



HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2022.45. hét



HÍREK

- Az angolszász KKV-k aggódnak, hogy az infláció miatt kevesebb jut majd a biztonságra
- SpookySSL sérülékenység: elérhetővé vált az OpenSSL hibajavítás
- Minden Internetre csatlakoztatott eszközt átvizsgálják az Egyesült Királyságban
- Kibertámadás miatt akadozott a vasúti közlekedés Dániában
- Jogosultságeszkalációs hibát javítottak az Androidban



Heti IT biztonsági tipp

- Google keresés – itt is érdemes odafigyelni, hogy mire kattintunk



STATISZTIKAI ADATOK

- Incidensek eloszlása típus és kockázati besorolás szerint
- Események eloszlása csapdatípusok alapján
- Támadott port szerinti eloszlás



CTI ELEMZÉS

Tudnivalók a biztonságos online vásárláshoz – I. rész

További érdekességekért és IT biztonsággal kapcsolatos tartalmakért látogasson el közösségi oldalainkra!



[Nemzeti Kibervédelmi Intézet](#)



[@nki.gov.hu](#)

További érdekességekért, látogasson el [weboldalunkra!](#)



NEWS

IT biztonsági
HÍREK

IT biztonsági
TIPP

Az angolszász KKV-k aggódnak, hogy az infláció miatt kevesebb jut majd a biztonságra
([infosecurity-magazine.com](https://www.infosecurity-magazine.com))

A kis-és középvállalkozások (KKV) 57%-a elképzelhetőnek tartja, hogy csökkentik a kiberbiztonsági költségvetésüket, derült ki az OpenText Security Solution 2022 [Global SMB Ransomware Survey](#) című jelentéséből. **Bővebben...**

SpookySSL sérülékenység: elérhetővé vált az OpenSSL hibajavítás
([darkreading.com](https://www.darkreading.com))

Az OpenSSL projekt október végén [tájékoztatót adott ki](#), amiben a kriptográfiai könyvtár kritikus sebezhetőségeit hozta nyilvánosságra, ígéretet téve, hogy november elsején a hibajavítást is közzéteszik. A javítás elérhetővé vált, javasolt az érintett szoftverek frissítése. **Bővebben...**

Minden Internetre csatlakoztatott eszközt átvizsgálják az Egyesült Királyságban
([bleepingcomputer.com](https://www.bleepingcomputer.com))

A Nemzeti Kiberbiztonsági Központ (NCSC) az Egyesült Királyságban lévő összes Internetre csatlakoztatott rendszert átvizsgálja sérülékenységek szempontjából. A vizsgálat célja, hogy felmérjék az ország támadásokkal szembeni sebezhetőségét, illetve hogy segítsék a rendszertulajdonosokat a kockázatok felmérésében. **Bővebben...**

Kibertámadás miatt akadozott a vasúti közlekedés Dániában
([securityweek.com](https://www.securityweek.com))

Október utolsó hétvégéjén egy kibertámadás miatt fennakadás volt tapasztalható a dán vonatközlekedésben. **Bővebben...**



Jogosultságeszkalációs hibát javítottak az Androidban
([securityweek.com](https://www.securityweek.com))

Több mint 40 sérülékenységet javít az Android 2022. novemberi frissítése, a sebezhetőségek az Android 10 vagy annál újabb verziókat érinti, sőt egy hiba kivételével az Android 13-as verzióra is kiterjed a hatásuk. A frissítés első része (2022-11-01) 17 sérülékenység javítását tartalmazza, amelyek közül 12 jogosultságkiterjesztéshez, három szolgáltatásmegtagadáshoz (DoS) és kettő az információk nyilvánosságra hozatalához vezethet. **Bővebben...**

IT biztonsági
tipp



Az NBSZ NKI [weboldalán](#) egy egyre gyakoribb adathalász technikáról olvashat, és azt is megtudhatja, miként tudja elkerülni, hogy áldozattá váljon.

További hírekért, látogasson el [weboldalunkra!](#)

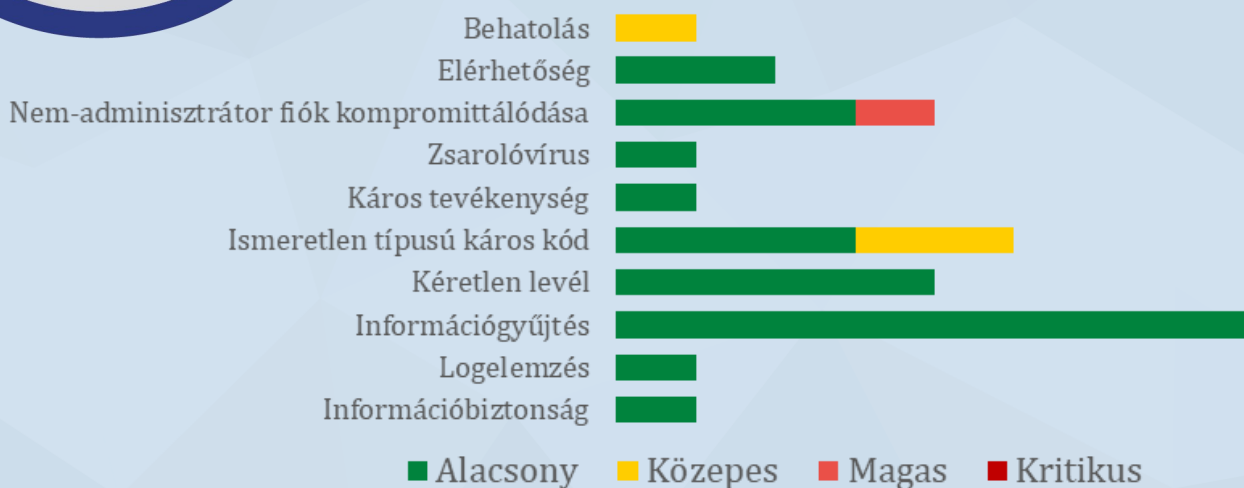


Statisztikai adatok

2022.11.04.-2022.11.10.

Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:

Fenyegetettségi szint: magas

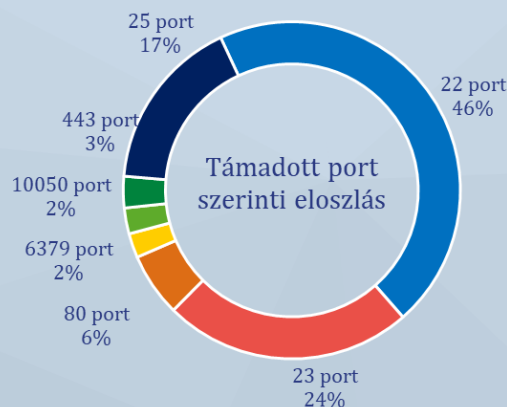


Incidensek eloszlása típus és kockázati besorolás szerint

Az elosztott kormányzati IT-biztonsági csapdarendszerből (Gov1probe) származó adatok:



Események eloszlása csapdatípusok alapján



Aktuális tartalmak



Tudnivalók a biztonságos online vásárláshoz

I. rész

Az e-kereskedelem röviden az online lebonyolított üzleti tranzakciókat jelenti. Legnépszerűbb formája az **online kereskedelem**, és olyan típusú tevékenységeket is magába foglal, mint például az online jegyértékesítés és aukciók. Lényege, hogy teljes mértékben megegyezik „offline” párjával annyi eltéréssel, hogy valamilyen elektronikus hálózaton, elsősorban **interneten keresztül zajlik**.

Jelen dokumentumban a B2C (Business-to-Customer) és C2C (Customer-to-Customer) biztonsági kockázatait taglaljuk és olyan praktikákat mutatunk be, amelyekkel az e-kereskedelem biztonságosan használható bármely felhasználó számára. A másik két értékesítési csatorna részleteit egy másik, ennek a sorozatnak a következő részének szánt tájékoztatóban részletezzük.

[Elovasom](#)

**További érdekességekért és IT
biztonsággal kapcsolatos
tartalmakért látogasson el
közösségi oldalainkra!**



[Nemzeti Kibervédelmi Intézet](#)



[@nki.gov.hu](#)

További érdekességekért, látogasson el **Facebook oldalunkra!**

