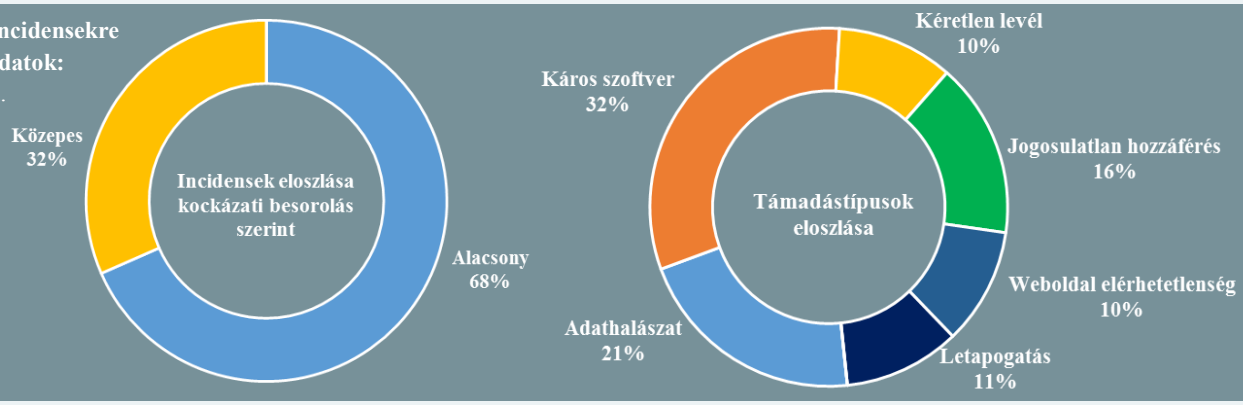
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.09.07. - 2018.09.13.



Kövessen minket online az itbiztonsag.govcert.hu oldalunkon, ahol naponta

Nem közvetlenül az erőműveket célzó támadások is komoly üzemzavart okozhatnak

(www.usenix.org)

A Princetoni Egyetem kutatói tanulmányukban egy elektromos erőművek ellen alkalmazható új támadási módszerről számolnak be, miszerint egy nagy elektromos teljesítményű okos eszközökből ─ például légkondicionálókból, vagy fűtőberendezésekből ─ álló „zombihálózat" (botnet) lehetőséget biztosít a villamosenergia-rendszer elleni nagyszabású, koordinált támadások végrehajtására. A „Manipulation of demand via IoT" (MadIoT) névre keresztelt módszer lényege, hogy a kompromittált eszközök szinkronizált ki és bekapcsolásával az áramfelvételt manipulálja a támadó, az áramfelvételi igény hirtelen növelése és csökkentése ugyanis komoly frekvencia instabilitást okozhat az elektromos hálózaton, ami a generátorok túlterheléséhez, egy küszöbérték fölött pedig azok leállásához vezet. **Bővebben...**

A vallási szektor csak jelentős késéssel eszmélt rá a kiberfenyegetésre

(www.cyberscoop.com)

A közelmúltban az amerikai vallási felekezetek létrehoztak egy információmegosztó- és elemző szervezetet (FB-ISAO) az adományozók adatainak és a vallási témájú weboldalak védelmének biztosításához. A vallási gyülekezetek tagjai potenciálisan kitettek a hacker támadásoknak, ugyanis a vallási szervezetek annak ellenére, hogy nagy mennyiségű információt gyűjtenek tagjaikról, a megfelelő kockázatkezelési döntések meghozásához még az olyan alapvető fontosságú képességekkel sem rendelkeznek, mint például az információmegosztás, vagy a megfelelő helyzeti tudatosság ─ nyilatkozta William Flynn, az FB-ISAO egy bizottsági tagja. A még júniusban alapított, de csak most nyilvánosságra hozott szervezet a technológiai gyártók együttműködésével fenyegetettség elemzéseket kínál, hogy a vallási szektor is rugalmasan tudja kezelni a számítógépes támadásokat. **Bővebben...**

Letartóztatták a ProtonMail ellen irányult DDoS támadás elkövetőjét

(www.gbhackers.com)

Az Egyesült Királyság Nemzeti Bűnüldözési Ügynöksége London határain kívül letartóztatta a ProtonMail e-mail szolgáltató ellen az utóbbi időben indított DDoS támadások egyik elkövetőjét. Öt különböző hackercsoport vezette a ProtonMail elleni támadásokat, köztük a „Apophis Squad" néven ismert orosz hackercsoport, amelynek a 19 éves George Duke-Cohan is a tagja volt. Cohan számos internetes bűncselekményt hajtott már végre, beleértve több túlterheléses támadást is. A ProtonMail még az első támadásokat észlelve megkezdte a vizsgálatokat, így az is kiderült, hogy az „Apophis Squad" csoport néhány tagja szintén felhasználója a ProtonMail-nek. A hétfői tárgyaláson arra is fény derült, hogy szintén George Duke-Cohan a felelős a csőbombával fenyegető hamis e-mailekért, amiket több száz iskola és az United Airlines légitársaság kapott az elmúlt hónapban. **Bővebben...**

Egyre több a felhasználói adatokat megosztó iOS alkalmazás

(www.securityaffairs.co)

A GuardianApp mobil tűzfal alkalmazás biztonsági kutatói kimutatták, hogy egyre több iOS alkalmazás gyűjt és értékesít felhasználói adatokat ─ például Wi-Fi hálózati azonosítókat, helyadatokat, akkumulátor töltöttségi állapotot ─ reklám és marketing cégeknek. Bár az alkalmazások tájékoztatják a felhasználókat az adatgyűjtés tényéről, arról azonban már nem tesznek említést, hogy a begyűjtött adatokat hirdetési- és marketingtevékenységet végző cégekkel is megosztják. A vizsgálat során felfedezték, hogy az említett alkalmazások olyan harmadik felek által beágyazott nyomkövető kódokat tartalmaznak, amelyek akár folyamatosan futhatnak az eszközökön, így mindvégig képesek az iPhone felhasználók adatainak gyűjtésére és továbbítására. **Bővebben...**

Hamarosan megérkeznek az Apple új biztonsági funkciói

(www.techcrunch.com)

A nemsokára megjelenő iOS 12 és a macOS Mojave a már júniusban kiszivárgott hírek szerint nagy hangsúlyt fektet majd a biztonságra és a magánélet védelmére. A 6. generációs macOS újításai között említhető, hogy a Safari böngésző „intelligens nyomkövetés elleni védelme" megakadályozza majd, hogy a reklámozó cégek információt szerezzenek a felhasználók által meglátogatott oldalakról, megnehezítve ezáltal a célzott reklámokhoz történő profilalkotást, valamint ezután engedélyhez kötött lesz, hogy egy applikáció hozzáférhet-e többek között a FaceTime kamerához és mikrofonhoz, a helyadatokhoz, vagy a backuphoz. Az iOS 12-vel a beépített jelszókezelő automatikusan figyelmeztetni fogja a felhasználókat, amennyiben olyan jelszót kívánnak használni, amit már más weboldalon, vagy alkalmazásban használnak, valamint a kétfaktoros azonosítás során SMS-ben, vagy push üzenetben érkező kódok automatikusan betöltésre kerülnek majd. **Bővebben...**

IT biztonsági Tanács

A héten kiemelt figyelmet kaptak az Apple platformján felbukkanó adatvadász alkalmazások, amelyek engedély nélkül gyűjtenek és értékesítenek felhasználói adatokat.

iOS rendszeren a „Beállítások" → „Adatvédelem" menüpontban érdemes bekapcsolni a „Kevesebb hirdetéskövetés" funkciót, valamint javasolt elutasítani az olyan helyadatokhoz való hozzáférési kéréseket, amelyek adatvédelmi irányelvekre történő hivatkozást tartalmaznak.

Figyelemmel kísérhető a Microsoft hibajavító folyamata

(www.zdnet.com)

Elérhető a Microsoft Security Response Center (MSRC) által publikált weboldal és pdf dokumentum, amelyek részletesen ismertetik a biztonsági hibák osztályba sorolásának és kezelésének folyamatát. A Microsoftot az elmúlt években sok kritika érte amiatt, hogy nem javítja rendszereiben a kutatók által bejelentett biztonsági hibákat, ezért az MSRC weboldalán (Microsoft Security Servicing Criteria for Windows) pontos leírást adnak a patch kedd során javításra kerülő Windows szolgáltatásokról, illetve azon kategóriájú további hibákról, amik a rendszerek következő kiadásaiban kerülnek javításra. A weboldalon három kategóriát különítenek el egymástól, a biztonsági korlátokat, a biztonsági funkciókat, illetve a mélységi védelmi funkciókat, amelyek közül az első kettő kategória jelenti a kritikus elemeket, amelyeket a patch kedd során kívánnak javítani, míg a harmadik kategóriába a további (kiegészítő) védelmi funkciók tartoznak. **Bővebben...**

Az eszköztitkosítás kijátszható egy új módszerrel

(www.techcrunch.com)

Az F-Secure új tanulmányában arról számol be, hogy „majdnem az összes" laptop és asztali munkaállomás sérülékeny egy új támadási módszerrel szemben. Mindez a már jól ismert „hidegindításos támadáson" alapul, az újdonság abban áll, hogy a kutatók megtalálták a módját, hogyan kapcsolják ki a memória újraírási folyamatot, ezt felhasználva pedig már az olyan népszerű merevlemez titkosító megoldások is gond nélkül megkerülhetők, mint a BitLocker, vagy a Mac-es FileVault. Olle Segerdahl, az F-Secure vezető biztonsági tanácsadója a TechCrunch-nak elmondta, a módszer ─ bár több lépcsőből áll ─ mégis olyannyira egyszerű, hogy valószínűtlennek tartja, hogy azt hacker csoportok ne fedezték volna fel már korábban. **Bővebben...**

Az EU fellép az autonóm fegyverek ellen

(www.euractiv.com)

Az Európai Parlament állásfoglalást fogadott el az emberi beavatkozást nem igénylő fegyverek fejlesztésének, gyártásának és felhasználásának nemzetközi szinten történő tiltásával kapcsolatban. Az autonóm fegyverek a mesterséges intelligencia segítségével önmaguktól, emberi ellenőrzés nélkül választhatnak célpontot, és indíthatnak támadásokat, ami a technológia ellenzői szerint egy kibertámadás, vagy programhiba esetén komoly veszélyt hordoz magában. A Human Rights Watch (HRW) emberi jogi szervezet úgy véli, az Egyesült Államok, Kína, Izrael, Észak-Korea, Oroszország és az Egyesült Királyság egyre közelebb kerülnek az autonóm fegyveres rendszerek alkalmazásához, amelynek első előfutárai a fegyveres drónok. A TASS hírügynökség egy 2017-es beszámolója szerint ráadásul az orosz fegyvergyártó Kalashnikov már egy olyan automatizált fegyvert is fejlesztett, ami képes azonosítani a célpontokat és önmagától döntéseket hozni. **Bővebben...**

Terror elleni harc: Az Európai Bizottság irányelvet terjeszt elő a hálózati feltöltések szűrési tárgyában

(www.heise.de)

Az internet- és felhőszolgáltatók, illetve adatmegosztó platformok kötelesek lesznek egy órán belül törölni a terror jellegű tartalmakat az Európai Bizottság egy friss javaslata alapján; az erre való kötelezést a koncepció szerint az Europol, vagy valamely tagország illetékes hatósága adhatná ki. Ezen tervezet a kisebb, illetve közepes szolgáltatók esetében sem állítana fel kivételeket ─ habár a szabályozás költségvonzatai problémát jelenthetnek majd számukra. **Bővebben...**