NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2025. 42. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58 A2D0 E9DD E078 ABD3 E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- PODCAST
- RIASZTÁSOK
- TÁJÉKOZTATÁSOK

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

A Windows 10 támogatásának megszűnésével járó kiberbiztonsági kockázatok

(gbhackers.com)

2025. október 14-én a Microsoft hivatalosan is leállította a Windows 10 frissítéseinek támogatását, ezzel véget vetve a történelem egyik legszélesebb körben használt operációs rendszerének rendszeres technikai támogatásának, funkciói frissítéseinek és biztonsági javításainak. A rendszeres frissítések hiányában a Windows 10 rendszereket futtató eszközök egyre inkább sérülékennyé válnak majd. **Bővebben...**

A MonsterV2 egy újgenerációs kártevő, amely önállóan támad

(thehackernews.com)

A Proofpoint biztonsági kutatói részletesen feltárták a TA585 nevű fenyegető szereplő működését, aki a MonsterV2 nevű, komplex kártevőt terjeszti. Ez a malware többfunkciós eszköz: egyszerre működik adatlopóként, távoli vezérlésű trójaiként (RAT) és kártevőterjesztőként (loader). A TA585 különös figyelmet érdemel, mert teljesen önállóan végzi a támadásokat. **Bővebben...**

Sebezhetőség a bizalmas számítási környezetekben

(techxplore.com)

Az érzékeny adatok védelme érdekében a felhőszolgáltatók speciális, bizalmas számítási környezeteket (confidential computing environments) alkalmaznak, ahol sem a szolgáltató, sem a gazda operációs rendszer nem férhet hozzá az adatokhoz. Ezek a környezetek lehetővé teszik az adatok biztonságos feldolgozását. **Bővebben...**

Az ASUS három, az Armoury Crate-et érintő sebezhetőséget javított

(asus.com)

ASUS 2025. október 13-án új biztonsági szoftverfrissítést adott ki, amely az Armoury Crate rendszerkezelő alkalmazást érinti. A javítás három ismert sérülékenységet orvosol, amelyek azonosítója: CVE-2025-9336, CVE-2025-9337, CVE-2025-9968. **Bővebben...**

Javítatlan Ivanti-t érintő zero-day sebezhetőségek

(cyberinsider.com)

A Zero Day Initiative (ZDI) nyilvánosságra hozott 13 javítatlan sebezhetőséget, amelyek az Ivanti Endpoint Managert érintik. A sérülékenységek közül 12 távoli kódfuttatást (remote code execution – RCE) tesz lehetővé, egy pedig helyi jogosultság-eszkalációs (privilege escalation) sebezhetőség. **Bővebben...**

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

2025. 10. 10. — 2025. 10. 16.

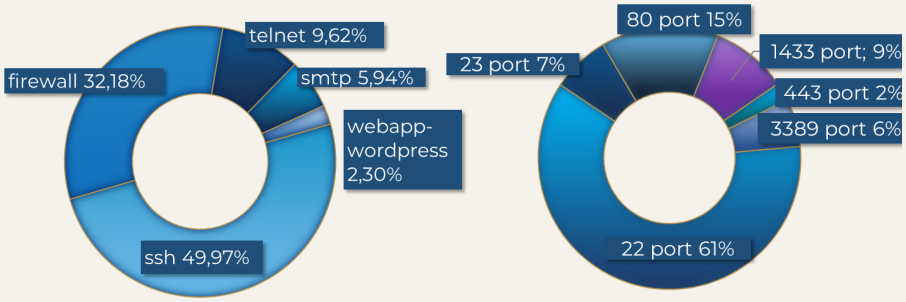
Fenyegetettségi szint:

alacsony | **közepes** | magas | kritikus

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.

Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok



NEMZETI KIBERBIZTONSÁGI INTÉZET

PODCAST

Beszéljünk az auditokról! vendégünk Csernák Gergő [aktuális]

Ebben az adásban Tamás vendége volt **Csernák Gergő információ biztonsági vezető**, akivel gyakorlati szemszögből beszélgetett a **NIS2 kiberbiztonsági auditok** részleteiről.

Gergő **rengeteg tapasztalatot oszt meg a kiberbiztonsági audittal kapcsolatban**, mint például: mik az audit fázisai, hogyan zajlik? Mik egy IBF eszköztárai? Milyen tapasztalatokat lehet leszűrni egy ransomware támadásból? Mik lehetnek a különbségek a követelményrendszerek között? Mik a tapasztalatok az auditorokkal kapcsolatban, és a legfontosabb: hátra dőlhetünk-e egy sikeres audit után?

Adásunkban minderre, és számos egyéb érdekes részletre is rávilágít vendégünk.

Meghallgatom

Érdekli, hogyan formálhatják a jövőt a különböző kiberbiztonsági kihívások?

Fedezze fel velünk a legizgalmasabb témákat, a szakértői tippektől egészen a legújabb trendekig! Kövesse podcastünket a legnépszerűbb felületeken!

RIASZTÁSOK TÁJÉKOZTATÁSOK

Riasztás F5 termékeket érintő sérülékenységekről

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** riasztást ad ki az F5 BIG-IP, F5OS, BIG-IP Next for Kubernetes, BIG-IQ, és APM eszközöket érintő sérülékenységek, valamint a **sebezhető eszközök elleni aktív várható kibertámadási** hullám kapcsán.

Elolvasom

Tájékoztatás feltételezett csaló konferenciaszervező tevékenységről

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet** (NBSZ NKI) tájékoztatót ad ki egy, az InSciTech Summits Pvt. Ltd. néven működő **feltételezett csaló konferenciaszervező tevékenységéről**, amely az elmúlt hetekben több magyar és nemzetközi kutató, illetve felsőoktatási intézmény munkatársait is érintette.

Elolvasom