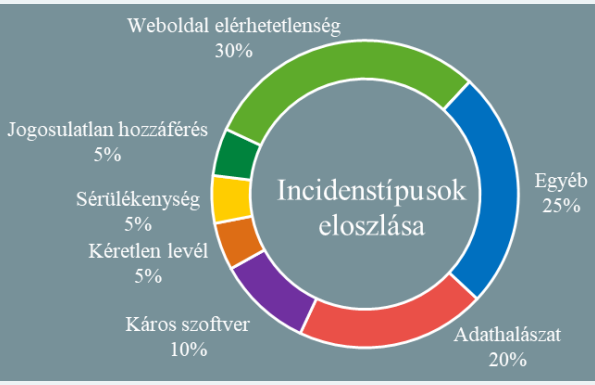
Nemzetközi IT-biztonsági sajtószemle

2021. 28. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.07.09. - 2021.07.15.



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

Törték már fel az Instagram fiókját? Ezeken a lépéseken érdemes végigmenni

(engadget.com)

Néhány biztonsági újítást vezetett be az Instagram, amelynek részeként a korábban feltört fiókoknál elindul egy biztonsági ellenőrzés, ami végigvezeti a felhasználókat a legfontosabb fiókvédelmi lépéseken. Ilyen például a profilinformációk ellenőrzése, a kontakt adatok frissítése, vagy azon fiókok ellenőrzése, amelyek hitelesítő adatokat osztanak meg. Emellett egyes régiókban az is bevezetésre került, hogy a WhatsApp fiókkal rendelkező felhasználóknak lehetőségük van a csevegő appot kétfaktoros hitelesítésre használni SMS vagy más hitelesítő alkalmazás helyett, ami annyit jelent, hogy az Instagram fiókba történő belépéskor WhatsAppban is érkezhet az egyszer használatos jelszó. **Bővebben...**

Safari hibán keresztül csaptak le egyes LinkedIn felhasználókra

(bleepingcomputer.com)

A Google Threat Analysis Group (TAG) és a Google Project Zero kutatói négy, támadók által aktívan kihasznált nulladik napi (zero day) sérülékenységet fedeztek fel a Google Chrome (CVE-2021-21166 és CVE-2021-30551) és Internet Explorer (CVE-2021-33742) böngészőben, valamint a Safari által használt WebKit (CVE-2021-1879) böngészőmotorban. A Google szerint 2021 második feléig már több zero day sebezhetőség került felfedezésre, mint az előző évben összesen, bár hozzáteszik, hogy a sérülékenységek hatékonyabb felderítése és nyilvánosságra hozatala is hozzájárulhat a növekvő trendhez. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat talál a **VirusTotal** használatával kapcsolatban.

Zsarolóvírus tranzakciók nyomon követésére szolgáló nyílt adatbázis indult

(zdnet.com)

A zsarolóvírusok globális problémát jelentenek, amely kapcsán már világvezetők is konzultálnak, azonban a ransomware fenyegetés valós gazdasági hatásáról nincs átfogó képünk. Egy biztonsági kutató ezért úgy döntött, készít egy adatbázist (ransomwhere.re) a zsaroló tranzakciók nyomon követéséhez, amelynek segítségével jobban felbecsülhető a zsarolóvírusok által okozott kár, illetve a védekező intézkedések hatékonysága. A nyilvántartásban gyakorlatilag váltságdíjként fizetett kriptovaluta tranzakciós adatok találhatók ransomware családokhoz rendelve. **Bővebben...**

Független biztonsági auditon esett át a ProtonMail

(protonmail.com/blog)

A svájci központú ProtonMail közleménye szerint lényeges hiba vagy sérülékenység feltárása nélkül zárult az e-mail és naptár szolgáltatásukat vizsgáló biztonsági audit. A legtöbb online szolgáltató az *ismeretlenség biztonsága* (security through obscurity) elv alapján jár el, azaz nem hozzák nyilvánosságra a működésük módját, beleértve az alkalmazott szoftvereket, kódokat, stb. A ProtonMail ezzel szemben az átláthatóságot tartja célravezetőnek, amelynek értelmében minden alkalmazásuk nyílt forrású ─ így IT biztonsági kutatók számára adott a lehetőség biztonsági hibák, problémák feltárására. **Bővebben...**

A LinkedIn szerint nem biztonsági esemény a felhasználói adatok tömeges gyűjtése és eladása

(cybernews.com)

Az elmúlt néhány hónap során immár harmadik alkalommal árulják LinkedIn felhasználók adatait egy hacker fórumon. Hasonlóan a múltkori esethez, a mostani adatok között is felhasználónevek, e-mail címek, szakmai tapasztalatokra vonatkozó információk, további közösségi oldalak elérhetőségei és egyéb, az érintett profilok nyilvánosan elérhető információi szerepelnek, mintegy 600 millió LinkedIn felhasználó kapcsán. **Bővebben...**