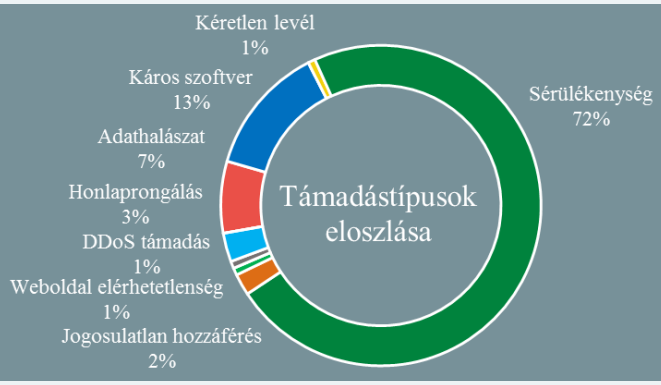
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 10. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.02.28. - 2020.03.05.



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

Koronavírussal kapcsolatos kulcsszavakat cenzúráz a WeChat

(theverge.com)

Népszerű online kínai platformok ─ mint az ország első számú üzenetküldő alkalmazása, a WeChat, valamint a szintén nagy népszerűségnek örvendő YY streaming oldal ─ már január eleje óta cenzúrázzák a koronavírus járvánnyal összefüggő kulcsszavakat. Minderre a kanadai Citizen Lab kutatócsoport derített fényt, akik több, kanadai és kínai fiókok között váltott tesztüzenet alapján azt találták, hogy egyre több ─ januárban 132, egy hónappal később már 516 ─ kulcsszó eltávolításra került a csoportos beszélgetésekből. **Bővebben...**

Egyre több a mobilfizetéseket érintő csalás

(securityweek.com)

Továbbra is a Windows a csalók által legtöbbet kompromittált operációs rendszer, azonban az iOS és az Android együttes adatai már az online csalási tevékenység 51%-át teszik ki ─ derült ki az online biztonsággal foglalkozó Sift vállalat által készített elemzésből. A csalók legnépszerűbb célpontja továbbra is a fizikai e-kereskedelem, ám a digitális e-kereskedelem incidensei is egyre növekvő tendenciát mutatnak. Az infokommunikációs technológiák fejlődésével az évek során a fizetési lehetőségek is bővültek, ennek eredményeként az online promóciók, a digitális pénztárcák és az átutalások is új alternatívákat jelentenek a csalók számára. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat az okos kamerák biztonságos használatával kapcsolatban.

3 millió Let's Encrypt tanúsítvány kerül visszavonásra

(threatpost.com)

A nagy népszerűségnek örvendő, ingyenes webes biztonsági tanúsítványt nyújtó Let's Encrypt szerdán bejelentette, hogy egy szoftverhiba miatt vissza kell vonnia több, mint 3 millió TLS tanúsítványt. A probléma a Boulder nevű szoftverüket érinti, amelynek feladata a domain tulajdonosának ellenőrzése a tanúsítványok kiállítása előtt. A hiba komoly biztonsági kockázatot jelent, ennek kihasználásával ugyanis a támadók hozzáférhetnek a titkosított webes forgalomhoz. A tanúsítványok visszavonása után ─ új tanúsítvány igényléséig ─ az érintett oldalak nem biztonságosként kerülnek megjelölésre a böngészőkben, illetve a weboldalak megjelenésével is problémák adódhatnak. **Bővebben...**

Az Apple szigorít a TLS tanúsítványok érvényességével kapcsolatban

(heise.de)

A „felhasználók webes biztonságát javító" törekvései részeként az Apple rövidebb érvényességi időtartamot határozott meg a TLS szerver tanúsítványokra vonatkozóan; a vállalat bejelentése szerint a 2020. szeptember 1-je után kiállított SSL/TLS tanúsítványok közül csak azokat fogja elfogadni, amelyek érvényességi ideje legfeljebb 398 nap. Az új normáknak nem megfelelő kiszolgálókkal a kapcsolat a jövőben meghiúsulhat, ami hálózat- és alkalmazáshibákhoz vezethet, és megakadályozhatja a webhelyek betöltését az Apple által gyártott eszközökön. **Bővebben...**

10 000 brit utas adatát szivárogtatta ki egy ingyenes Wi-Fi szolgáltató

(bleepingcomputer.com)

Közel 10 000 személy érzékeny adatai ─ például e-mail címek, születési évszámok és egyéb utazási információk ─ váltak szabadon hozzáférhetővé az egyes brit vasútállomásokon ingyenes Wi-Fit szolgáltató C3UK hibájából. Az incidenst a cég alacsony kockázati besorolásúnak ítélte, azzal indokolva, hogy kritikus információk, mint például jelszavak, vagy pénzügyi adatok nem váltak elérhetővé, valamint konkrét hozzáférés sem történt harmadik fél részéről. **Bővebben...**