NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023. 43. hét

HÍREK

- Figyelem: A Cisco újabb zero day sérülékenységre figyelmeztet
- Az MI befolyásolhatja az EU választásokat
- Hogyan védekezzünk az adathalászat ellen? Az amerikai kormány útmutatót készített a témában
- Ukrán hacktivisták törték fel a Trigona ransomware csoport szervereit
- A kínai BlackTech a router firmware-ében rejtőzik

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

Európai Kiberbiztonsági Hónap (ECSM)

KIBERBIZTONSÁGI KÉRDŐÍV 2023

A kérdőív összeállításával és az évenkénti rendszeres vizsgálattal az a célunk, hogy felmérjük a magyar lakosság biztonságtudatosságát a kibertérben.
Az eredmények által lehetőségünk adódik arra, hogy pontosabban megtervezhessük, hogy milyen módon szükséges javítani a magyar kibertér védelmét, és ebben a lakosság számára milyen segítség, ismeret vagy készségfejlesztés szükséges.

A kérdőív kitöltése anonim és kb. 6-8 percet vesz igénybe.

A kérdőív segítségével néhány alapvető kiberbiztonsági kockázatra is megpróbáljuk felhívni a figyelmet, illetve ezzel Ön is segíti a mi munkánkat, hogy mindannyian biztonságosabban érezzük magunkat a kibertérben!

https://ec.europa.eu/eusurvey/runner/NKI_kiberbiztonsagi_kerdoiv_lakossagi_2023

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

Nemzeti Kibervédelmi Intézet

@nki.gov.hu

További érdekességekért, látogasson el **Facebook oldalunkra**!

NEWS

IT biztonsági
HÍREK

Figyelem: A Cisco újabb zero day sérülékenységre figyelmeztet

(bleepingcomputer.com) (securityweek.com)

A Cisco a múlt héten figyelmeztette ügyfeleit, hogy a támadók legalább szeptember közepe óta kihasználhatják a CVE-2023-20198 azonosítójú kritikus hibát, távoli hozzáférésre a IOS XR webes felületén keresztül. A hálózatépítő óriás most egy második aktívan kihasznált IOS XE zero day sebezhetőségre hívta fel a figyelmet, amelyet fenyegetési szereplők jogosultság kiterjesztésre használhatnak fel, miután hozzáfértek egy sérülékeny rendszerhez. **Bővebben...**

Az MI befolyásolhatja az EU választásokat

(enisa.europa.eu)

Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) 2023-as Threat Landscape jelentésében rámutat, hogy éberségre van szükség a közelgő 2024-es európai választások előtt, az AI chatbotok és a mesterséges intelligencia által támogatott információmanipuláció bomlasztó hatásai miatt. **Bővebben...**

Ukrán hacktivisták törték fel a Trigona ransomware csoport szervereit

(bleepingcomputer.com)

Kiberaktivisták egy csoportja törte fel a Trigona ransomware csoport szervereit, és az összes rendelkezésre álló információ lemásolása után törölte azokat. **Bővebben...**

A kínai BlackTech a router firmware-ében rejtőzik

(cisa.gov)

A BlackTech bizonyítottan képes a router firmware-ének észlelés nélküli módosítására, valamint a routerek megbízhatósági (domain-trust) kapcsolatainak kihasználására. **Bővebben...**

Hogyan védekezzünk az adathalászat ellen? Az amerikai kormány útmutatót készített a témában

(securityweek.com)

Az amerikai Kiberbiztonsági és Infrastruktúra Biztonsági Ügynökség (CISA) valamint az NSA, az FBI és az MS-ISAC közös útmutatót adott ki, amelyben részletesen ismertetik a leggyakrabban használt adathalász technikákat, továbbá ajánlásokat tesznek a támadások hatásának mérséklésére.
Bővebben...

Aktuális tartalmak

KIBERTÁMADÁS! PODCAST

Riasztás Cisco termékeket érintő sérülékenységekről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) riasztást ad ki a Microsoft szoftvereket érintő kritikus kockázati besorolású sérülékenységek kapcsán, azok súlyossága, kihasználhatósága és a szoftverek széleskörű elterjedtsége miatt.

Az NBSZ NKI a biztonsági frissítések haladéktalan telepítését javasolja, amelyek elérhetőek az automatikus frissítéssel, valamint manuálisan is letölthetők a gyártói honlapokról.

A biztonsági figyelmeztetés az alábbi hivatkozáson keresztül érhető el:

Riasztás

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

Nemzeti Kibervédelmi Intézet

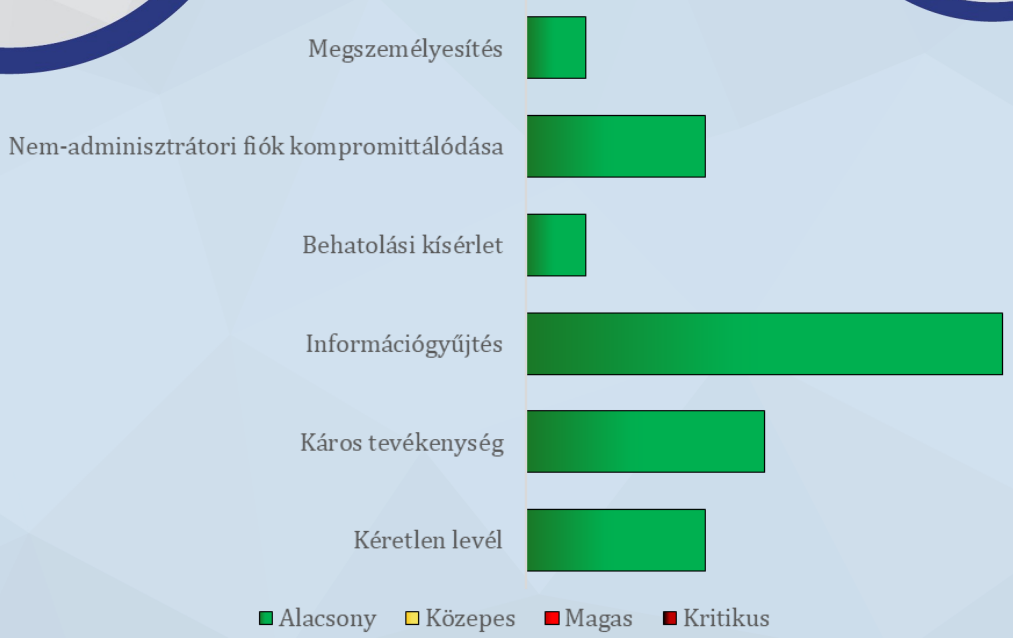
@nki.gov.hu

Statisztikai adatok

2023.10.20-2023.10.26.

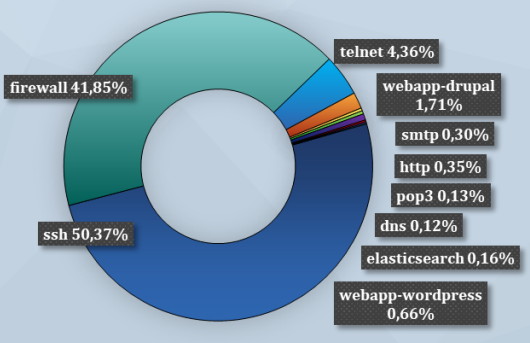
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

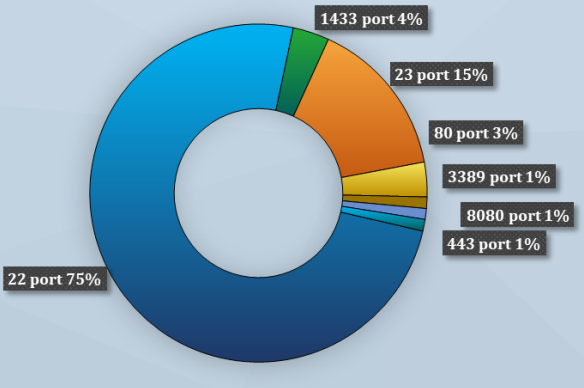
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

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





További információkért, látogasson el **weboldalunkra**!