NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 10. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- TÁJÉKOZTATÁS
- IT BIZTONSÁGI TIPP

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

Nyilvános Google Cloud API-kulcsok jelenthetnek kockázatot a Gemini API engedélyezése után

(thehackernews.com)

Egy friss biztonsági kutatás szerint a Google Cloud-projektekben használt API-kulcsok, amelyeket eredetileg elsősorban számlázási azonosítóként kezeltek, váratlanul hozzáférést biztosíthatnak a Gemini (Generative Language) API érzékeny végpontjaihoz. A Truffle Security elemzése szerint közel 3000 „AIza" előtagú Google API-kulcs található nyilvánosan elérhető kliensoldali kódban. **Bővebben...**

Böngészőből indított támadással vehették át az irányítást az OpenClaw felett

(bleepingcomputer.com)

Biztonsági kutatók egy „ClawnJacked" nevű, magas kockázatú sérülékenységet fedeztek fel az OpenClaw saját hosztolású MI-ügynök platformjában. A hiba lehetővé tette, hogy egy rosszindulatú weboldal észrevétlenül átvehesse az irányítást a felhasználó számítógépén lokálisan futó OpenClaw-példánya felett. **Bővebben...**

Javításra került egy aktívan kihasznált nulladik napi Qualcomm sérülékenység

(securityweek.com)

A Google hétfőn bejelentette az Android biztonsági frissítések legújabb csomagjának kiadását, amely közel 130 sérülékenységet javít, köztük egy már aktívan kihasznált nulladik napi (zero-day) sérülékenységet is. A kihasznált sebezhetőség a CVE-2026-21385 azonosító alatt nyomon követhető (CVSS 7,8), és több mint 200 Qualcomm chipset grafikus komponensét érinti. **Bővebben...**

Tömeges iPhone-fertőzések a „Coruna" exploit kittel

(gbhackers.com)

Egy friss kutatás szerint a „Coruna" nevű, kifejezetten összetett iOS exploit keretrendszerrel több ezer iPhone-t kompromittáltak. Nem egyetlen „trükkös app" vagy egyszerű átverés áll a háttérben, hanem egy olyan több lépésből álló támadási csomag, amely régebbi iOS-verziókon képes lehet átvenni a készülék feletti irányítást. **Bővebben...**

OAuth átirányítás, mint támadási felület

(microsoft.com)

A Microsoft Defender kutatói 2026. március elején olyan kampányt írtak le, ahol a támadók az OAuth protokoll egyik szabványos működését használják ki. Bizonyos hibák esetén az identitásszolgáltató (pl. Microsoft Entra ID) átirányítja a böngészőt a korábban megadott visszatérési címre. **Bővebben...**

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

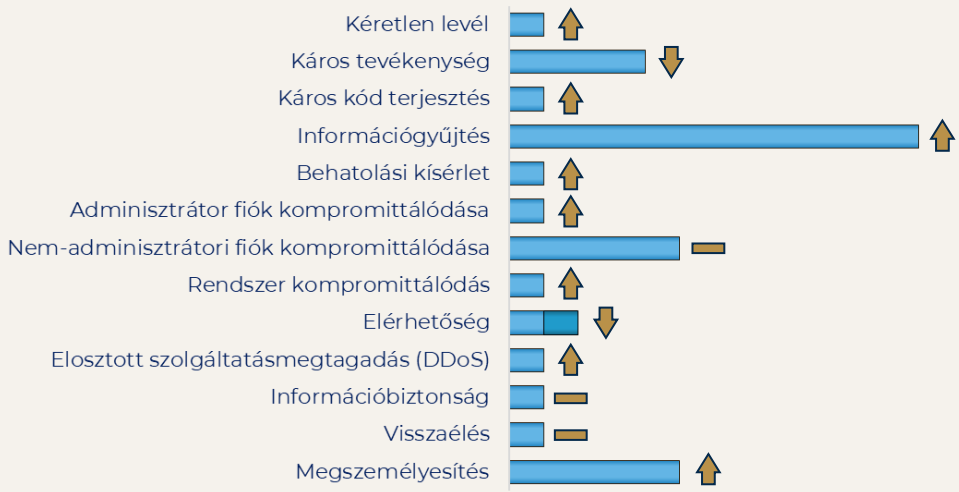
2026. 02. 27. — 2026. 03. 05.

Fenyegetettségi szint:

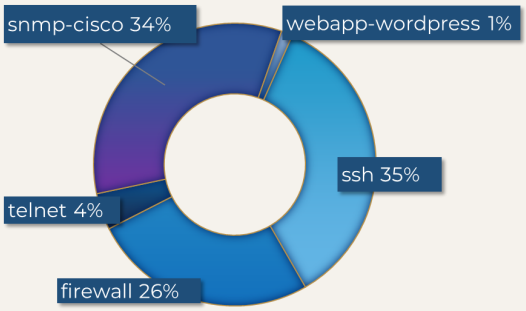
alacsony | **közepes** | magas | kritikus

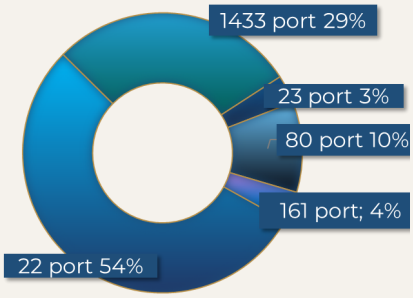
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.



Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok





NEMZETI KIBERBIZTONSÁGI INTÉZET

TÁJÉKOZTATÁS

Tájékoztatás a GLS nevével visszaélő adathalász támadásokról

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) **tájékoztatót** ad ki egy **iMessage**-en terjedő **adathalász kampánnyal** kapcsolatban, amely **visszaél a GLS futárszolgálat** nevével és arculati elemeivel, hogy **személyes és bankkártya adatokat** gyűjtsön.

Elolvasom

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!

NEMZETI KIBERBIZTONSÁGI INTÉZET

IT BIZTONSÁGI TIPP

Így tehető biztonságosabbá a Signal

Mivel az elmúlt időszakban kifejezetten nőtt a **Signal felhasználók ellen irányuló kibertámadások** száma, az **NBSZ NKI** összeszedte azokat a technikákat és beállításokat, amelyekkel **megakadályozható** vagy legalábbis **csökkenthető** annak **a kockázata**, hogy **illetéktelenek hozzáférjenek** a Signal fiókunkhoz és üzeneteinkhez.

Elolvasom

Célkeresztben az üzenetküldő alkalmazások – óvatosan a meghívókkal!

További érdekességekért, hasznos tippekért és tanácsokért olvassa el korábbi tippünket is!