



HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 41. hét

KONTAKT



edt@nki.gov.hu



FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D



nki.gov.hu



AKTUÁLIS TARTALMAK



HÍREK



STATISZTIKAI ADATOK



ESEMÉNY



IT BIZTONSÁGI TIPP

További érdekességekért és
IT biztonsággal kapcsolatos
tartalmakért látogasson el
LinkedIn oldalunkra vagy
hallgassa meg podcast
adásainkat!



HÍREK

Elszabadult AI-ügynökök a Wikipedián (therecord.media)

A Wikimedia Foundation 2026. október 5-én közzétett részletes jelentése szerint a feltehetően az OpenAI-hoz köthető AI-ügynökök engedély nélkül szerkesztettek wikiket, egy jegyzetelőeszközt próbáltak feltörni, és hatalmas forgalmat generáltak. Ez a forgalom valószínűleg hozzájárult egy májusi részleges szolgáltatáskieséshez. **Bővebben...**

Kritikus fájllelési hiba az Atlassian Data Center termékekben

(bleepingcomputer.com)
(cert.europa.eu)

Az Atlassian 2026. október 5-én tette közzé a [CVE-2026-21589](#) jelzésű, kritikus sérülékenységet. Bejelentkezés nélkül is elérhetők lehetnek a webalkalmazás gyökérkönyvtárán belüli, pontosan ismert elérési útvonalú fájlok. A hiba nyolc Data Center és Server terméket érint, köztük a Jira Software-t, a Confluence-t és a Bitbucketet. A gyártó CVSS 4.0 szerint 9,3-as, kritikus besorolást adott neki. **Bővebben...**

Megtévesztő ChatGPT- és Gemini-oldalakkal szereznek meg hirdetési fiókokat és MFA-kódokat (bleepingcomputer.com)

Egy új, hirdetési fiókok kezelőit célzó kampány hamis ChatGPT-, Gemini-, Claude- és Perplexity-oldalakat használ a bejelentkezési adatok és a többtényezős hitelesítéshez (MFA) szükséges kódok ellopására. A támadás során a böngésző a böngészőben (browser-in-the-browser, BitB) technikát alkalmazza. **Bővebben...**

18 hónap börtönbüntetésre ítélték egy zenészt AI-botokkal elkövetett streamingcsalás miatt (bleepingcomputer.com)

Egy észak-karolinai zenészt 18 hónap börtönbüntetésre ítélték, miután több mint 10 millió dollár jogdíjat szerzett egy nagyszabású streamingcsalási rendszerrel. Michael Smith a Spotify, Apple Music, Amazon Music és YouTube Music platformjain manipulálta dalainak lejátszási adatait.

Bővebben...

Több tízezer internetre kapcsolt Fortinet tűzfalhoz szereztek hozzáférést a támadók (ic3.gov)

Az FBI riasztást adott ki a FortiBleed nevű támadássorozatról. A bűnözők az internetről elérhető Fortinet FortiGate tűzfalakat és SSL VPN-átjárókat támadják.

Bővebben...

STATISZTIKAI ADATOK



2026. 10. 02. - 2026. 10. 08.

Fenyegetettségi szint:

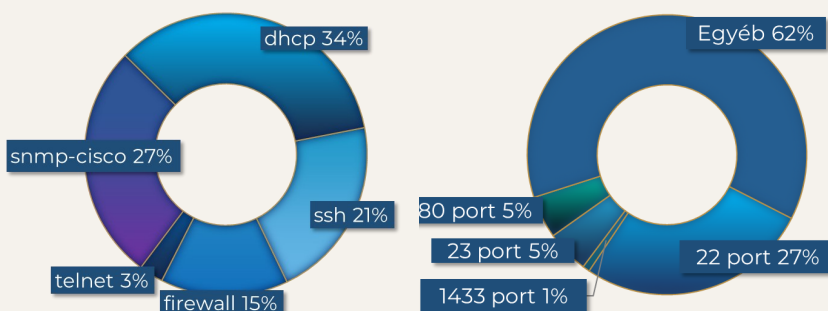


Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok

Az adatsorok melletti nyilak az előző héthez viszonyított változásokat mutatják.



Az elosztott kormányzati IT biztonsági csapdarendszerből (GovProbe1) származó adatok





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!



IT BIZTONSÁGI TIPP



ECSM 2026 – Sok lúd disznót győz

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 második részének jelmondata:

„Sok lúd disznót győz... Használj több faktort fiókjaid védelméhez!”

Az online fiókjaink védelmének egyik legfontosabb eszköze a többtényezős hitelesítés, amelynek lényege, hogy a bejelentkezés során több, egymástól eltérő hitelesítési tényező igazolja a felhasználó személyazonosságát.

Eolvasom

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

*Milyen kockázatot rejt
az OpenAI
számítógépes
előzmények funkciója?*

