NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 19. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- PODCAST
- IT BIZTONSÁGI TIPP

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

Új korszak vagy tempóváltás? Mit jelent a Claude Mythos a kiberbiztonságban

(anthropic.com)

2026 áprilisában az Anthropic által bemutatott Claude Mythos Preview modell nem csak egy újabb fejlesztés, hanem egy olyan lépés, amely látványosan átrajzolja az autonóm sebezhetőség-kutatás és exploit-fejlesztés eddigi kereteit. A modell megjelenéséről portálunk már április 9-én beszámolt. **Bővebben...**

A megtévesztő „Notepad++ for Mac” weboldal biztonsági kockázatot jelenthet a macOS felhasználók számára

(gbhackers.com)

Egy megtévesztő weboldal jelent meg az interneten, amely „Notepad++ for Mac” néven hirdet letöltést, és azt a látszatot kelti, hogy a Notepad++ natív macOS verziója elérhetővé vált. Az oldal arculati elemei, beleértve a logót, a zöld színvilágot és a vizuális elemeket megtévesztően hasonlítanak a hivatalos Notepad++ projektre, így könnyen félrevezetheti a felhasználókat. **Bővebben...**

Végre érkezik a titkosított RCS alapú üzenetküldés az iPhone és Android eszközök között

(macrumors.com)

Az Apple megerősítette, hogy az iOS 26.5-ös verziója támogatni fogja a végponttól végpontig történő titkosítást (E2EE) az Apple és Android eszközök közötti internet alapú üzeneteknél (RCS). Az Apple még az iOS 26.4-es verzióban kezdte meg az E2EE tesztelését az Android és Apple eszközök közötti RCS üzenetekben. **Bővebben...**

Aktívan kihasználják a Palo Alto zero-day sérülékenységét

(securityweek.com)

A CVE-2026-0300 azonosítón nyomon követett sérülékenység a Palo Alto Networks tűzfalait érinti. A hiba egy puffertúlcsordulás (buffer overflow), amely a PAN-OS rendszer User-ID Authentication Portal (Captive Portal) szolgáltatásában található.
Bővebben...

Kritikus Android-sebezhetőséget javított a Google

(securityaffairs.com)

A Google javította a CVE-2026-0073 azonosítón nyomon követett, kritikus, Android-rendszert érintő sebezhetőséget, amely a System-komponensben lehetővé tette a távoli kódfuttatást felhasználói interakció nélkül.
Bővebben...

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

2026. 04. 30. — 2026. 05. 07.

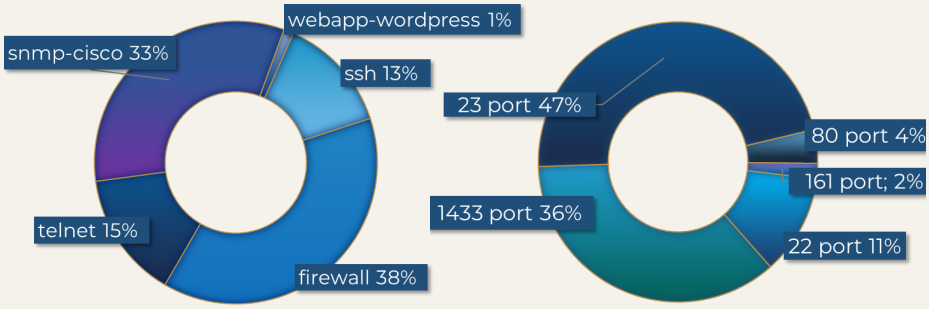
Fenyegetettségi szint:

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

Beszélgessünk újra, Igazgató Úr! - 1.rész [házunk tája]

Ebben az epizódban vendégünk **Szabó Lajos**, **az NKI igazgatója**, akivel az NKI elmúlt néhány évéről beszélgetünk, illetve önreflexiót tartunk.

Lajos jó régen járt már a stúdiószobánkban, akkor az NKI előtt álló feladatokról, tervekről beszélgettünk. **Tekintsünk vissza az elmúlt évekre!**
Ezekből a tervekből mi hogyan sikerült?
Változott azóta az elképzelés?
Esetleg van olyan terv ami időközben átalakult?

Az **önreflexió** közben arra is időnk volt, hogy visszatekintsünk néhány emlékezetes NKI által kezelt **kiberbiztonsági incidensre**, továbbá megválaszolásra kerül a kérdés: **miért változott meg az NKI neve Nemzeti Kiberbiztonsági Intézetre?**

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!

NEMZETI KIBERBIZTONSÁGI INTÉZET

IT BIZTONSÁGI TIPP

Kerüljük el a csalásokat az adóbevallási időszakban is!

Kevesebb, mint egy hónap áll rendelkezésre az **adóbevallás** elkészítésére és az **szja** (személyi jövedelemadó) befizetésére. Ebben az időszakban **jelentősen megugranak** az ilyen témájú **csalások**, ugyanis a kiberbűnözők könnyebben el tudják rejteni a megtévesztő leveleket az ilyenkor amúgy is megnövekedett hivatalos kommunikáció között, ráadásul a **visszatérítés lehetősége** és a **határidők betartása** okozta **kapkodás** miatt **a felhasználók gyakran kevésbé óvatosak** és megfeledkeznek a megkeresések alapos ellenőrzéséről.

Elolvasom

Így tehető biztonságosabbá a Signal

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