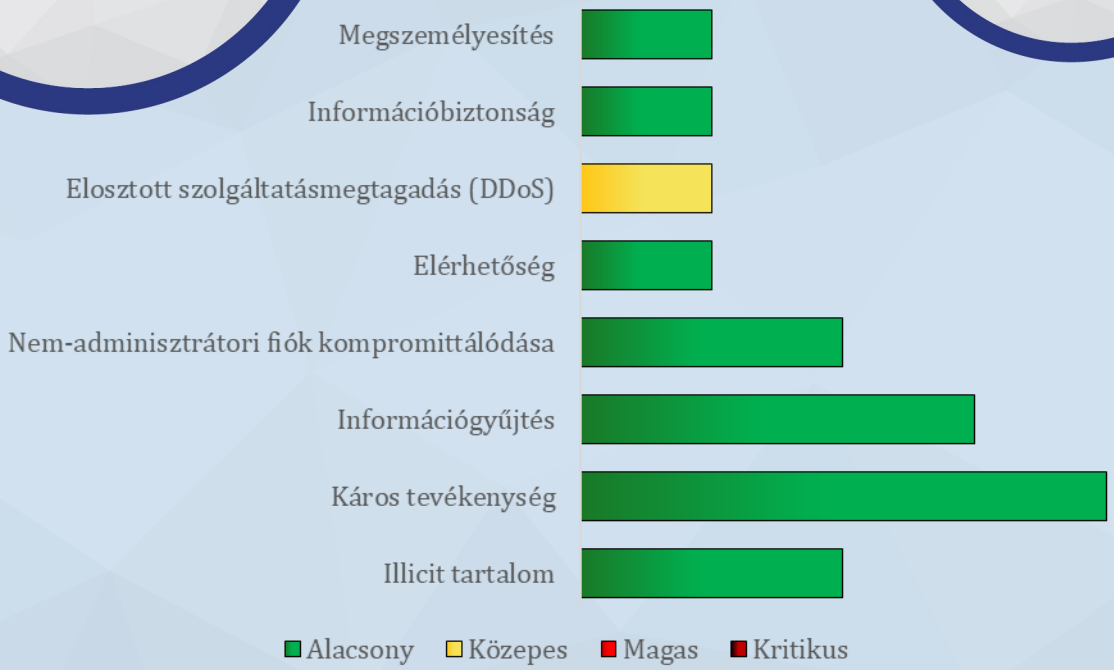
Facebook

Statisztikai Adatok

2024.07.12.-2024.07.18.

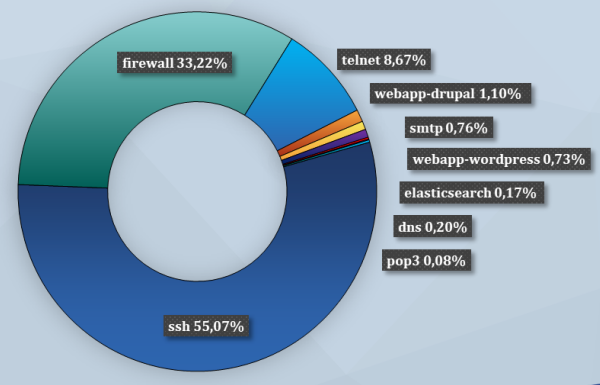
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

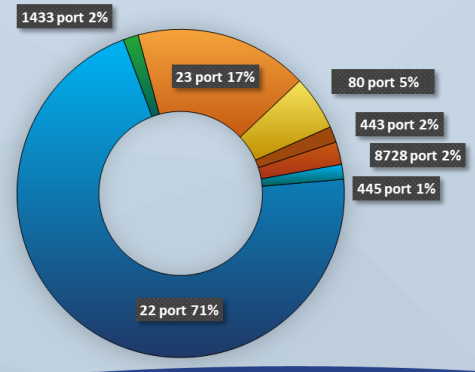
Fenyegetettségi szint: közepes



Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!