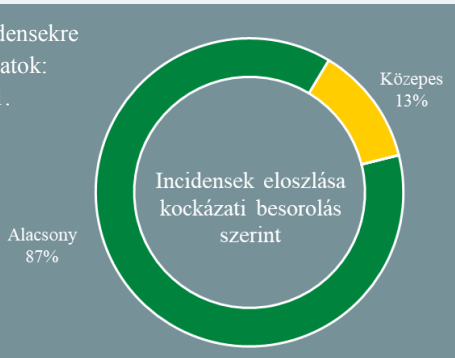
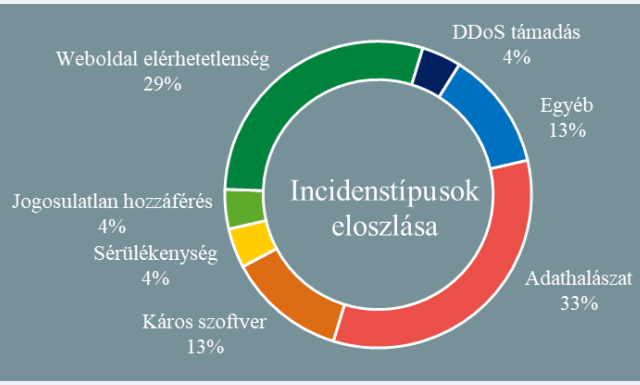
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 13. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.03.26. - 2021.03.31.





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

Zsarolóvírus támadás bénította meg az egyik legnagyobb ausztrál hírcsatornát

(9news.com.au)

Több mint 24 órás szolgáltatáskiesést eredményezett az ausztrál Nine Network televíziós hálózat elleni kibertámadás. Az incidens elsősorban a cég hírszolgáltatói rendszereit érintette, beleértve a vállalat weboldalát is. Bár március 29-én reggelre a csatorna műsorai ismét adásba kerültek, kétséges, hogy a cég mikor tud visszatérni a megszokott, normális működéshez. A támadás kivizsgálása az ausztrál kibebiztonsági központ (Australian Cyber Security Centre – ACSC) segítségével még folyamatban van. Egyelőre annyi ismert, hogy az elkövetők zsarolóvírust használtak, váltságdíjat azonban ez idáig nem kértek a cégtől. **Bővebben...**

Aktívan kihasznált sérülékenységeket javított az Apple

(securityweek.com)

Előző hét pénteken került kiadásra az iOS **14.4.2**-es verziója. A biztonsági frissítés olyan iPhone, iPad és Apple Watch eszközöket érintő súlyos sebezhetőségeket javít, amelyeket a vállalat közlése szerint fenyegetési szereplők aktívan ki is használnak, ezért **telepítése minél előbb javasolt**. Az Apple szokásához híven ennél részletesebb információkat nem közölt, azonban mindezt kapcsolatba lehet hozni a Google Project Zero fenyegetéselemző csapatának egy korábbi közlésével, így feltételezhető, hogy állami támogatású csoportoknak (APT) is közük lehet a támadásokhoz. 2020 januárja óta az Apple már legalább 7 aktívan kihasznált nulladik napi sebezhetőséget foltozott be.

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat arról, hogy miként védhetjük meg QNAP hálózati adattárolónkat (NAS).

Biztonsági rést találtak a netmask npm csomagjában

(securityweek.com)

A netmask npm csomagot érintő nemrég felfedezett biztonsági rés privát hálózatokat tehet elérhetővé, és számos támadási típus kivitelezésére adhat módot. A programcsomagot IPv4 CIDR blokkok elemzésére, illetve összehasonlításukra tervezték. A program nagy népszerűségnek örvend, heti több millióan töltik le, és jelenleg több mint 278 000 projekt esetében használják. A szóban forgó sebezhetőséget (CVE-2021-28918), lényegében a megadott IP címek téves értelmezése eredményezi, a csomag ugyanis helytelenül olvassa a nyolcas számrendszerű kódolást. **Bővebben...**

Brute force támadásokra figyelmeztet a QNAP

(ehackingnews.com)

A tajvani QNAP arra figyelmezteti ügyfeleit, hogy megélénkültek a támadások hálózati adattároló termékei (Network Attached Storage – NAS) ellen. QNAP termékek az elmúlt években már több esetben váltak kampányszerűen fellángoló támadások áldozatává, amelyek során a kiberbűnözők sok esetben vírust (pl.: QSnatch, eCh0raix) telepítettek a megcélzott eszközökre. A mostani figyelmeztetés erről nem közöl információkat, mindössze annyit tudni, hogy a támadók az interneten keresztül elérhető QNAP eszközökre próbálnak illetéktelenül bejelentkezni, azáltal, hogy megpróbálják feltörni az admin fiókok jelszavát. Ezért mindenképp kerüljük a gyenge, könnyen kitalálható jelszavak alkalmazását. *(A QNAP további biztonsági javaslatairól e heti* IT-biztonsági tippünkben olvashat bővebben.)

Ellátási lánc támadás a PHP ellen

(news-web.php.net)

2021. március 28.-án Nikita Popov, a PHP egyik core kontributora a PHP levelezőlistáján bejelentette, hogy ismeretlen támadóknak sikerült az ő és Rasmus Lerdorf fejlesztő nevében két kártékony kódrészletet feltölteni a php-src git.php.net kódtárába. Az esettel kapcsolatos nyomozás erejéig szüneteltetik a közösségi git.php.net repository üzemeltetését, és a GitHub kódtárukba töltik fel a változásokat. **Bővebben..**