NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 20. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- RIASZTÁSOK, TÁJÉKOZTATÁSOK
- PODCAST
- CTI RIPORT

HÍREK

Milliókat vertek át hamis androidos hívásnapló-appokkal

(thehackernews.com)

Több millió felhasználót tévesztettek meg a Google Play alkalmazásboltban elérhető különböző hamis hívásnapló alkalmazásokkal, az ESET kutatói CallPhantom névre keresztelték a rosszindulatú műveletet. Összesen 7,3 milliószor töltötték le a 28 darab hamis alkalmazást, amelyek egyikét 3 millióan telepítették. **Bővebben...**

A támadók mesterséges intelligenciát használtak egy nulladik napi sérülékenység kihasználásához

(bleepingcomputer.com)

A Google Threat Intelligence Group (GTIG) kutatói szerint egy népszerű, nyílt forráskódú, webalapú adminisztrációs eszközt érintő nulladik napi (zero-day) sérülékenység kihasználására szolgáló kód nagy valószínűséggel mesterséges intelligencia segítségével készült. **Bővebben...**

A ShinyHunters csoport tevékenysége az oktatási szektorban több millió diákot érinthet

(abc.net.au)

ShinyHunters kiberbűnözői csoport 2019 óta aktív, elsősorban felhők konfigurációs hibáit, ellopott OAuth tokeneket, supply chain támadásokat és 0-day sérülékenységeket használnak arra, hogy az áldozataiktól adatokat lopjanak, majd pedig ezen adatok nyilvánosságra hozatalával zsarolják őket. Ha az érintett vállalatok nem fizetik ki a követelt összeget, akkor a megszerzett adatokat a dark weben árverezik el. **Bővebben...**

Újabb védelmi funkció érkezik a Signal alkalmazáshoz

(bleepingcomputer.com)

A különféle social engineering és adathalász támadások elleni védelem jegyében a Signal új, alkalmazáson belüli értesítéseket és figyelmeztetéseket vezet be, amelyek célja, hogy elegendő időt biztosítsanak a felhasználóknak a megkeresések valódiságának ellenőrzéséhez.

Bővebben...

Újabb szintlépés a Shai-Hulud ügyben: nyílt forráskódúvá vált a kártékony kód

(theregister.com)

Alig néhány órája számoltunk be arról, hogy a hírhedt, npm csomagokat célzó féreg újra aktívan terjed, és úgy tűnik, igen gyorsan újabb szintet lépett. Ugyanis a TeamPCP malware-csoport minden jel szerint nyílt forráskódúvá tette a Shai-Hulud nevű férget.

Bővebben...

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

2026. 05. 08. — 2026. 05. 14.

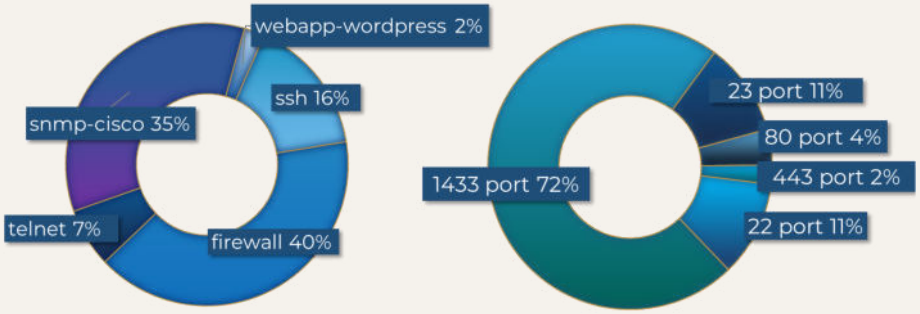
Fenyegetettségi szint:

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, TÁJÉKOZTATÁSOK

Riasztás a Linux rendszereket érintő Dirty Frag sérülékenységről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki a **Dirty Frag** néven ismert, **Linux rendszereket érintő, magas kockázatú kernel sebezhetőségről.**

A sérülékenységek számos ismert Linux disztribúciót érintenek, amelyek 2017 után kiadott kernelverziót használnak.

Elolvasom

Riasztás az NGINX Rift sérülékenységről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki az **NGINX webszervereket érintő, távoli kódfuttatást lehetővé tevő sebezhetőségről**.

A CVE-2026-42945 azonosítón nyomon követett, **NGINX Rift** kódnevű sérülékenység az NGINX **széles körben használt HTTP rewrite modulját**, az ngx_http_rewrite_module-t **érinti**.

Elolvasom

Riasztás Microsoft termékeket érintő sérülékenységekről – 2026. május

Intézetünk riasztást ad ki a Microsoft szoftvereket érintő **kritikus kockázati besorolású sérülékenységek kapcsán**, azok súlyossága, kihasználhatósága és a szoftverek széleskörű elterjedtsége miatt.

Elolvasom

Tájékoztatás Adobe szoftverek sérülékenységeiről – 2026. május

Intézetünk **tájékoztatót** ad ki az **Adobe** szoftverfejlesztő cég **termékeit érintő sérülékenységekkel kapcsolatban**, azok súlyossága, valamint az egyes biztonsági hibákat érintő aktív kihasználások miatt.

Elolvasom

Beszélgessünk újra, Igazgató Úr! - 2.rész [házunk tája]

A Kibertámadás! következő adásában **folytatódik a beszélgetés Szabó Lajossal, az NKI igazgatójával**.

A második rész fókuszában a **NIS2 irányelv hazai átültetése**, az **új kiberbiztonsági jogszabályi környezet**, az **NKI megújuló hatósági és incidenskezelési szerepe**, valamint **Magyarország erősödő nemzetközi kiberbiztonsági jelenléte** áll.

Szó esik az **NCC**-ről és az **uniós forrásokból elérhető kiberbiztonsági pályázatokró**l is, majd a beszélgetés a **jövőbeli fejlesztésekkel** zárul: AI, OT-rendszerek, integrált NKI-platform, megújuló energiatermelők védelme és az incidensbejelentési kultúra erősítése.

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

HAVI CTI RIPORT

2026. április 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 „SS7 protokoll sérülékenységei” című elemzésünket!