NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 25. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- RIASZTÁS
- CTI ELEMZÉS
- PODCAST

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

Kritikus sérülékenység a Splunk Enterpriseban

(cybersecuritynews.com)

A SIEM megoldások egyik fő feladata az, hogy az eszköz maga ne váljon a támadók belépési pontjává. A Splunk Enterprise legújabb, CVE-2026-20253 azonosítóval nyilvántartott sebezhetősége azonban pontosan erre ad lehetőséget a támadóknak.A CVSS 9.8-as, kritikus besorolású hiba lehetővé teszi, hogy egy előzetesen nem hitelesített, azaz semmilyen érvényes fiókkal nem rendelkező támadó teljes kódfuttatási jogosultságot (RCE) szerezzen az érintett rendszeren. **Bővebben...**

Francia nyugdíjrendszert célzó MI-vezérelt adathalász kampány

(brinztech.com)

Egy magas kockázatú, pénzügyi szolgáltatásokat és közigazgatási rendszereket célzó, mesterséges intelligenciával támogatott személyazonosság-lopási műveletet azonosítottak 2026. június 10-én. Az elemzések alapján egy szervezett kiberbűnözői csoport egy nagyméretű, összehangolt adathalász infrastruktúrát épített ki. **Bővebben...**

Ez az új támadás egykattintásos adatlopóvá változtatja a Microsoft 365 Copilotot

(bleepingcomputer.com)

A Microsoft 365 Copilot Enterprise szolgáltatásban felfedezett, SearchLeak névre keresztelt kritikus sérülékenységi lánc lehetővé tehette a támadók számára, hogy egy speciálisan kialakított URL segítségével érzékeny adatokat szivárogtassanak ki a célpont postaládájából, OneDrive vagy SharePoint fiókjából. **Bővebben...**

Több gigabájtnyi adat szivároghatott ki egy amerikai vízszolgáltatótól

(securityweek.com)

A California Water Service (Cal Water), az Egyesült Államok egyik legnagyobb befektetői tulajdonban lévő víziközmű-szolgáltatója vizsgálatot indított, miután az iráni kötődésűként számontartott Handala hackercsoport állítása szerint több gigabájtnyi adatot szerzett meg a vállalat rendszereiből. **Bővebben...**

A Microsoft dolgozik a „RoguePlanet” Defender sérülékenység javításán

(bleepingcomputer.com)

A Microsoft megerősítette, hogy dolgozik a „RoguePlanet” néven ismertté vált, a Microsoft Defenderhez kapcsolódó nulladik napi sérülékenység javításán, amely egy héttel ezelőtt került nyilvánosságra. **Bővebben...**

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

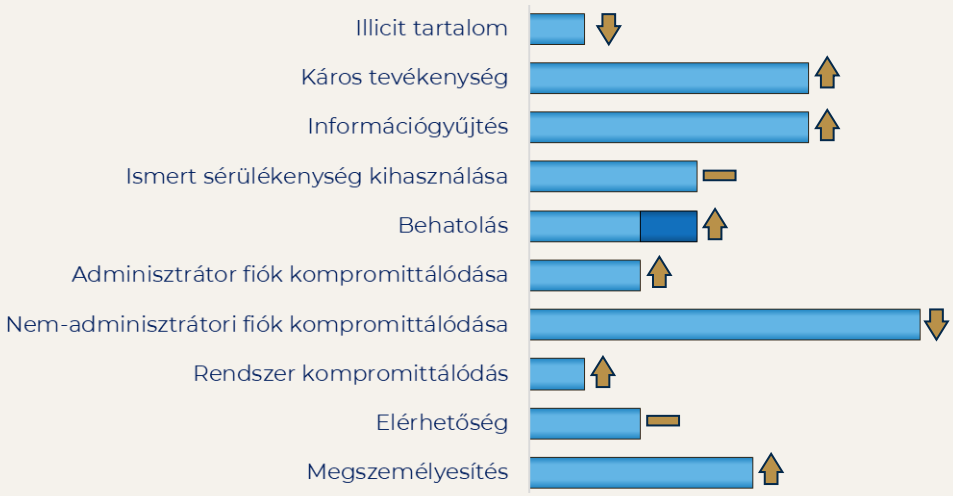
2026. 06. 12. - 2026. 06. 18.

Fenyegetettségi szint:

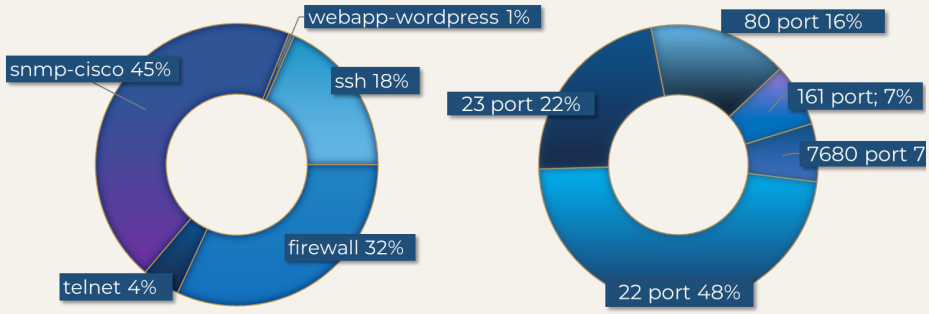
alacsony | közepes | **magas** | kritikus

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

RIASZTÁS

Riasztás
Fortinet VPN- és tűzfaleszközöket érintő aktív kibertámadási tevékenységről

A **Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki** a Fortinet VPN és tűzfal eszközöket érintő, jelenleg is aktív kibertámadási tevékenységgel kapcsolatban.

Nyilvánosságra került információk szerint egy **nagyszabású, automatizált támadási kampány** zajlik internet felől elérhető Fortinet FortiGate eszközök ellen. A biztonsági kutatók által „**FortiBleed**” néven azonosított kampány során a támadók korábban kompromittálódott vagy kiszivárgott hitelesítő adatok felhasználásával kísérlik meg a hozzáférést VPN- és webes menedzsmentfelületekhez. A kutatók szerint **több mint 30 000 működő hitelesítő adat** került nyilvánosságra, amelyek számos szervezet Fortinet eszközeihez biztosíthatnak hozzáférést.

Elolvasom

Sérülékenységek listája

Kövesse folyamatosan frissülő sérülékenység listánkat, hogy naprakész maradhasson a legújabb, és legaktuálisabb fenyegetésekkel kapcsolatban!

NEMZETI KIBERBIZTONSÁGI INTÉZET

CTI ELEMZÉS

Az OT rendszerek hálózatbiztonsága

Az **operatív technológiák (OT) világa a digitalizáció térnyerésével alapvetően megváltozott**, hiszen a korábban jellemző mechanikus működtetést, manuális beavatkozást és helyszíni mérést fokozatosan digitális vezérlési, felügyeleti és adatfeldolgozási megoldások váltották fel. Az OT és az IT fejlődési útja az elmúlt évtizedekben **egyre szorosabban összekapcsolódott**, amelynek eredményeként az ipari rendszerekben is megjelent az IP-alapú kommunikáció, a távoli hozzáférés és a különböző adatkapcsolati megoldások. Bár ez a fejlődés jelentős üzemeltetési előnyöket biztosít, egyúttal **új kiberbiztonsági kockázatokat is teremt**.

Elolvasom

Érdekesnek találta elemzésünket? Szívesen olvasna hasonló témakörben?

Figyelmébe ajánljuk a *„CMS rendszerek biztonsága”* című elemzésünket!

NEMZETI KIBERBIZTONSÁGI INTÉZET

PODCAST

Deepfake - már a szemünknek sem hihetünk? [aktuális]

A Kibertámadás! 111. epizódjában a deepfake jelenség kerül a középpontba. Vendégünk **Dr. Veszelszki Ágnes kommunikáció kutató**, az NKE Nemeskürty István Tanárképző Karának dékánja, aki **Tamással** arról beszélget, **mit jelent a deepfake fogalma**, **hogyan kapcsolódik** a mesterséges intelligenciához, és **milyen formái vannak** a videó-, hang- és kép manipulációnak. Szó esik **ismert deepfake-esetekről**, a **dezinformációról**, valamint arról is, **miért válik egyre nehezebbé** eldönteni, hogy egy online tartalom hiteles-e. Az adás bemutatja a „három T" módszert: Tartalom**, Technológia, Terjesztő**, amely segíthet tudatosabban vizsgálni a gyanús tartalmakat. A beszélgetés végső tanulsága, hogy a digitális világban a biztonság **egyik alapja a médiatudatosság**, a **kontextus értelmezése** és a **kritikus gondolkodás**.

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!