



AKTUÁLIS TARTALMAK



HÍREK



STATISZTIKAI ADATOK



IT BIZTONSÁGI TIPP



RIASZTÁSOK



ESEMÉNY

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 40. hét

KONTAKT



edt@nki.gov.hu



FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D



nki.gov.hu



HÍREK

Felhasználói képeket töltöttek fel külső szolgáltatásokhoz az OpenAI MI-ágensei (bleepingcomputer.com)

Az OpenAI megerősítette azt az új biztonsági incidenst, amely során a mesterséges intelligencia (MI) ágensei felhasználók által megadott képeket töltöttek fel külső képtároló szolgáltatókhoz. A vállalat [tájékoztatása](#) szerint eddig 53 ilyen esetet azonosítottak annak az átfogó vizsgálatnak a részeként, amelyet az ágensek nem kívánatos viselkedésével kapcsolatban indítottak még a [Hugging Face-t érintő biztonság incidens](#) következtében. **Bővebben...**

Biztonsági aggályok miatt nem adják ki az OpenAI új modelljét (techcrunch.com)

Az OpenAI még a hónap elején [mutatta be](#) az Astrát, mint eddigi legerősebb modelljét. A cég a következő hónapban tervezte az újabb modell kiadását, azonban biztonsági aggályok miatt úgy döntöttek, egyelőre elmarad a megjelenés. **Bővebben...**

Több tucat szervezetet érinthet a ShinyHunters új PeopleSoft-kampánya (therecord.media)

[Újra](#) aktívan kihasználja a ShinyHunters kiberbűnözői csoport a [CVE-2026-35273](#) azonosítójú, Oracle PeopleSoft rendszereket érintő sérülékenységet. A hibát az [Oracle](#) június 10-én javította, miután a Mandiant korábban jelezte, hogy a támadók május 27. és június 9. között, zero-dayként használták ki, elsősorban felsőoktatási intézmények ellen. **Bővebben...**

Esetleges zero-day támadás miatt a Kiteworks a rendszerek leállítását kérte (heise.de) (therecord.media)

A Kiteworks arra figyelmeztette ügyfeleit, hogy egy esetleges zero-day támadás miatt ideiglenesen állítsák le rendszereiket. A vállalat a hatóságoktól kapott hiteles információkat egy lehetséges támadásról, ugyanakkor jelenleg nincs tudomása a Kiteworks-rendszerek kompromittálódásáról.

Bővebben...

Kibertámadás érte a spanyol Renfe vasúttársaságot (grupo.renfe.com)

A Renfe spanyol állami vasúttársaság rendszereibe behatolás történt egy korábban kompromittálódott vasúti infrastruktúrakezelő vállalat, az Adif szerverei miatt, amelyekkel hálózati kapcsolatban álltak.

Bővebben...

STATISZTIKAI ADATOK



2026. 09. 25. - 2026. 10. 01.

Fenyegetettségi szint:

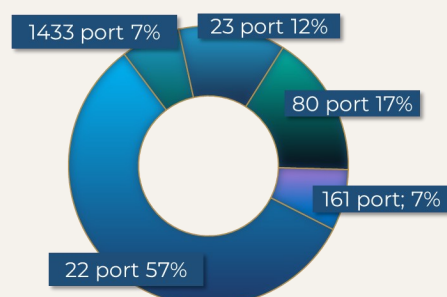
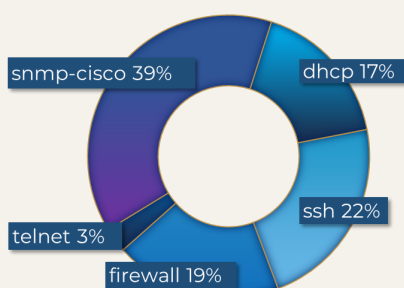


Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.



Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok



RIASZTÁSOK



Riasztás a NetScaler ADC és NetScaler Gateway termékeket érintő sérülékenységekről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete riasztást ad ki a NetScaler ADC és NetScaler Gateway termékeket érintő [CVE-2026-88771](#) és [CVE-2026-88772](#) azonosítójú, aktívan kihasznált kritikus sérülékenységek kapcsán. A gyártó 2026. szeptember 27-én adott ki biztonsági közleményt, amelyben megerősítette, hogy a hibákat a javítások nyilvánosságra hozatala előtt már kihasználták támadók.

Eloivasom

Riasztás a Cisco Catalyst SD-WAN Manager rendszert érintő sérülékenységről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete riasztást ad ki a Cisco Catalyst SD-WAN Manager API-jának hitelesítését érintő, aktívan kihasznált kritikus sérülékenység miatt. A hibát a Cisco közlése szerint 2026 szeptemberében már aktívan kihasználták.

Eloivasom

Riasztás a WordPress Core-t érintő sérülékenységről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete riasztást ad ki a széles körben használt WordPress tartalomkezelő rendszer (Core) aktívan kihasznált sérülékenysége miatt.

A CISA 2026. szeptember 25-én vette fel a KEV-katalógusába. A hiba hitelesítés nélkül kihasználható, és bizonyos feltételek teljesülése esetén távoli kódfuttatáshoz vezethet.

A [CVE-2026-87902](#) azonosítón nyomon követett, magas súlyosságú sérülékenység önmagában helyi fájl beágyazását (Local File Inclusion) teszi lehetővé. Ez távoli kódfuttatássá (RCE) akkor válik, ha a szerverkörnyezet és az aktív téma is teljesít bizonyos előfeltételeket.

Eloivasom



IT BIZTONSÁGI TIPP



Kezdetét veszi az idei ECSM

Az Európai Kiberbiztonsági Hónap (ECSM) az Európai Unió éves kiberbiztonsági **tudatosságnövelő kezdeményezése**, amely még 2012-ben indult az Európai Unió Kiberbiztonsági Ügynökség, az ENISA, valamint az Európai Bizottság támogatásával, illetve az uniós tagállamok, állami intézmények, vállalatok, oktatási intézmények és más szervezetek részvételével. A program célja, hogy felhívja a figyelmet a **tudatos internethasználatra** és a **digitális biztonság fontosságára**.

Sorozatunk első epizódjának jelmondata:

**„Nem tudhatod, hogy ki áll a profil mögött.
A farkas is bújhat báránybőrbe.”**

Sosem lehetünk teljesen biztosak abban, ki áll valójában azok mögött a profilok mögött, akikkel online beszélgetést folytatunk. Éppen ezért fontos, hogy az ilyen digitális kapcsolataink során, **ne szavazzunk feltétlen bizalmat** a másíknak és **soha ne adjunk ki magunkról túl korán bizalmas személyes információkat**, illetve pénzügyi adatokat.

Eolvasom

**További
érdekességekért,
olvassa el korábbi
tippünket is!**

*Gyakori online csalási
kampányok az
iskolakezdési
időszakban*





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!

