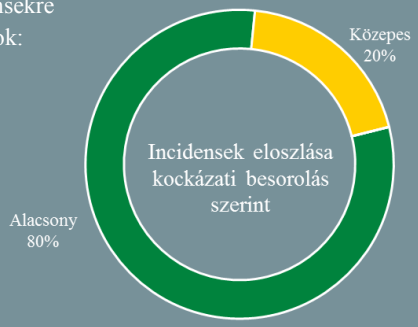
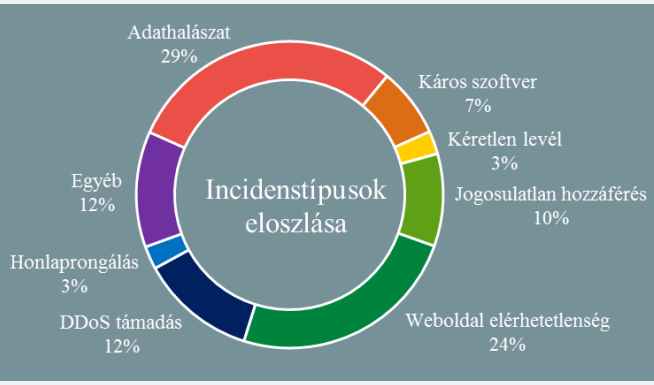
Nemzetközi IT-biztonsági sajtószemle

2021. 07. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.02.12. - 2021.02.18.





Kövessen minket megújult weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

Az ivóvízkészlet-mérgezési incidens tanulságaira figyelmeztet az FBI

(securityaffairs.co)

Az amerikai Szövetségi Nyomozó Iroda figyelmeztetést adott ki a múlt héten nyilvánosságra hozott incidens kapcsán, amelynek során ismeretlenek megpróbálták megmérgezni egy amerikai város ivóvízkészletét. Az eset kivizsgálása során világossá vált, hogy több alapszintű biztonsági jó gyakorlat figyelmen kívül hagyása tette lehetővé a hackerek betörését. Mint kiderült, a támadók a TeamViewer nevű program segítségével fértek hozzá a kritikus létesítmény infrastruktúrájához. Önmagában a program egy legitim, hasznos szoftver, amely lehetőséget ad számítógépes rendszerekhez történő távoli hozzáférésre. **Bővebben...**

Androidos spywarekkel kémkednek a pakisztáni hadsereg után

(bleepingcomputer.com)

Fény derült két olyan androidos kémszoftverre, amelyeket feltételezések szerint indiai állami támogatású hackerek vetettek be az indiai-pakisztáni konfliktus során. A „Hornbill” és a „SunBird” nevű spyware-ek legális és ártalmatlannak tűnő Android alkalmazásokba rejtve üzemeltek a Confucius-ként hivatkozott APT csoport irányítása alatt, amely már 2013 óta ismert pakisztáni és dél-ázsiai célpontok elleni műveleteiről. A káros kódok sokoldalú képességekkel rendelkeznek, többek között fénykép készítésre, jogosultságok változtatására, WhatsApp üzenetek másolására is módot adnak a támadó számára. **Bővebben...**

Mégsem volt annyira titkos a csevegés Telegramon, mint azt a cég állította

(thehackernews.com)

A **Telegram 7.4**-es verziójában javításra került az az adatvédelmi hiba, amely lehetővé tette “titkos csevegések” módban küldött videó- és hangfájlokhoz történő hozzáférést. Fontos tudni, hogy ellentétben a Signallal vagy a WhatsAppal, a félmilliárdos felhasználói bázissal rendelkező Telegram esetében nem alapértelmezett a végponti tikosítás, ezt a felhasználók a “secret chat” mód aktiválásával kapcsolhatják be. **Bővebben...**

„Ghost in the shell” – Egyre jellemzőbb a web shellek káros célú alkalmazása

(bleepingcomputer.com)

„Web shelleknek” nevezzük a különböző szkriptelési nyelveken írt rendszerfelügyeleti szkripteket, programokat, amelyek alapvetően az üzemeltetők munkáját segítik. A Microsoft jelzése szerint azonban az ilyen programok a kiberfenyegetési szereplők részéről történő károkozási célú használata az utóbbi időben egyre gyakoribbá vált ─ csaknem duplázódott tavaly óta. A kibertámadók a web shelleket jellemzően webes alkalmazások sérülékenységeinek kihasználásával, vagy más módon már korábban kompromittált rendszerekre telepítik, rejtett kapcsolatfenntartás vagy káros kódok távoli futtatása érdekében. **Bővebben...**

Egyesült államokbeli Gmail felhasználókat céloz a legtöbb adathalász támadás

(bleepingcomputer.com)

A Google és a Stanford Egyetem közös kutatása szerint a Gmail által blokkolt támadások kereszttüzében leginkább az Egyesült Államok Gmail felhasználói (42%) állnak, őket követik a brit (10%), majd japán (5%) felhasználók. A mintegy 1,2 milliárd káros program és adathalász e-mail anonim módon történő elemzése során kiderült, hogy a támadók elsősorban a gyors és rövid életű kampányokra támaszkodnak: ezek a kampányok átlagosan csupán három napig tartanak, egy-egy sablonnal mintegy 1 000 potenciális áldozatot megcélozva. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán a TikTok Safety Center For Parents súgó oldalán található beállításokról olvashatnak.