NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2024. 17. hét

HÍREK

- Több mint 42 millió dollárt csalt ki áldozataiból az Akira zsarolóvírus
- A HelloKitty nyilvánosságra hozott néhány dekódoló kulcsot
- Két ismerten kihasznált sérülékenységet találtak a Cisco ASA-ban
- PoC exploitot adtak ki a Flowmon súlyos biztonsági réséhez
- Több százezer webhelyet érint a Forminator bővítmény sebezhetősége

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

További érdekességekért, látogasson el **weboldalunkra**!

NEWS

IT biztonsági

HÍREK

Több mint 42 millió dollárt csalt ki áldozataiból az Akira zsarolóvírus

(securityweek.com)

A CISA, az FBI, az Europol és a Holland Nemzeti Kibervédelmi Intézet (NCSC-NL) szerint az Akira több mint 250 szervezetet támadott meg világszerte, és több mint 42 millió dollárt keresett a váltságdíjfizetésekből 2023 eleje óta. **Bővebben...**

A HelloKitty nyilvánosságra hozott néhány dekódoló kulcsot

(bleepingcomputer.com)

A HelloKitty ransomware egyik üzemeltetője bejelentette, hogy a nevét „HelloGookie”-ra változtatja, és elindítja a HelloGookie ransomware műveletet. **Bővebben...**

PoC exploitot adtak ki a Flowmon súlyos biztonsági réséhez

(bleepingcomputer.com)

A Flowmon egyesíti a teljesítménykövetést, a diagnosztikát, valamint a hálózati észlelési és válaszadási funkciókat. Az eszközt világszerte több mint 1500 vállalat használja, köztük a SEGA, a KIA és a TDK, a Volkswagen, az Orange és a Tietoevry. **Bővebben...**

Több százezer webhelyet érint a Forminator bővítmény sebezhetősége

(securityaffairs.com)

A Forminator WordPress bővítmény sebezhetőségére figyelmeztet a japán CERT (továbbiakban: JPCERT). A Forminator egy népszerű plugin, amely lehetővé teszi a felhasználók számára, hogy könnyedén hozzanak létre különféle űrlapokat a webhelyükhöz kódolási ismeretek nélkül, illetve korlátlan fájlfeltöltést tesz lehetővé a szerverre. **Bővebben...**

Két ismerten kihasznált sérülékenységet találtak a Cisco ASA-ba

(thehackernews.com)

Egy új malware kampány a Cisco hálózati eszközeinek két nulladik napi hibáját használja ki, hogy kártevőket juttasson el és megkönnyítse a célkörnyezetekben a titkos adatgyűjtést.
Bővebben...

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

KIBERTÁMADÁS! PODCAST

Adatbiztonság a felhőben - Vendégünk a Tresorit [meglepetés_adás]

Felhő és **adatbiztonság**. Ez a két szó általában nem passzol valami jól, hiszen "a felhő az más számítógépe", és onnantól kezdve, hogy ilyen szolgáltatást veszünk igénybe, bizalmi kérdések merülnek fel. Honnan tudhatjuk, hogy adataink biztonságban vannak egy felhőszolgáltatónál? Mi az a nulla tudás elve? Hogyan használják a kriptográfiát a felhőben?

Következő adásunkban ehhez hasonló kérdésekről beszélgetünk **Balogh Turullal**, aki a témában egy élen járó vállalat, a **Tresorit** információbiztonsági és adatvédelmi csapat vezetője. Levezetésképpen pedig megvitatjuk az **Informatikai Biztonság Napja** részleteit, ami az ország egyik legnívósabb kiberkonferenciája.

Meghallgatom

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

LinkedIn

Instagram

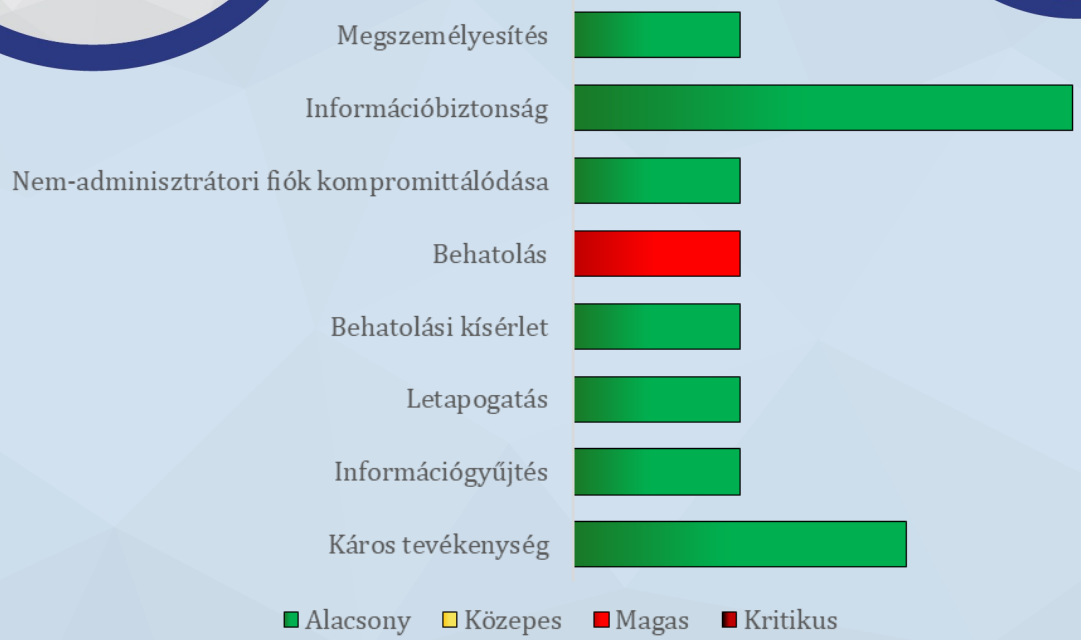
Facebook

Statisztikai Adatok

2024.04.19.-2024.04.25.

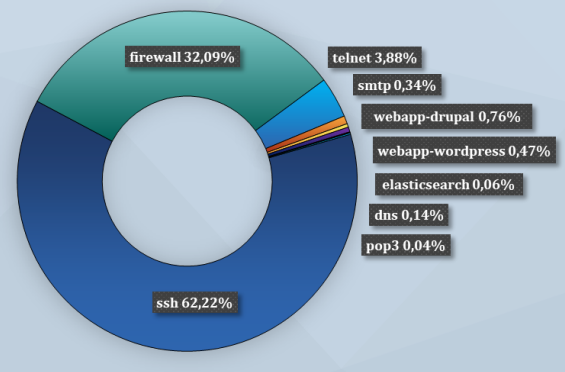
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

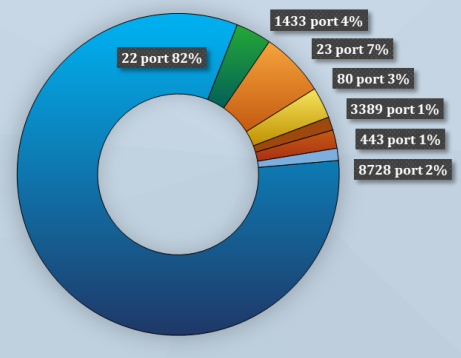
Fenyegetettségi szint: magas



Incidensek eloszlása típus és kockázati besorolás szerint

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





További érdekességekért, látogasson el **weboldalunkra**!