



AKTUÁLIS TARTALMAK



HÍREK



STATISZTIKAI ADATOK



PODCAST

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el LinkedIn oldalunkra vagy hallgassa meg podcast adásainkat!



HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 15. hét

KONTAKT

@ edt@nki.gov.hu

🔑 FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

🌐 nki.gov.hu



HÍREK

QR-kódok révén terjed egy új adathalász kampány (bleepingcomputer.com)

Az Egyesült Államokban új adathalász kampány terjed, amelyben a támadók bíróságok nevében küldenek hamis, „fizetési felszólítás” (Notice of Default) tárgyú szöveges üzeneteket közlekedési szabálysértésekre hivatkozva. Az üzenetek célja, hogy a címzetteket egy QR-kód beolvasására ösztönözzék, amely egy adathalász weboldalra irányít. **Bővebben...**

A Microsoft javította a Classic Outlook e-mail küldési hibáját (bleepingcomputer.com)

A Microsoft [javította](#) azt a problémát, amely egyes Classic Outlook felhasználóknál megakadályozta az e-mailek küldését az Outlook.com szolgáltatáson keresztül. A vállalat közleménye szerint az érintett felhasználók értesítést kaptak arról, hogy bizonyos üzeneteik nem jutottak el a címzettekhez. A hiba különösen gyakran fordult elő akkor, amikor a levélküldéshez használt Outlook.com-fiók egy másik Exchange -fiókhoz társított Outlook-profil része volt. **Bővebben...**

Nyilvánosságra hozták a Windows „BlueHammer” nulladik napi sérülékenységet (bleepingcomputer.com)

Nyilvánosságra hozta a „BlueHammer” névre keresztelt, Windows zero day sérülékenység kihasználásához szükséges kódokat annak felfedezője, mert nem volt elégedett azzal, ahogyan a Microsoft Biztonsági Válaszközpontja (MSRC) kezelte a bejelentett hiba közzétételi folyamatát. **Bővebben...**

A CISA elrendelte az aktívan kihasznált Fortinet EMS sebezhetőség sürgős javítását (bleepingcomputer.com)

A CISA sürgős intézkedést rendelt el a FortiClient Enterprise Management Server (EMS) rendszereket érintő, aktívan kihasznált sérülékenység kezelése érdekében. **Bővebben...**

Az Anthropic bejelentette a Claude Mythost – Kiberbiztonsági AI-áttörés (securityweek.com)

A kiberbiztonsági iparág Claude Mythos iránti érdeklődése 2026 márciusának végén erősödött fel, amikor a Fortune magazin egy közel 3000 fájlt tartalmazó szivárgás alapján részleteket közölt az Anthropic egyik közelgő fejlesztéséről. **Bővebben...**

STATISZTIKAI ADATOK



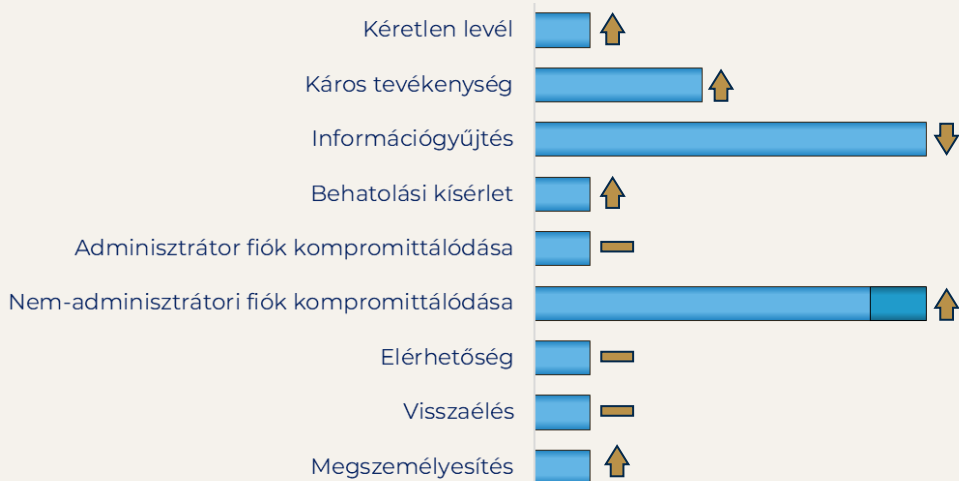
2026. 04. 03. — 2026. 04. 09.

Fenyegetettségi szint:

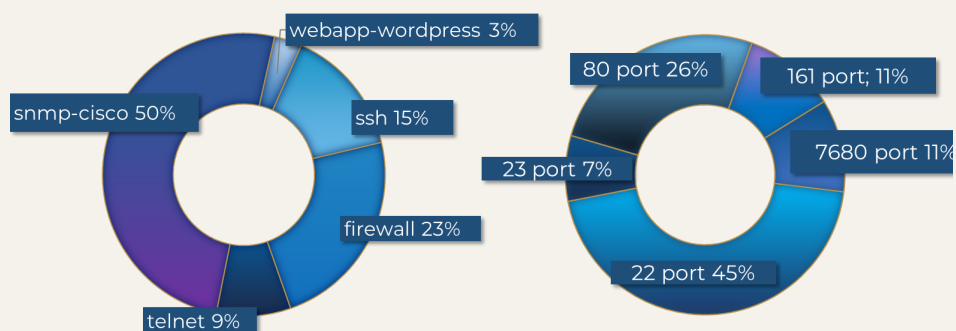


Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.



Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok





PODCAST



Mit tud az a MITRE ATT&CK? [örökzöld]

Munkatársunk, Réka szakdolgozatot ír, mégpedig a támadási **vektorokról**, a támadások felismeréséről, de leginkább a **MITRE ATT&CK keretrendszeréről**. Ismerkedjünk meg ezzel a "csodamátrixszal", ami könnyen **átláthatóvá és érthetővé teszi a kibertámadások általános lefolyását és a kiberbűnözők gondolatmenetét**.

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!

