NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍRLEVÉL

Nemzetközi
IT biztonsági sajtószemle
2026. 29. hét

KONTAKT

edt@nki.gov.hu

FBC3 88A2 BF51 AD58
A2D0 E9DD E078 ABD3
E75D

nki.gov.hu

AKTUÁLIS TARTALMAK

- HÍREK
- STATISZTIKAI ADATOK
- RIASZTÁSOK
- PODCAST

KIBERTÁMADÁS! PODCAST

NEMZETI KIBERBIZTONSÁGI INTÉZET

HÍREK

EU: jöhet a 13 éves korhatár a közösségi médiában?

(therecord.media)

Az Európai Bizottság fontolóra veszi, hogy a közösségi média használatát 13 éves korhatárhoz kösse – közölte Ursula von der Leyen. Hozzátette: az intézkedés az uniós tagállamokban egységes szabályozást vezetne be, amely korlátozná a szülői vagy gondviselői felügyelet nélkül internetező, 13 év alatti gyermekek hozzáférését a közösségi platformokhoz. **Bővebben...**

Újabb adathalász kampány célozza a LastPass és Bitwarden felhasználóit

(bleepingcomputer.com)

A LastPass egy olyan adathalász kampányra figyelmeztette a felhasználóit, amely hamis biztonsági értesítésekkel próbálja rosszindulatú weboldalakra irányítani az áldozatokat. Az adathalász e-maileket úgy alakították ki, hogy megtévesztésig hasonlítsanak a vállalat hivatalos kommunikációjára. **Bővebben...**

Az Európai Parlament meghosszabbította a CSAM-tartalmak önkéntes szkennelését lehetővé tevő szabályozást

(therecord.media)

Az Európai Parlament megszavazta annak a jogszabálynak a meghosszabbítását, amely lehetővé teszi a nagy technológiai vállalatok számára, hogy önkéntes alapon átvizsgálják a felhasználók kommunikációját a gyermekekkel szembeni szexuális visszaéléseket ábrázoló tartalmak (CSAM – Child Sexual Abuse Material) felderítése érdekében. **Bővebben...**

Új képességeket kapott a RedHook Androidos kártevő

(bleepingcomputer.com)

A Group-IB kiberbiztonsági cég elemezte a RedHook mobilkártevő újabb kiadását, amely a 2025-ös verziójához képest számos új képességgel bővült.

Bővebben...

A Joomla-bővítmények aktívan kihasznált RCE-hibáira figyelmeztet a CISA

(bleepingcomputer.com)

A CISA további két, ezúttal az iCagenda és Balbooa Forms Joomla-bővítmények sebezhetőségeinek aktív kihasználására hívja fel a figyelmet. A hibák a legmagasabb prioritásúként kerültek megjelölésre, így a szövetségi ügynökségeknek három napon belül telepíteniük kell a rendelkezésre álló biztonsági frissítéseket, illetve végrehajtani az enyhítő műveleteket.

Bővebben...

NEMZETI KIBERBIZTONSÁGI INTÉZET

STATISZTIKAI ADATOK

2026. 07. 10. - 2026. 07. 16.

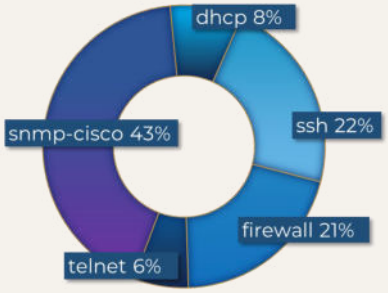
Fenyegetettségi szint:

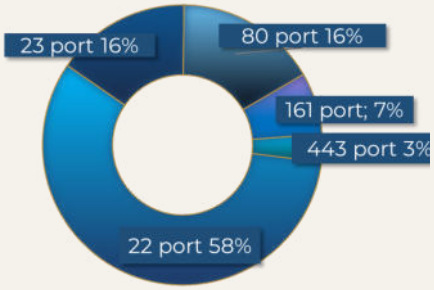
alacsony | közepes | magas | kritikus

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 káros csatolmányt tartalmazó levelekkel kapcsolatban

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki a **Budapesti Műszaki és Gazdaságtudományi Egyetem nevében küldött, káros csatolmányt tartalmazó levéllel** kapcsolatban.

Intézetünkhöz több bejelentés is érkezett arról, hogy ismeretlen elkövetők a Budapesti Műszaki és Gazdaságtudományi Egyetem nevével és arculati elemeivel visszaélő, káros hivatkozást tartalmazó levelet küldenek. Az üzenetekben **árajánlatra hivatkozva próbálják rávenni a címzetteket a csatolmány megnyitására**.

Elolvasom

Riasztás Microsoft szoftverek 2026 júliusában javított sérülékenységeiről

A Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézet riasztást ad ki a **Microsoft szoftvereket érintő kritikus kockázati besorolású sérülékenységek** kapcsán azok súlyossága, a szoftverek széleskörű elterjedtsége, valamint az egyes biztonsági hibákat érintő **aktív kihasználások miatt**.

A Microsoft tárgyhavi biztonsági csomagjában **összesen 622 különböző biztonsági hibát javított, köztük 3 db nulladik napi (zero-day) sebezhetőséget** is amelyet a Microsoft tájékoztatása szerint támadók kihasználhattak, mivel már a javítás előtt publikálásra került.

Elolvasom

PODCAST

Só, bors és... hash? - A jelszavak titkos élete [örökzöld]

Ebben az epizódban a **jelszavak kulisszái mögé nézünk**: mi történik velük a háttérben, hogyan kellene őket biztonságosan tárolni, és miért nem elég önmagában az, ha egy szolgáltatás „hasheli” a jelszavakat.

Tamás és Réka a **plain text jelszótárolás veszélyeiről**, a **hashelés működéséről** beszélnek, valamint arról, hogyan nehezítik meg a támadók dolgát az olyan technikák, mint a **salting, a peppering és a stretching**.

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!