



HÍRLEVÉL

Nemzetközi
IT-biztonsági sajtószemle
2023. 40. hét

ELINDULT AZ EURÓPAI KIBERHÓNAP KAMPÁNY!



HÍREK

- Kritikus sérülékeny az Exim MTA-ban
- A NIST kiadta a 800-82r3-as verziójú OT biztonsági útmutatót
- Brutális ransomware támadás ért egy multinacionális vállalatcsoportot
- Cloudflare-rel a Cloudflare DDoS védelme ellen
- Ügyes social engineering trükköt vetettek be észak-koreai hackerek



STATISZTIKAI ADATOK

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



Új CTI Jelentés

A Google térkép működése,
hasznos tudnivalók



KONTAKT

edt@nki.gov.hu

PGP kulcs

FBC3 88A2 E465 BF51
AD58 A2D0 E9DD E078
ABD3 E75D



Európai Kiberbiztonsági Hónap (ECSM)



KiberPajzs
Védelem a pénzügyekben

CyberSec2023

NBSZ NKI szakmai konferencia

Az idei rendezvény középpontjában a kritikus ágazatok kiberbiztonsági erősítése állt.

A résztvevők többek között képet kaptak a **NIS2** implementációjának alakulásáról, az orosz-ukrán kiberhelyzetről, a **KiberPajzs** együttműködés aktualitásairól, az NBSZ NKI saját rendezésű kiberversenyéről (**HCSC**), valamint a Nemzetbiztonsági Szakszolgálat Infokommunikációs és **Információtechnológiai Nemzeti Laboratórium kutatási projekteiről**.

Az előadások anyagai pdf formátumban [letölthetők](#) az esemény oldaláról.

KiberKedd Tipp

Az elmúlt hetekben hírportálok is cikkeztek arról, miszerint a csalók milliók összeggel károsították meg az áldozatukat azzal, hogy a nevében kölcsönt vettek fel. A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézetéhez is érkezett ilyen témájú bejelentés.

A csalás „különlegessége” abban rejlik, hogy a csalók nem csak a netbankos fiókadatokat, és az áldozat összes megtakarítását szerezték meg, hanem a nevében még egy személyi hitelt is felvettek, amelyet a bejelentő szerint a bank az áldozattal fizettetne ki.

[Eloivasom](#)

Az ECSM események:



További érdekességekért, látogasson el [Facebook oldalunkra!](#)



NEWS

IT biztonsági HÍREK

Kritikus sérülékeny az Exim MTA-ban

([bleepingcomputer.com](#))

Egy kritikus nulladik napi sebezhetőség érinti az Exim Mail Transfer Agent (MTA) szoftver minden verzióját, ami támadók számára hitelesítés nélkül távoli kód futtatást (RCE) tesz lehetővé a nyílt Internetről elérhető sérülékeny szervereken. **Bővebben...**

A NIST kiadta a 800-82r3-as verziójú OT biztonsági útmutatót

([securityweek.com](#))

Az Ivanti MDM termékének (EPMM) egy kritikus sebezhetőségét (CVE-2023-35078) fenyegetési szereplők kihasználták norvég államigazgatási szervek elleni támadások során. A tech cég néhány napja egy újabb sebezhetőségről (CVE-2023-35081) közölt információkat. **Bővebben...**

Brutális ransomware támadás ért egy multinacionális vállalatcsoportot

([bleepingcomputer.com](#))

Izrael legnagyobb olajfinomító üzemeltetőjének, a BAZAN Groupnak a honlapja a világ legtöbb pontjáról elérhetetlen, mivel a fenyegetési aktorok azt állítják, hogy feltörték a csoport rendszereit. **Bővebben...**

Cloudflare-rel a Cloudflare DDoS védelme ellen

([bleepingcomputer.com](#))

Veszélyes új malware technikára hívja fel a figyelmet a Trend Micro. Az új, CherryBlos nevű Android malware ún. optikai karakterfelismerő (Optical Character Recognition – OCR) technikát használ a képeken tárolt érzékeny adatok megszerzésére. **Bővebben...**

Ügyes social engineering trükköt vetettek be észak-koreai hackerek

([bleepingcomputer.com](#))

Az észak-koreai „Lazarus” hacker csoport egy spanyol repülőgép ipari vállalat alkalmazottait célozta meg hamis munkalehetőségekkel, hogy egy korábban ismeretlen „LightlessCan” backdoor segítségével feltörjék a vállalati hálózatot. Az ESET által rekonstruált „Operation Dreamjob” támadás a Lazarus tagjának LinkedIn üzenetével indult, aki a Meta (Facebook) Steve Dawson nevű toborzójának adta ki magát. Az „állásinterjú” későbbi szakaszaiban a Lazarus hackereinek egy trükkel sikerült megtéveszteniük az áldozatot, amikor arra kérték, hogy bizonyítson C++ programozási tudásáról néhány kvíz kitöltésével, amelyeket ISO fájlként osztottak meg. **Bővebben...**



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

Aktuális tartalmak



A Google térkép működése, hasznos tudnivalók

A Google Térkép (Google Maps) a legismertebb navigációs alkalmazás. Rengetegen használjuk a mindennapok során – az androidos telefonokon ezt előre telepítve kapjuk – ezért az Intézet szakértőiként úgy gondoltuk, érdemes megosztani néhány gondolatot a Google térkép általános tudnivalóiról, működéséről egyszerű, közérthető formában.

Természetesen a kiberbiztonsági aspektust is szem előtt tartottuk, így a helymeghatározás során felbukkanó veszélyekről is szó esik, és a biztonságos használatra is adunk tanácsokat.

Reméljük minél többen hasznosnak talják a kiadványt!

[Elovasom](#)

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



Nemzeti Kibervédelmi Intézet



@nki.gov.hu

További érdekességekért, látogasson el [Facebook oldalunkra!](#)



Statisztikai adatok

2023.09.28.-2023.10.05.

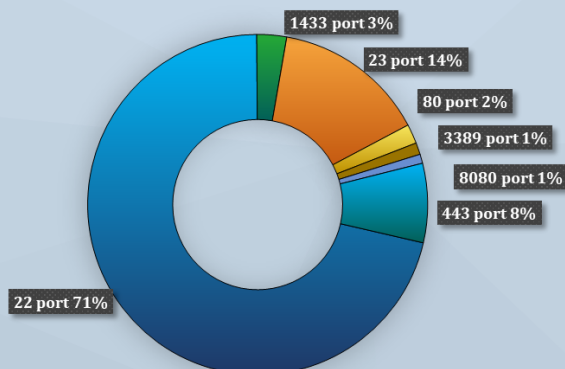
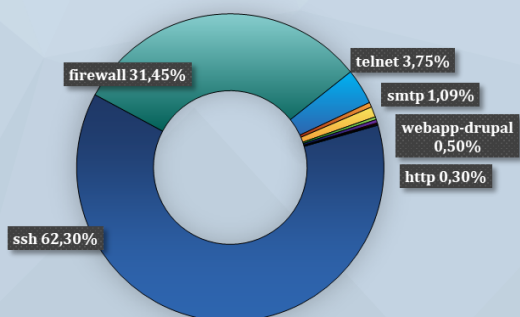
Az NBSZ NKI által kezelt incidensekre vonatkozó statisztikai adatok:



■ Alacsony ■ Közepes ■ Magas ■ Kritikus

Incidensek eloszlása típus és kockázati besorolás szerint

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



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

