NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 24. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- RIASZTÁSOK
- CTI RIPORT

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

20 000 Instagram-fiókot törhettek fel egy MI-eszköz kihasználásával

(securityweek.com)

A Meta tájékoztatása szerint mintegy 20 ezer Instagram-fiók eshetett áldozatul egy közelmúltbeli támadásnak, amely során a támadók egy mesterséges intelligenciával ellátott fiók-helyreállítási eszközt használtak ki. A támadók a Meta chatbotját vették rá arra, hogy a saját e-mail-címüket kapcsolja össze a célzott fiókokkal. **Bővebben...**

Kritikus UniFi OS sérülékenységek root jogosultsághoz vezethetnek

(bleepingcomputer.com)

A Ubiquiti UniFi OS Server három, már javított sérülékenységének láncolt kihasználásával hitelesítés nélkül, távoli kódfuttatás (RCE) érhető el rendszergazdai jogosultsággal az érintett rendszereken. A hibákat 2026 májusában javították, és a UniFi OS Server 5.0.6-os vagy korábbi verzióit érintik. **Bővebben...**

Több százezer felhasználót érinthet a Tchap biztonsági incidense

(bleepingcomputer.com)

A francia kormány digitális ügyekért felelős szervezete, a DINUM megerősítette, hogy illetéktelenek hozzáférést szereztek a Tchap kormányzati kommunikációs platformhoz egy kompromittált felhasználói fiókon keresztül. Az incidensre az ANSSI figyelt fel, a támadás forrását azonosították és a hozzáférést azonnal megszüntették. **Bővebben...**

Hamis BlueWallet oldal terjeszt macOS kártevőt

(malwarebytes.com)

Egy a valódi Bitcoin-tárcaként ismert BlueWallet nevével visszaélő, hamis weboldal a Mac-felhasználókat veszi célba. Maga a BlueWallet nem kompromittálódott, a kiberbűnözők csupán a legitim szolgáltatás nevét és arculati elemeit használják fel arra, hogy a rosszindulatú letöltés megbízhatónak tűnjön. **Bővebben...**

RoguePlanet: A „rémálom folytatódik”

(bleepingcomputer.com)

Mindössze néhány órával a 2026. júniusi Patch Tuesday frissítések megjelenése után Nightmare Eclipse nyilvánosságra hozta a RoguePlanet nevű, hetedik Windows zero-day exploitját. A teljesen patchelt Windows 10 és Windows 11 rendszerek egyaránt sebezhetők. **Bővebben...**

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

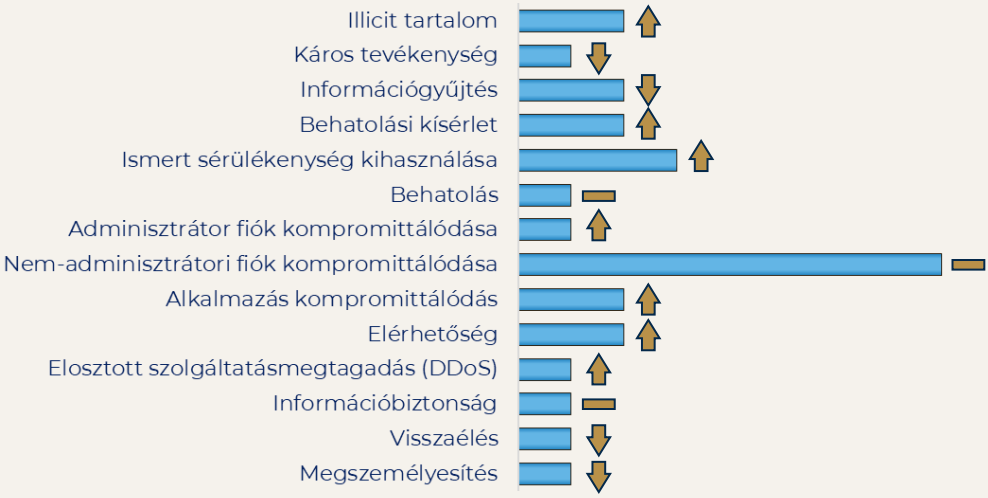
2026. 06. 05. - 2026. 06. 11.

Fenyegetettségi szint:

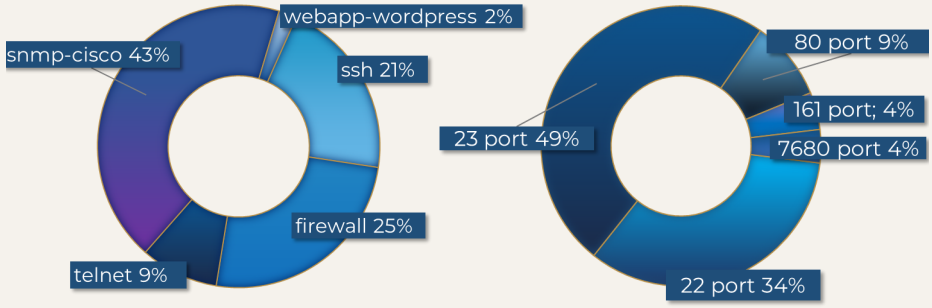
alacsony | közepes | magas | kritikus

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

RIASZTÁSOK

Riasztás
Microsoft és Adobe szoftverek 2026 júniusában javított sérülékenységeiről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet **riasztást** ad ki a **Microsoft és az Adobe szoftvereket** érintő **kritikus kockázati besorolású** sérülékenységek kapcsán azok súlyossága, a szoftverek széleskörű elterjedtsége, valamint az egyes biztonsági hibákat érintő aktív kihasználások miatt.

Elolvasom

Riasztás
Check Point peremvédelmi eszközök sebezhetőségéről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet **riasztást** ad ki a **Check Point Spark Firewall** és **Quantum Security Gateway** peremvédelmi eszközöket érintő, **kritikus besorolású** sebezhetőséggel kapcsolatban.

Elolvasom

NEMZETI KIBERBIZTONSÁGI INTÉZET

HAVI CTI RIPORT

2026. május havi CTI riport

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet **havi rendszerességgel** ad ki **fenyegetéselemzést**, mely **összefoglalja** a **kibertér globális**, valamint **magyarországi helyzetét**.

A riport megismerése megfelelő támpontot adhat az olvasó számára, hogy szervezete milyen IT biztonsági kihívásokkal nézhet szembe a közeli jövőben.

Elolvasom

Érdekesnek találta elemzésünket? Szívesen olvasna hasonló témakörben?

Figyelmébe ajánljuk *„Szórakozástól a jogsértésig – hogyan használható a DeepFake”* című elemzésünket!