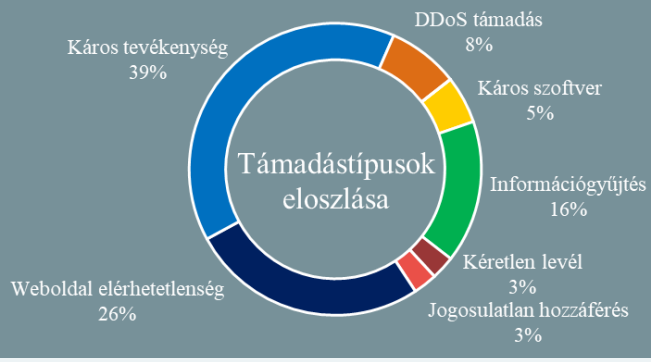
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 47. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.11.13. - 2020.11.20.



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

A Black Friday közeledtével egyre nő az adathalász támadások száma

(itpro.co.uk)

A Check Point Software jelentése arról számol be, hogy az elmúlt hetekben több mint 13 szorosára nőtt az adathalász támadások száma. A biztonsági kutatók szerint az online csalási kísérletek elszaporodásához a járványügyi helyzet miatti szigorítások is hozzájárulnak, a fizikai vásárlás korlátok közé szorulásával. November első két hetében 80%-kal több értékesítéssel összefüggő adathalász kampányt azonosítottak, amelyek olyan kifejezéseket tartalmaztak, mint az *„ajánlat”*, *„eladás”*, *„olcsó”* és *„% kedvezmény”*. **Bővebben...**

GDPR szabályokat sérthet az Apple nyomon követési gyakorlata

(securityweek.com)

Az Apple szoftverek által végzett nyomkövetés törvényességének kivizsgálását kérte a bécsi székhelyű NOYB („none of your business”) adatvédelmi csoport német és spanyol adatvédelmi hatóságoktól. Az iOS készülékek – webes sütikhez hasonló – egyedi hirdetési azonosítói (IDFA) alkalmasak arra, hogy az Apple, illetve harmadik felek nyomon kövessék az eszköz használójának online és mobil applikációkon végzett tevékenységét. A NOYB indoklása szerint ez a gyakorlat sérti Európai Unió elektronikus adatvédelmi elveit, mivel a cég nem kér kifejezett hozzájárulást az érintettektől. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a Firefox webböngésző új verziójával érkező “Csak HTTPS mód” funkciójáról.

Nyilvános konzultációt kezdeményez a Mozilla a DoH bevezetése előtt

(.zdnet.com)

A Mozilla szeretné elérhetővé tenni a DNS-over-HTTPS (DoH) szolgáltatást a Firefoxban, azonban előtte kikéri a tech cégek, kormányzatok és internetszolgáltatók véleményét konzultációt indítva a témában. A szokatlan lépést kritikák hada előzte meg kormánytisztviselők, bűnüldöző hatóságok és internetszolgáltatók részéről, arra hivatkozva, hogy a funkció a bűnözőknek kedvez ─ egyesek még az “Internet Gonosztevője” címre is jelölték a böngészőgyártót. A legnagyobb ellenkezés brit hatóságok részéről merült fel, amelynek hatására a Mozilla visszakozott és elhalasztotta a DoH bevezetését az Egyesült Királyság területén. **Bővebben...**

WordPress oldalak veszélyben

(bleepingcomputer.com)

A Wordfence jelzése szerint hackerek olyan WordPress oldalak után kutatnak, amelyeken sérülékeny Epsilon Framework sablonok vannak használatban. A sérülékenységek ún. funkció befecskendezéses támadásokat tehetnek lehetővé, ami a támadott oldal teljes kompromittálódásához vezethet. A Wordfence szerint a támadók a sérülékenységek kihasználhatóságát próbálgatják, az érintett WordPress oldalak adminjai számára javasolt a biztonsági javítások mielőbbi telepítése. **Bővebben...**

Új biztonsági funkció jelent meg a Zoomhoz

(zdnet.com)

A “Zoombombing” megelőzését segíti elő a Zoom új biztonsági funkciója az “At-Risk Meeting Notifier”. A szolgáltatás lényege, hogy folyamatosan szkenneli a közösségi oldalak publikus posztjait Zoom meeting linkek után kutatva, és amennyiben talál ilyet, automatikusan e-mailt küld a meeting gazdájának, figyelmeztetve arra, hogy a videokonferenciát idegenek is megtalálhatják. Egy Zoom meetinghez történő illetéktelen becsatlakozást és a meeting szándékos megzavarását nevezik Zoombombingnak. Ez legtöbbször úgy fordul elő, hogy egy videokonferencia szervezője ─ vagy épp az egyik résztvevő ─ valamelyik közösségi oldalon közzéteszi a meeting elérésére szolgáló hivatkozást, sőt esetenként még a csatlakozáshoz szükséges jelszót is.