NEMZETI KIBERVÉDELMI INTÉZET

HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023. 47. hét

HÍREK

- A CISA aktívan kihasznált Windows, Sophos és Oracle hibákra figyelmeztet
- A Google szerint hackerek kihasználták a Zimbra sebezhetőséget a kormányzati szervek elleni támadásokban
- Orosz hackerek a WinRAR exploitját használják ki
- A FortiSIEM kritikus parancsinjekciós hibájára figyelmeztet
- A Microsoft meghosszabbítja az Extended Security Update programját a Windows Server 2012 esetén
- A Windows 10 lehetővé teszi adminok számára az opcionális frissítések telepítésének vezérlését

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

Aktuális tartalmak

NEMZETI KIBERVÉDELMI INTÉZET

1996 NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

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

NEWS

IT biztonsági
HÍREK

A CISA aktívan kihasznált Windows, Sophos és Oracle hibákra figyelmeztet

(bleepingcomputer.com)

A CISA három olyan biztonsági problémát vett fel az ismert sérülékenységek (KEV) katalógusába, amelyek a Microsoft eszközeit, egy Sophos terméket és az Oracle egyik vállalati megoldását érintik. **Bővebben...**

A Google szerint hackerek kihasználták a Zimbra sebezhetőséget a kormányzati szervek elleni támadásokban

(bleepingcomputer.com)

A Google fenyegetéselemző csoportja (TAG) felfedezte, hogy egyes támadók a Zimbra Collaboration e-mail szerver zero day sebezhetőségét kihasználva érzékeny adatokat loptak el több ország kormányzati rendszereiből. **Bővebben...**

Orosz hackerek a WinRAR exploitját használják ki

(bleepingcomputer.com)

Az APT29 (UNC3524,/NobleBaron/Dark Halo/NOBELIUM/Cozy Bear/CozyDuke, SolarStorm) kihasználja a CVE-2023-38831 sebezhetőséget a WinRAR programban, amely a a WinRAR 6.23 előtti verzióit érinti. Lehetővé teszi .RAR és .ZIP archívumok készítését, amelyek által a támadó rosszindulatú kódot futtathat a háttérben. **Bővebben...**

A FortiSIEM kritikus parancsinjekciós hibájára figyelmeztet

(bleepingcomputer.com)

A Fortinet figyelmezteti ügyfeleit a FortiSIEM-et érintő kritikus parancsinjekciós sebezhetőségre, amelyet kihasználva távoli, nem hitelesített parancsokat hajthatnak végre speciálisan kialakított API kéréseken keresztül. **Bővebben...**

A Windows 10 lehetővé teszi adminok számára az opcionális frissítések telepítésének vezérlését

(bleepingcomputer.com)

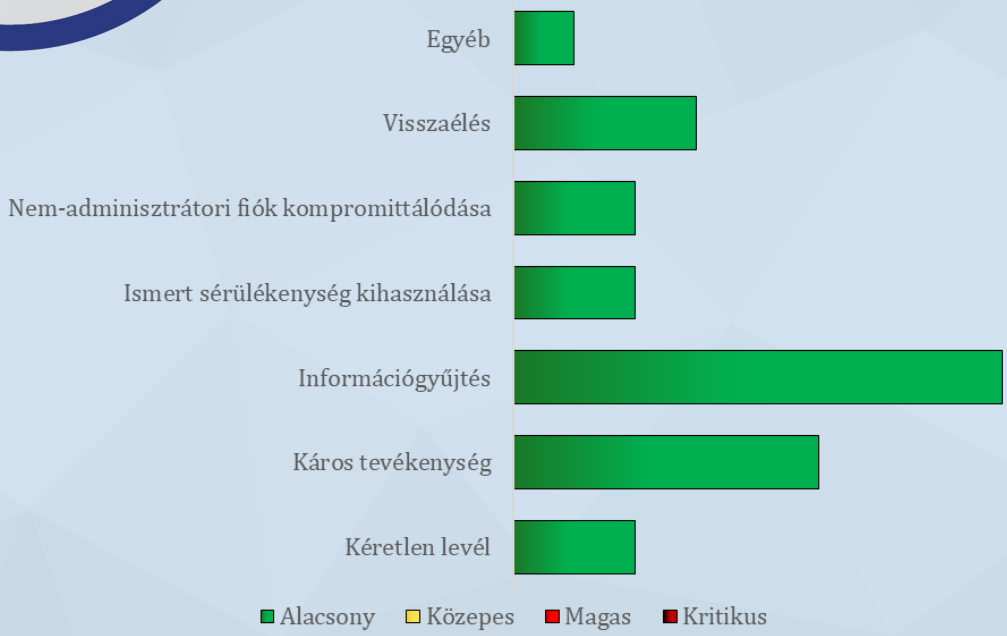
A Microsoft bejelentette, hogy lehetővé teszi a rendszergazdák számára az opcionális frissítések telepítésének ellenőrzését a Windows 10 vállalati végpontokon. A házirend a novemberi opcionális frissítés telepítése után lesz elérhető, és Group Policy Object-ként vagy Configuration Service Provider-ként konfigurálható. Kiválasztható lesz, hogy a havi előzetes frissítések hogyan kerüljenek a felhasználókhoz a Windows Update for Business rendszeren keresztül. **Bővebben...**

Statisztikai adatok

2023.11.23.-2023.11.29.

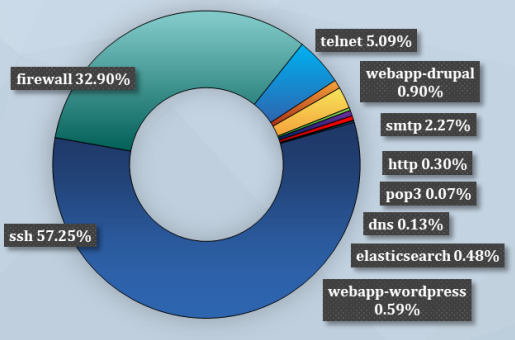
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

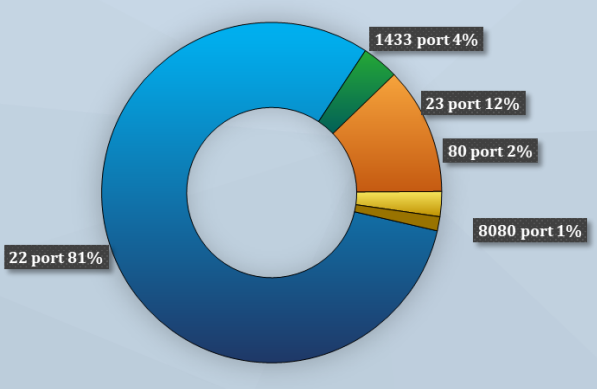
Fenyegetettségi szint: alacsony



Incidensek eloszlása típus és kockázati besorolás szerint

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





További információkért, látogasson el **weboldalunkra**!