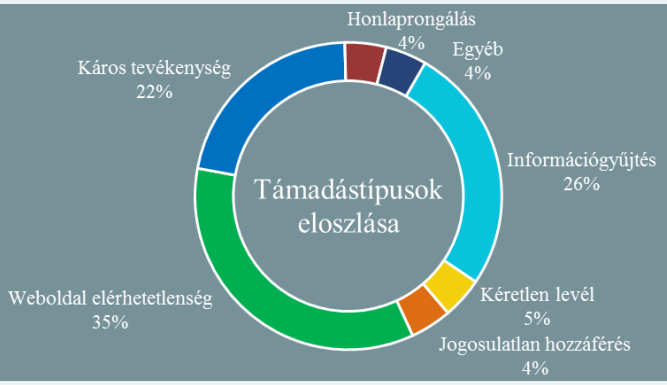
Nemzetközi IT-biztonsági sajtószemle

2020. 34. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.08.14. - 2020.08.18.



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

Több ezer kanadai kormányzati fiókot ért támadás

(securityweek.com)

Kanadai hatóságok szombati bejelentése szerint támadók megpróbáltak hozzáférni több, mint 9 000 online kormányzati ügyintézésre szolgáló **GCKey** fiókhoz. A GCKey kormányzati elektronikus szolgáltatásokhoz nyújt hozzáférést és az ország több, mint 30 kormányzati ügynöksége használja, köztük a kanadai adóhatóság is (Canada Revenue Agency – CRA). Esetükben mintegy 5 500 felhasználói fiók érintett, amelyeket az adófizetők adatai védelmében átmenetileg felfüggesztettek. Az incidens kivizsgálása a szövetségi rendőrség bevonásával megkezdődött. A kanadai állami csatorna CBC szerint augusztus eleje óta több kanadai állampolgár is jelentette, miszerint a fiókjukban szereplő banki információk módosításra kerültek.

EDR funkcióval bővül a Microsoft Defender ATP

(bleepingcomputer.com)

Végpontvédelmi és elhárítási technológiával (EDR – Endpoint Detection and Response) bővül a Microsoft Defender Advanced Threat Protection (ATP) védelmi szolgáltatása, amely viselkedés alapú fenyegetés-elhárítást tesz lehetővé. A gépi tanulás-vezérelt védelmi megoldás valós időben észleli és állítja meg azon fenyegetéseket, amelyeket a vírusvédelmi megoldás nem detektált. A szolgáltatás minden Windows 10 verzión és a Windows Server 2016 vagy ennél újabb szerver verzión elérhető, azonban jelenleg még csak nyilvános tesztelésen. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán arról olvashat, milyen funkciókra érdemes figyelni Google Home használata esetén.

Parancsikonnal indítható inkognitó módot kap a Chrome böngésző

(bleepingcomputer.com)

Egyelőre még csak a Chrome Canary verziójában érhető el az új funkció, ami lehetővé teszi olyan parancsikon létrehozását a Windows asztalon, ami egyből inkognitó módban indítja a böngészőt. A Google Canary alapértelmezetten nem engedélyezi ezt a funkciót, ezért előbb engedélyezni kell a **chrome://flags** alatt az "Inkognitó mód asztali parancsikon" beállítást. **Bővebben...**

Megszünteti a vegyes űrlapok automatikus kitöltését a Chrome

(bleepingcomputer.com)

A Google Chrome böngésző 86-os verziója figyelmezteti fogja a felhasználókat, amennyiben egy olyan webhely űrlapját készülnek kitölteni, ahol a webhely ugyan HTTPS kapcsolattal rendelkezik, azonban az információkat nem titkosított HTTP kapcsolaton keresztül továbbítja. Az ilyen, ún. vegyes űrlapok lehetővé teszik a támadók számára a felhasználóktól érkező adatok olvasását és módosítását, ezért a 86-os verziótól a böngésző tiltani fogja a vegyes űrlapok automatikus kitöltésének lehetőségét. **Bővebben...**

Egy ügyes kill-switch fél évre hatástalanította az EMOTET malware-t

(securityaffairs.co)

Az EMOTET egy veszélyes kártevő család, amelynek újabb és újabb verziói látnak napvilágot, folyamatosan bővítve a meglévő funkciókat. Legutóbb februárban történt egy jelentős fejlesztés, ekkor a Wi-Fi hálózatokon történő továbbterjedéssel egészült ki a malware támadási eszköztára. Azonban ─ akár bármely programozó ─ a kártevő fejlesztők is követnek el hibákat. Egy ilyen hibát fedezett fel a Binary Defense, akik képesek voltak egy ún. kill-switchet készíteni, ami megakadályozta a malware futását, pusztán egy registry kulcs értékének kinullázásával. **Bővebben...**