NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 33. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- RIASZTÁSOK
- APT ELEMZÉS
- IT BIZTONSÁGI TIPP

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

EU-s megfelelés, globális hatás: az Anthropic világszerte vízjellel látja el a Claude kimeneteit

(euronews.com)

Az Anthropic 2026. augusztus 2-től láthatatlan jelöléssel látja el a Claude által generált szövegeket és támogatott fájlokat, hogy megfeleljen az Európai Unió AI Act rendelet átláthatósági követelményeinek. A változtatás nemcsak az európai felhasználókat érinti: a vállalat minden olyan régióban alkalmazza a technológiát, ahol a Claude elérhető. **Bővebben...**

Az OpenAI bemutatta új, kiberbiztonsági modelljét, a GPT-5.6-Cybert

(securityweek.com)

Az OpenAI hétfőn jelentette be új, kifejezetten kiberbiztonsági feladatokra fejlesztett mesterségesintelligencia-modelljét, a GPT-5.6-Cybert, valamint a Daybreak Cyber Partner programjának kibővítését. A GPT-5.6-Cyber a GPT-5.6-Sol alapjaira épül, de olyan speciális feladatokra optimalizálták, mint a zero-day sérülékenységek felkutatása, exploitláncok kialakítása, jogosultságkiterjesztés és a hitelesítés megkerülése. **Bővebben...**

Oroszország fokozza a dezinformációs kampányát a németországi tartományi választások előtt

(reuters.com)

A Reuters biztonsági forrásokra hivatkozva arról számolt be, hogy Oroszország jelentősen felerősítette dezinformációs tevékenységét Németországban, néhány héttel a szeptemberi tartományi választások előtt. **Bővebben...**

A csalók a Spotify nevével élnek vissza

(theguardian.com)

Egy újabb adathalász kampányban a Spotify nevével visszaélve próbálják megszerezni a felhasználók bejelentkezési, személyes és bankkártyaadatait. A támadók olyan e-maileket küldenek, amelyek szerint probléma merült fel az előfizetéshez kapcsolódó fizetés feldolgozásával, ezért a felhasználónak frissítenie kell fizetési adatait.
Bővebben...

Lengyelország kibertámadást fedezett fel egy hőerőműnél

(therecord.media)

A lengyel CERT Polska nyilvánosságra hozott egy új jelentést egy 2025. december 29-i kibertámadásról, amely egy közepes méretű, mintegy 50 000 lakost kiszolgáló hő- és villamosenergia termelő erőművet ért.
Bővebben...

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

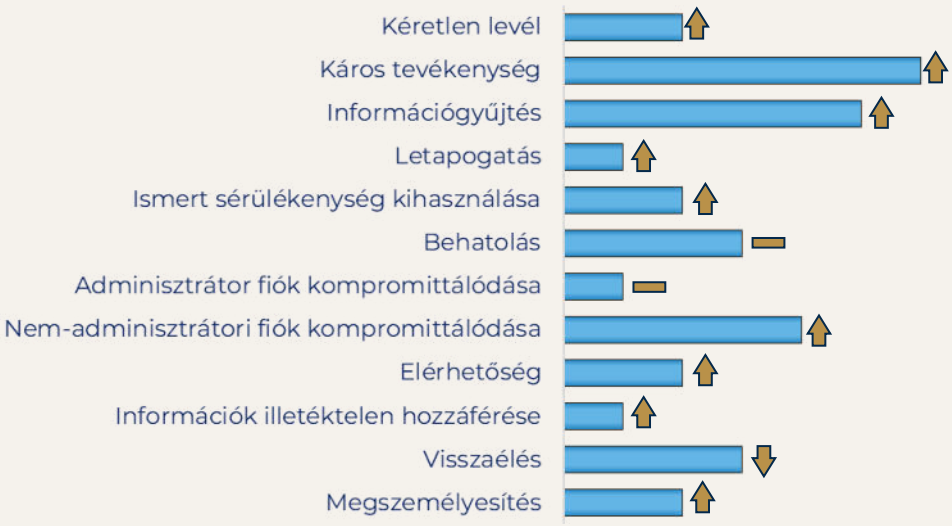
2026. 08. 07. - 2026. 08. 13.

Fenyegetettségi szint:

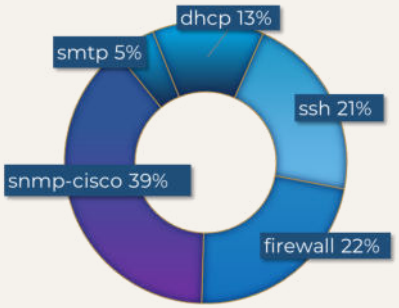
alacsony | közepes | magas | kritikus

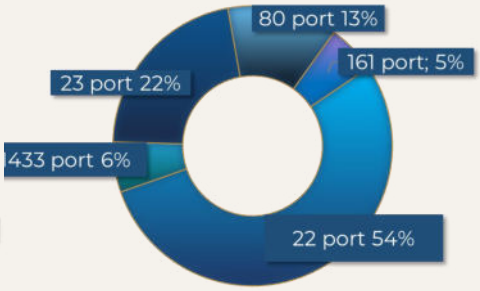
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.



Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok





NEMZETI KIBERBIZTONSÁGI INTÉZET

RIASZTÁSOK

Riasztás a Lazarus „Operation Dream Job” kampányról és a CVE-2026-68820 Windows sérülékenységről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki a **Windows kernelt érintő, észak-koreai kötődésű Lazarus csoport által végrehajtott célzott kampánnyal** kapcsolatban.

A kampány részeként a támadók a Microsoft Windows AFD.sys illesztőprogram egy **korábban nem publikált** (0-day) use-after-free típusú helyi jogosultságkiterjesztési sérülékenységét (CVE-2026-68820) kihasználva kernel szintű rootkitet (FudModule) telepítenek, és **hosszú távú hozzáférést létesítenek** a kompromittált rendszereken.

A támadók **célzott spear-phishing kampányt folytatnak** „álommunka” ajánlatokra építve (Operation Dream Job), trojanizált PDF nézőt és rosszindulatú PDF dokumentumokat terjesztve, amelyek letöltő (MISTPEN) és backdoor (ForestTiger, Troy) komponenseket töltenek le Microsoft Graph / OneDrive infrastruktúra felhasználásával.

Elolvasom

Riasztás Microsoft szoftverek 2026 augusztusában javított sérülékenységeiről

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

A Microsoft tárgyhavi biztonsági csomagjában összesen **421 különböző biztonsági hibát javított**, köztük **3 db nulladik napi (zero-day) sebezhetőséget** is amelyet a Microsoft tájékoztatása szerint támadók kihasználhattak, mivel már a javítás előtt publikálásra került.

Elolvasom

NEMZETI KIBERBIZTONSÁGI INTÉZET

APT ELEMZÉS

A ByteToBreach fenyegető csoport elemzése

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet új elemzéssorozattal jelentkezik, amelyben az Advanced Persistent Threat, vagyis az **egyes APT-csoportok tevékenységei kerülnek bemutatásra**. Az elemzések célja, hogy ismertesse e fenyegetési szereplők **működését, célpontjait, alkalmazott eszközeit és taktikáit**, valamint az **általuk jelentett biztonsági kockázatokat**.

Jelen elemzésben a **ByteToBreach** néven ismert, **pénzügyi motivációjú kiberbűnöző tevékenységét** vizsgáljuk, aki legalább **2025 júniusa óta aktív** adatkereskedőként működik. A szereplő elsősorban **felhő- és vállalati infrastruktúrákban található ismert sebezhetőségeket**, illetve **lopott vagy gyenge hitelesítő adatokat kihasználva** jut kezdeti hozzáféréshez, majd kormányzati szervek, kritikus infrastruktúra-üzemeltetők és nagyvállalatok rendszereiből **szivárogtat ki érzékeny adatokat**, egyre gyakrabban az általa fejlesztett, Linux-alapú "**ByteToCrypt**" zsarolóvírussal kombinált kettős zsarolási (double extortion) módszerrel.

Elolvasom

Érdekesnek találta elemzésünket? Szívesen olvasna hasonló témakörben?

Figyelmébe ajánljuk *„A FrostyNeighbor fenyegető csoport elemzése"* című kiadványunkat!

NEMZETI KIBERBIZTONSÁGI INTÉZET

IT BIZTONSÁGI TIPP

Hogyan rejthetjük el és védhetjük meg alkalmazásainkat iPhone és iPad eszközeinken?

Van, amikor nem szerencsés alkalmazásainkat szem előtt tartani. Egyes javaslatok szerint például jelentősen csökkenthető a képernyőidő, ha a közösségi oldalak alkalmazásait eltávolítjuk a kezdőképernyőről, de a szenzitív adatokat kezelő alkalmazások pl.: banki appok elrejtése is célszerű lehet, különösen, ha illetéktelenek is hozzáférhetnek az eszközeinkhez.

Ennél talán gyakoribb eset, mikor önszántunkból adjuk oda valakinek a telefonunkat, hogy megnézhessen rajta valamit, és nem szeretnénk, hogy az illető belefusson bizonyos appjainkba.

Elolvasom

További érdekességekért, olvassa el korábbi tippünket is!

Ne hagyd, hogy a csalók fesztiválozzanak a pénzedből!