NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 36. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- RIASZTÁSOK
- ESEMÉNY

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

Ügyféladatok kompromittálódtak a Tixelnél

(7news.com.au)

Adatvédelmi incidens érintette a melbourne-i székhelyű Tixel jegyviszonteladó platform felhasználóit. A vállalat tájékoztatása szerint az incidens során a támadók egyes ügyfelek e-mail-címéhez és mobiltelefonszámához férhettek hozzá. A Tixel hangsúlyozta, hogy a támadás nem érintette a felhasználók jelszavait, bankkártyaadatait, fizetési információit és vásárlási előzményeit. A felhasználói fiókok, valamint a hozzájuk kapcsolódó jegyek és hirdetések szintén nem kerültek veszélybe. **Bővebben...**

Kibertámadás érte a McKessont: 284 millió rekord kerülhetett a támadókhoz

(malwarebytes.com)

Kiberbiztonsági incidensről számolt be az amerikai egészségügyi és gyógyszeripari óriás, a McKesson Corporation. A vállalat augusztus 25-én fedezte fel, hogy illetéktelenek fértek hozzá bizonyos külső, harmadik fél által biztosított alkalmazásokhoz, és adatokat is kimentettek azokból. **Bővebben...**

Hamis GTA 6-demó terjeszt Vidar infostealert

(malwarebytes.com)

A GTA VI körüli érdeklődést a kiberbűnözők is kihasználják. A Malwarebytes kutatói olyan hamis Rockstar Games-weboldalakat azonosítottak, amelyek nem létező GTA 6-demót kínálnak letöltésre. Az oldalak a hivatalos Rockstar-megjelenést és a játék promóciós anyagait utánozzák, a „Play Now” vagy „Official Download” gomb azonban egy gta6_installer.exe nevű kártevőt tölt le. **Bővebben...**

Aktívan kihasznált zero-day sebezhetőségek a SonicWall SMA1000-es sorozatban

(sonicwall.com)

A SonicWall 2026. szeptember 1-jén kiadott biztonsági tanácsadójában megerősítette, hogy támadók két, korábban ismeretlen (zero-day) sebezhetőséget láncolnak össze az SMA1000 sorozatú távoli hozzáférési eszközök (Secure Mobile Access) ellen, távoli kódfuttatás (RCE) elérése céljából.

Bővebben...

Nemzetközi összefogással törték meg a Sality botnetet

(bleepingcomputer.com)

Nemzetközi akcióban bénították meg a több mint két évtizede működő Sality P2P-botnetet, amelynek infrastruktúrájához az évek során több mint 11 millió egyedi IP-címet kapcsoltak.

Bővebben...

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

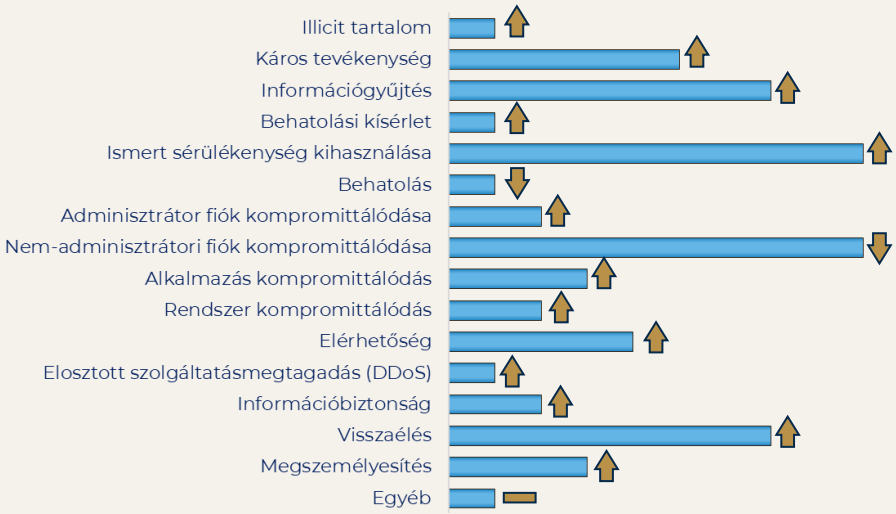
2026. 08. 28. - 2026. 09. 03.

Fenyegetettségi szint:

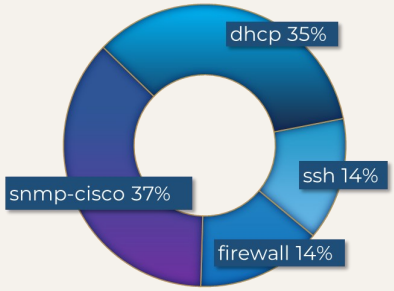
alacsony | közepes | magas | kritikus

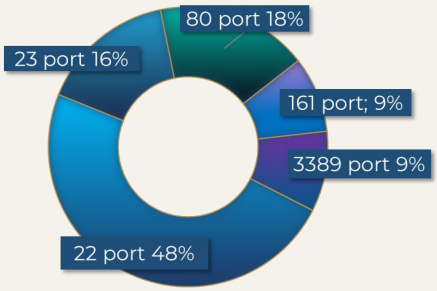
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

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 CVE-2026-73570 Zimbra Collaboration Suite szoftvert érintő sérülékenységről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet **riasztást ad ki a Zimbra Collaboration Suite (ZCS)** szoftvert érintő, CVE-2026-73570 azonosítón nyomon követett kritikus sérülékenység kapcsán.

Intézetünkhöz megnövekedett számú bejelentés érkezett a **CVE-2026-73570 sérülékenység aktív kihasználásáról**. A sebezhetőség kihasználása hitelesítés nélküli támadók számára távoli kódfuttatást tehet lehetővé.

A sérülékenység a Zimbra **SNMP-monitorozási komponensét érinti**, és akkor használható ki, ha az SNMP-értesítések engedélyezve vannak.

Elolvasom

Riasztás Magyarország Ügyészségének nevével visszaélő ransomware támadásokkal kapcsolatban

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet (NBSZ NKI) **riasztást ad ki Magyarország Ügyészségének** nevével és arculati elemeivel visszaélő, zsarolóvírus fertőzéshez vezető **adathalász üzenetekről**.

A bejelentések alapján a támadók **hamis, hivatalos megkeresés látszatát keltő leveleket** küldenek, amelyekben ügyészségi alkalmazottak nevével élnek vissza. A kampány célja az, hogy a felhasználó a levélben szereplő **hivatkozásra kattintson**, majd a megtévesztő oldalon keresztül **rosszindulatú fájlt töltsön le**. A fertőzés végső célja a végponton található dokumentumok, képek, archívumok és más állományok titkosítása, majd váltságdíj követelése.

Elolvasom

NEMZETI KIBERBIZTONSÁGI INTÉZET

ESEMÉNY

Future IT 2026

2026. november 10-12.
Siófok, Azúr Hotel

Nagy örömmel jelentjük be, hogy idén ismét **saját színpaddal készülünk** az ICT Global Future IT konferenciáján, ahol izgalmas témákról beszélgetünk a kiberbiztonság **kiváló, elismert szakembereivel**. Az esemény idén is **több színpaddal és sokszínű, tartalmas programmal** várja az érdeklődőket, remek lehetőséget teremtve a kapcsolatépítésre, az új gondolatok megosztására és az értékes szakmai beszélgetésekre.

2026. szeptember 1. és 2026. október 31. között a **FUTUREIT2026-NKI-VIP** promóciós kód **15% kedvezményt** biztosít a normál jegyárakból.

A kedvezmény a szállásdíjra nem vonatkozik.

Érdekel

Ne maradjon le!

Látogasson el a **kibernaptar.hu** weboldalra és tudja meg milyen további hazai és nemzetközi kiberbiztonsági események várhatók.