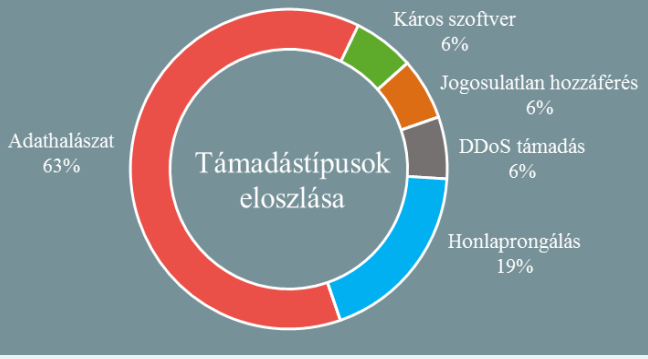
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.06.21. - 2019.06.27.



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

A Protonmail szerint a Gmail-féle „bizalmas mód” csupán marketingfogás

(protonmail.com)

A Protonmail blog posztban fejti ki álláspontját a Gmail által bevezetett „bizalmas móddal” szemben. Ebben arra hívják fel a figyelmet, hogy a saját szolgáltatásuk esetében alkalmazott végponti titkosítással, és a zero-access encryptionnel szemben a Google levelező szolgáltatásának nevezett funkciója nem garantál sem biztonságot, sem adatvédelmet. A szóban forgó szolgáltatás alapvetően két dolgot tesz lehetővé: meghatározható egy érvényességi idő az üzenethez (ennek elteltét követően a címzett már nem tudja elolvasni a levelet), a második opció pedig egy jelszó megadását teszi lehetővé, amit a Google generál és küld ki a címzettnek SMS-ben. Mindezek mellett a bizalmas leveleket nem lehet sem forwaldolni, sem másolni, sem pedig letölteni, vagy nyomtatni. **Bővebben...**

Nyíltan elérhetők az amerikai határőrségtől kiszivárgott anyagok

(grahamcluley.com)

Jelentős adatszivárgás történt egy, az amerikai határőrség (United States Customs and Border Protection – CBP) részére felügyeleti szolgáltatást nyújtó vállalatnál (Perceptics), amelynek során 400 GB-nyi bizalmas adatot tulajdonítottak el, köztük kézikönyvekkel, PowerPoint prezentációkkal, költségvetésekkel, eszközlistákkal, jelszavakkal, valamint a határátlépőkről készült képanyagokkal. A Perceptics az eset kapcsán többszörösen vétkes, hiszen mint kiderült a CBP rendszeréből a hatóság tudtán kívül másolta át az adatokat saját rendszerére. A kiszivárogtatott információkat a hackerek először torrent hálózaton osztották meg, jelenleg pedig már a Distributed Denial of Secrets (DDOS) weboldalon is elérhetőek. **Bővebben...**

Távközlési cégek elleni kiberkémkedéssel vádolják Kínát

(cyberscoop.com)

A Cybereason kiberbiztonsági cég egy telekommunikációs vállalatok ellen zajló globális támadási kampányt fedezett fel, amelynek során már több száz gigabájtnyi adatot szereztek meg. Az azonosított hacking eszközök alapján a szakértők nagy bizonyossággal állami támogatású kínai hackereket sejtenek a háttérben, azonban fenntartják a tévedés vagy a szándékos félrevezetés lehetőségét is. A legalább 2017 óta zajló kampány körülbelül 10 afrikai, európai, közel-keleti és ázsiai mobil szolgáltatót érint, azonban a konkrét cégeket nem nevezték meg. A Cybereason vezető kutatója szerint a támadások célzottak voltak és minden valószínűség szerint kiberkémkedési célból hajtották végre őket. **Bővebben...**

Az orosz bankok nem felelnek meg a kiberbiztonsági követelményeknek

(ehackingnews.com)

Oroszország központi bankja, mint szabályzó szerv, jogosult a pénzintézetek kiberbiztonsági követelményeinek történő megfelelés vizsgálatára. A tavalyi évben 58 hitelesített bankot ellenőriztek, míg idén már 75 pénzintézet került átvizsgálásra, amelyek közül az összes intézménynél megállapítottak problémákat és hiányosságokat. A központi bank vezetője, Elvira Nabiullina a Moszkvában megrendezésre került II. International Cybersecurity Congress (ICC) rendezvényen hozta nyilvánosságra az eredményeket, amelyek kapcsán hozzátette, hogy bár jelenleg nem kritikus hibákról van szó, a megelőzésre irányuló intézkedések elmaradása esetén azok könnyen kritikussá válhatnak. **Bővebben...**

Ön tudja mivel van elfoglalva az iPhone-ja éjszaka?

(washingtonpost.com)

Az Apple nemrég az „Ami az iPhone-ján történik, az az iPhonján is marad” jelmondattal indított kampányt, úgy tűnik némiképp félrevezető módon. Kiderült ugyanis, hogy egy alapértelmezett engedély (Alkalmazásfrissítés a háttérben), birtokában az ún. alkalmazáskövetőknek lehetőségük van felhasználói adatokat és eszközinformációkat továbbítani harmadik feleknek. Egy ezzel kapcsolatban végzett vizsgálat során mintegy 5 400 olyan rejtett alkalmazást fedeztek fel, amelyek ilyen adatokat továbbítottak különböző cégeknek. Mindez jellemzően az éjszaka közepén történik, mivel az alkalmazások készítői igyekeznek a tevékenységet észrevétlenül végezni. **Bővebben...**

IT biztonsági Tanács

A következő beállításokkal korlátozhatja iPhone-ján az alkalmazáskövető funkciókat.

- A „Beállítások” > „Adatvédelem” menüpontban kapcsolja ki a helymeghatározást, azoknál az alkalmazásoknál, amelyeknek nincs szüksége helyadatokra.
- Szintén az „Adatvédelem” menüpontban a „Hirdetések”-en belül kapcsoljuk be a „Kevesebb hirdetéskövetés” opciót.
- A „Beállítások” > „Általános” menüpont alatt korlátozzuk az „Alkalmazásfrissítés a háttérben” funkciót.
- Hagyatkozzunk az Apple saját fejlesztésű alkalmazásaira, ugyanis adatvédelmi szabályoknak való megfelelés érdekében a legtöbb esetben titkosítja az adatokat és csökkenti az adatgyűjtés lehetőségét.

Zsarolóvírus támadások zajlanak IT outsourcing cégek ellen

(zdnet.com)

Hackerek Sodinokibi zsarolóvírussal támadtak meg legalább három, menedzselt IT szolgáltatásokat (Managed Service Provider – MSP) nyújtó vállalatot. Az incidenskivizsgálásban néhány cégnek segítséget nyújtó Huntress Lab szerint a támadók RDP (Remote Desktop Endpoints) végpontokon fértek hozzá a rendszerekhez, majd képesek voltak emelt jogosultságot szerezni és hatástalanítani a vírusvédelmi megoldásokat. A támadás következő fázisában a hackerek Webroot SecureAnywhere fiókok után kutattak, amely szoftvert MSP-k az ügyfelek rendszereinek távoli kezelésére használják. Ahol sikerült ehhez is hozzáférést szerezniük, egy Powershell szkript segítségével indították útjának a zsarolóvírust. Egyes Reddit felhasználók szerint olyan támadás is történt, ahol a Webroothoz hasonló célú Kaseya VSA-t is használták, ám hivatalos megerősítés ezzel kapcsolatban nem történt. **Bővebben...**

PoC jelent meg az androidos MS Outlook sérülékenységéhez

(thehackernews.com)

A Microsoft korábban biztonsági javítást adott ki az Outlook androidos verziójához egy távoli kódfuttatásra módot adó sérülékenység miatt (CVE-2019-1105), amely több, mint 100 millió ügyfelet érinthet. A biztonsági hibáról készített leírásban ugyanakkor nem szerepelt bővebb információ, pusztán annyi, hogy egy cross-site scripting (XSS) típusú hibáról van szó, amely a támadóknak lehetőséget ad káros kód futtatására, amelyhez csupán egy speciálisan szerkesztett e-mailt kell küldeniük az áldozatnak. A hibát elsőként felfedező Bryan Appleby azonban most újabb információkat és egy bizonyítást (proof-of-concept – PoC) is megosztott a nyilvánossággal. Habár aktív kihasználásról eleddig nem érkeztek hírek, a felhasználóknak mindenképp javasolt telepíteni a frissítést.

Rendkívüli ütemben fertőz egy IoT eszközöket támadó káros kód

(zdnet.com)

A Silex névre keresztelt malware mindössze 3-4 óra alatt több, mint 2 000 IoT (Internet-of-things) eszközt támadott meg. A támadások jelenleg is zajlanak, amelyek során a malware ismert hitelesítő adatok segítségével igyekszik hozzáférést szerezni a célkeresztben álló eszközökhöz. A káros kód egy ún. wiper, ami törli a berendezések háttértárát, a tűzfal szabályokat, hálózati beállításokat, majd végül le is állítja az eszközt. Egy sikeres támadás utáni helyreállításhoz az áldozatnak manuálisan újra kell telepítenie a firmware-t, amely ugyanakkor a legtöbb felhasználó számára túl komplikált feladat. **Bővebben...**

Venmo mobilfizetési tranzakciós adatokat hoztak nyilvánosságra a Githubon

(heise.de)

Dan Salmon informatikai hallgató egy több, mint 7 millió rekordból álló adatbázist tett közzé a Githubon a Venmo mobil fizetési platformon zajló tranzakciókból. Érdekesség, hogy a rekordok nem egy adatszivárgásból erednek, hanem a cég által működtetett „hírcsatornából”, amelyen összefoglalják az ügyfelek tranzakcióit, de egy API lekérdezéssel is hozzáférhetőek lehetnek. A Venmo alkalmazásának alapértelmezett beállításai ugyanis lehetőséget biztosítanak a cég számára, hogy tömegesen gyűjtse az ügyfelek tranzakciós adatait. **Bővebben...**