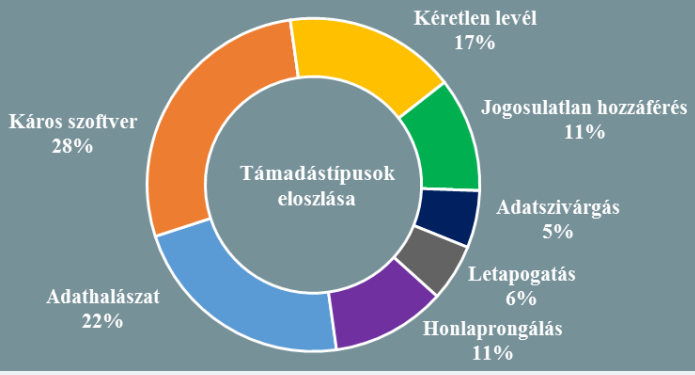
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.08.03. - 2018.08.09.



Kövessen minket online az itbiztonsag.govcert.hu oldalunkon, ahol naponta olvashatja legújabb híreinket!

Új kutatási eredményeket mutattak be az ipari vezérlő rendszereket támadó, hírhedt TRITON malware-ről

(www.nozominetworks.com)

A Black Hat USA 2018 konferencián hozták nyilvánosságra a NOZOMI Networks kutatását, amely az ICS rendszereket érő kibertámadások közül kiemelkedő TRITON malware-rel foglalkozik. A TRITON (más néven TRISIS, vagy HatMan) az első olyan szofisztikált káros kód, ami az ún. Safety Instrumented System (SIS) rendszereket, vagyis az ipari létesítmények automatizált védelmi rendszereit célozza, amelyek feladata a meghibásodások és különböző katasztrófa állapotok megelőzése. Többek között ennek a malwarenek tulajdonítják több közel-keleti olaj- és gázipari létesítmény 2017 decemberében történt leállását. A kutatók részletesen bemutatják, hogyan alakították ki a szimulációs környezetet, és hogyan voltak képesek egyes szoftverek visszafejtésével káros tevékenységeket végrehajtani. Az elemzés arra a következtetésre jut, hogy egy TRITON támadás kivitelezése nem igényel sem komoly anyagi erőforrásokat, sem jelentős szakismeretet, így az üzemeltetők sürgős feladata a SIS rendszerek monitorozása és biztosítása. Mindennek a támogatására két saját fejlesztésű, ingyenes eszközt is közreadtak a GitHubon. **Bővebben...**

Teljes a bizalom a Let's Encrypt tanúsítványok felé

(www.bleepingcomputer.com)

A Let's Encrypt bejelentette, hogy tanúsítványaikat immáron direkt módon elfogadja az összes nagy gyökértanúsító (root) szervezet, mint a Microsoft, a Google, az Apple, a Mozilla, az Oracle, és a Blackberry, ezeken keresztül pedig a nagyobb böngészők és operációs rendszerek is. A korábbi köztes elem, az IdenTrust kiiktatásra került, mivel ez magában hordozta annak az esélyét, hogy amennyiben az IdenTrust felé meggyengülne a bizalom ─ ami a közelmúltban például a Symantec esetében megtörtént ─ akkor az az összes Let's Encrypt tanúsítványt érintené. A cég közleménye szerint azonban egyes régebbi rendszerek nem kompatibilisek az új eljárással, és még legalább öt év kell ahhoz, hogy ezek kikopjanak a webes ökoszisztémából. **Bővebben...**

Ransomware támadás utáni helyreállító programot ad ki a BlackBerry

(www.techrepublic.com)

A Black Hat USA 2018 konferencián nyilvánosságra hozott szoftver a BlackBerry állítása szerint zsarolóvírus támadáskor képes „befagyasztani" a fertőzésben érintett fiókokat, és segítséget nyújtani egy korábbi, még biztonságos állapotra való visszaállásban. A rendszeradminisztrátorok ennek segítségével pontosan meg tudják határozni, hogy mely felhasználók, illetve mely könyvtárak és fájlok érintettek a fertőzésben, és lehetőségük van szelektíven, csak ezeket helyreállítani, amivel jelentős időt takaríthatnak meg. A cég szerint a tool-t hasznosnak fogják találni az ügyfelek, mivel a ransomware támadások ismét élénkülő periódusba kerültek. **Bővebben...**

Az Apple lecsapott egy összeesküvés-elméleteket terjesztő podcastre

(www.techcrunch.com)

A Google-t és a Facebookot követve az Apple is eltávolította az Infowars, egy hírhedt konteókat gyártó szervezet epizódjait az iTunesból és podcast alkalmazásaiból. Az említett tech cégekhez képest ─ akik csak négy részt töröltek ─ Tim Cook-ék szigorúbban jártak el, ők az összesen hat részből csak egyet, a „Real News With David Knight"-ot kímélték meg. A cég közleménye szerint az intézkedésre a gyűlöletbeszéd ellen felállított egyértelmű irányelvek megsértése miatt került sor. Az Infowarst korábban a Spotify és a Stitcher is letiltotta. **Bővebben...**

Az Apple Pay Cash vezeti a biztonságos mobil fizetési szolgáltatások listáját

(www.engadget.com)

Bár a tesztben résztvevő összes mobil P2P fizetési szolgáltatás használhatónak bizonyult, kiderült, hogy az Apple Pay Cash az átlagnál nagyobb hangsúlyt fektet a személyes adatok védelmére ─ állítja a Consumer Report által közzétett jelentés. A vizsgált mobil fizetési platformok közül jelenleg az Apple-é az egyetlen, amelyik irányelveiben kifejezetten korlátozza az ügyfelekről gyűjtött felhasználói és fizetési információkat ─ például a kártyaadatokat sem tárolja el ─ valamint vállalja, hogy amit mégis, azt nem értékesíti harmadik felek részére.
A teszt során a Venmo, a Square Cash és a Facebook Messenger is az átlagnál jobban teljesített, leszámítva az adatvédelmi szempontokat. A banki háttérrel rendelkező Zelle maradt le leginkább versenytársaitól, ami a tisztázatlan adatvédelmi irányelveknek és a fizetést megerősítő funkció hiányának köszönhető, utóbbit a cég október végéig kívánja pótolni. A teszt nem volt teljes körű, számos fizetési szolgáltatás, köztük a Google Pay újonnan integrált pénzátutalási funkciója is kimaradt. **Bővebben...**

IT biztonsági Tanács

Nemrég felfedeztek egy új metódust, amivel a Wi-Fi hálózatok biztosítására jelenleg még használt, azonban ismert módon sérülékeny WPA/WPA2 protokollok könnyebben törhetőek. Az új eljárás ugyan jelentősen megkönnyíti a támadó számára a Wi-Fi jelszó (PSK) hash illetéktelen megszerzését, azonban ennek visszafejtése továbbra is időigényes feladat. Emiatt javasolt az alapértelmezett helyett komplex, speciális karaktereket (pl.: &%$!) is tartalmazó PSK-t használni. E célból célszerű egy legalább 20-30 karakter hosszú, véletlen karakterláncot alkalmazni, amit jelszó generátorral is előállíthatunk.

Milyen tanulságai vannak a francia elnökválasztásnak?

(www.csis.org)

A 2017-es francia elnökválasztás során került nyilvánosságra napjaink legnyilvánvalóbb (sikertelen) kísérlete arra, hogy egy idegen ország egy másik nemzet belügyeibe, választásába beavatkozzon, ugyanis a később megválasztott francia elnök, Emmanuel Macron elleni orosz fellépés sem zavarkeltésben, sem a francia nemzet megosztásában nem érte el a célját. A CSIS által a közelmúltban megjelentetett tanulmány rávilágít arra, hogy hogyan állt ellen a társadalom a befolyásolási kísérletnek, illetve, hogy milyen tanulságok vonhatóak le, amelyek a 2018 őszi amerikai időközi választások során alkalmazhatók lehetnek. A beavatkozási kísérlet sikertelenségét több tényező okozta, többek közt az eltérő választási rendszer, az eltérő kulturális háttér, de még a sajtó és a média eltérő felépítése is szerepet játszott abban, hogy a kísérletnek nem lett választásokat befolyásoló hatása. **Bővebben...**

Az USA kiberbiztonsági gyakorlatot tart az energiaszektor ellenálló képességének felméréséhez

(www.securityaffairs.co)

Az Egyesült Államok Energiaügyi Minisztériuma (DoE) bejelentette, hogy az amerikai kritikus rendszereket érő kiberfenyegetések miatt gyakorlatot irányoztak elő, amelynek során a villamosenergia-hálózat kibertámadások utáni helyreállítási képességét fogják felmérni a célból, hogy felkészülhessenek egy valós támadásra. Az E&E News szerint a „Liberty Eclipse”-nek keresztelt, várhatóan egy hetes tesztet egy elszeparált elektromos hálózaton ─ a New York-közeli Plum Island-en ─ hajtják majd végre. Az energetikai rendszerek teljes leállás (Black Out) utáni újraindítása (Black Start) még a legkedvezőbb körülmények között is bonyolult és időigényes feladat, mivel az erőművek saját felhasználásra nem termelnek energiát. **Bővebben...**

Az angol jogszabályok megengedik a kettős mércét?

(www.theregister.co.uk)

Egy angliai biztonsági kutató rámutatott arra, hogy az angliai Halifax Bank oldalán olyan kliens oldali programok futnak, amik ellenőrzik, hogy a kliensen milyen portok vannak nyitva. A bank szerint ez biztonsági intézkedés, ezzel védik az ügyfeleiket, és véleményük szerint tevékenységük teljesen legális, hiszen azon túl, hogy ellenőrzik a nyitott portokat, más tevékenységet nem folytatnak. A biztonsági kutató ezzel szemben azzal érvel, hogy egyrészt, ha Ő, mint fehérsapkás hacker, felkérés nélkül szkennelné a bank rendszereit, azon nyomban megsértené a számítógépes visszaélésekről szóló törvényt (Computer Misuse Act), ahogy ez több független biztonsági kutatóval is megtörtént már. A bejelentő nem vitatja a bank jó szándékát, ám úgy véli az ilyen tevékenységhez a felhasználók explicit hozzájárulása szükséges, mely feltétel jelenleg nem teljesül. Véleménye szerint, ha a kód nem a belépő oldalon futna le, hanem bejelentkezés után, akkor legalább csak a saját ügyfelein végeznék a vizsgálatot és nem bárki gépén, aki az adott oldalt meglátogatja. Ennek kapcsán igyekszik felhívni a figyelmet arra, hogy a törvényeket nem lehet kettős mércével alkalmazni, azaz, vagy legális mindenki számára, hogy hozzájárulás hiányában végezzen port szkennelést, vagy jogszerűtlen, ebben ez esetben azonban a bank szorítkozzon saját ügyfeleire. **Bővebben...**

Hacker unikornisok márpedig léteznek

(www.warontherocks.com)

A „War on the Rocks” külpolitikai elemző portál szerint a hackerek számára a (z Amerikai Egyesült Államok)hadsereg(e) nem nyújt megfelelő lehetőségeket, emiatt még a tehetséges fiatalok is a civil szférában keresik a boldogulást. A szerző hátrányként említi az elavult, és nem megfelelően testre szabható előmeneteli rendszert, a civil szféránál jóval alacsonyabb bérezést, valamint a hadsereg sajátosságaként közismert többi, például ápoltság, testsúly, és fizikai követelményeket. **Bővebben...**