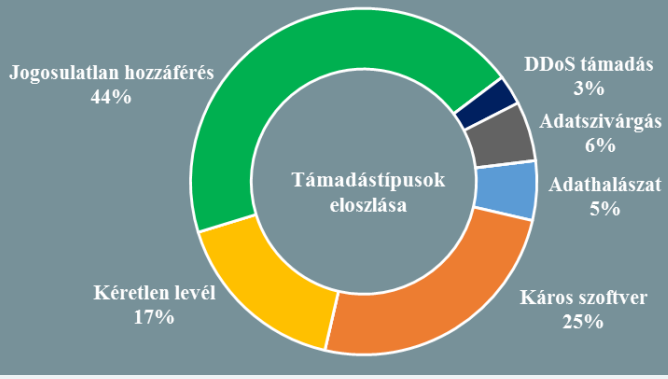
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.07.20. - 2018.07.26.



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

Kibervédelmi tervezetet hozott nyilvánosságra az USA Igazságügyi Minisztériuma

(www.securityweek.com)

Az amerikai főállamügyész által 2018 februárjában létrehozott kibervédelmi munkacsoport (Cyber-Digital Task Force) egy 156 oldalas jelentésben foglalja össze az Egyesült Államok számára aktuálisan legégetőbb kiberfenyegetéseket. A részleg elsősorban a szavazórendszerek és kritikus infrastruktúrák elleni támadásokat, az álhírek, valamint az erőszakos ideológiák terjesztését, illetve a bűnözői tevékenységek technológiai támogatását vizsgálja. A most publikált jelentés mindemellett kiemelten foglalkozik a 2018-as időközi választásokkal kapcsolatos aspektusokkal ─ köztük Oroszország szerepével ─ valamint a külföldi befolyásoló műveletek kezeléséhez javasolt tervekkel és javaslatokkal. **Bővebben...**

Oroszokhoz köthető kibertámadásokra fókuszál az új munkacsoport

(www.engadget.com)

Az NSA és a Cyber Command vezetője Paul Nakasone egy dedikált munkacsoportot (Russia Small Group) hozott létre az orosz rezsimhez köthető online fenyegetések kezelésére. Bár egyelőre nincs konkrét megfogalmazás a csoport feladatát illetően, Nakasone elárulta, hogy a tevékenységük összhangban áll majd a 2016-os amerikai elnökválasztás óta végzett műveletekkel, vagyis koncentráltan törekszenek elkerülni az akkori hackertámadások megismétlődését. A parancsnok azzal indokolta a csoport szükségességét, hogy amennyiben Amerika nem összpontosít digitális ellenfeleire, mint Oroszország és Kína, kimarad a virtuális csatatér formálásából, ezáltal ezek az ellenfelek alááshatják az amerikai választásokat, érzékeny információkhoz juthatnak és társadalmi feszültséget is szíthatnak. Felmerül a kérdés azonban, hogy az újonnan létrehozott munkacsoport számára elegendő idő áll-e rendelkezésre, hogy elérje teljes potenciálját és felkészüljön a 2018-as félidei választásokra. **Bővebben...**

Újabb aggályok merültek fel a Huawei termékekkel kapcsolatban

(www.reuters.com)

Az Egyesült Királyságban működő Huawei Kiberbiztonsági Értékelő Központ (HCSEC) múlt héten kiadott jelentésében azonosított hiányosságok új kockázatokat tártak fel a brit távközlési hálózatokban. A kormányzati jelentés tovább fokozza a kínai kormánnyal kapcsolatos kémkedési aggodalmakat, ugyanis csak korlátozott biztosítékot találtak arra vonatkozóan, hogy a Huawei nem jelent nemzetbiztonsági kockázatot, így a korábbi állapothoz képes rosszabb minősítést kapott a cég. A brit kormány és a hírszerző ügynökségek alá tartozó HCSEC az infrastruktúrájukban működő összes Huawei terméket és folyamatot átvizsgálta, amelynek során több technikai kérdést is megfogalmaztak, például a külső beszállítókkal, a harmadik felektől származó szoftverek biztonságával, továbbá a belső termékkódok ellenőrzésével kapcsolatban. Utóbbi javítására már folyamatban van a megoldási program, amelynek teljesítési határideje 2020 közepe. **Bővebben...**

Már lehet regisztrálni a 6. NCSS workshopra

(www.enisa.europa.eu)

Idén szeptember 18-án, Helsinkiben kerül megrendezésre a 6. NCSS (National Cyber Security Strategy) workshop, amelyet az ENISA a Finn Hírközlési Szabályozó Hatósággal közösen szervez. Az esemény az NCSS fejlesztésére, végrehajtására és értékelésére, valamint az információ megosztási és analitikai központok (ISAC) Unión belüli létrehozására összpontosít majd, amelynek során a különböző tagállamokból érkező szakértők bemutatják az információcserével kapcsolatos főbb fejlesztési megközelítéseket, legjobb gyakorlatokat, kihívásokat és lehetőségeket. **Bővebben...**

Ezért (is) nehéz detektálni az androidos vírusokat

(www.bleepingcomputer.com)

Androidon is egyre jellemzőbb, hogy a támadók a káros kódok készülékekre juttatását több fázisban valósítják meg, ennek során az ún. „droppereknek” van nagy jelentősége. Ezek olyan káros kódok, amelyek fő feladata, hogy további, jóval potensebb összetevőket ─ például egy banki trójait ─ töltsenek le az áldozat eszközére. Mivel a dropperek az átlagos malware-eknél jóval kevesebb jogosultságot igényelnek, és csak igen korlátozott tevékenységet végeznek, sokkal könnyebben képesek észrevétlen maradni. A segítségükkel végrehajtott támadások többek közt azért hatékonyabbak mobil platformon, mint a desktop környezetben, mivel a mobil eszközökre jóval kevesebben telepítenek vírusvédelmi termékeket. Az aktuális trend szerint a legtöbb támadás során nagyon hasonló felépítésű droppereket használnak, aminek vélhető oka az, hogy egyes bűnözői csoportok egy népszerű üzleti modellt alkalmazva a különböző malware kampányokhoz „bérbe adják” a letöltő modult (downloader-as-a-service ─ DaaS). **Bővebben...**

IT biztonsági Tanács

Jellemző zsarolási kísérlet, hogy a zsarolók a felhasználó otthoni webkamerájával készített kompromittáló felvételekre hivatkozva igyekeznek pénzt kicsalni az áldozattól. A fenyegetés alátámasztásának legegyszerűbb módja, hogy a támadó a videó fájlt eleve csatolja a fenyegető levélhez, ennek hiányában kevéssé valószínű, hogy a támadó valóban rendelkezik kompromittáló anyaggal. Ám ne csupán emiatt ne fizessünk a zsarolónak, hanem mert soha nem bizonyosodhatunk meg arról, hogy a hivatkozott tartalom valóban törlésre kerül.

Hamis hírek elleni törvényt mutattak be Oroszországban

(www.nytimes.com)

Oroszországban már egy ideje büntethetőek azok a felhasználók, akik bizonyos tiltott ─ például szélsőséges eszméket hirdető, vagy a közrendet veszélyeztető ─ tartalmakat osztanak meg a közösségi fiókjukon keresztül, azonban egy új törvényjavaslat szerint magukat a platformokat is felelősségre vonnák ─ írja a The New York Times. Eszerint a több, mint 100 000 felhasználóval rendelkező online közösségi médiaoldalak 50 millió rubel összegű pénzbírságra számíthatnak, amennyiben az észlelést követő 24 órán belül nem távolítják el platformjukról a „pontatlanságot” tartalmazó felhasználói posztokat. A jogszabálytervezet sok kritika éri, egyesek amiatt aggódnak, hogy a moderátorok az igazságtartalom megállapításakor inkább a hatóságoknak kedvezve döntenek majd, a szolgáltatók pedig attól tartanak, hogy nem lesznek képesek 24 órán belül kivizsgálni az eseteket a megjelenített tartalmak számossága miatt. **Bővebben...**

A GDPR-t is megsértve gyűjtött a böngészőkből személyes adatokat egy cég

(www.bleepingcomputer.com)

A hirdetésblokkoló AdGuard vizsgálata során több olyan Chrome és Firefox bővítményt, valamint Android és Apple alkalmazást azonosított, amelyek különböző megtévesztő technikákat alkalmazva személyes adatokat gyűjtenek a felhasználókról. A vizsgálatok során kiderült, hogy mindegyik hátterében ugyanaz a cég, a Big Star Labs áll, akik több szinten is megsértették az Európai Unió általános adatvédelmi rendeletét (GDPR), ugyanis alkalmazásaik esetenként az összes böngészési előzményt begyűjtötték, és az URL-eket is változatlan formában tárolták el, ellentétben az adatvédelmi irányelvekben állítottakkal, miszerint kizárólag anonimizált adatokat gyűjtenek. Mindezek mellett azt is elmulasztották közölni a felhasználókkal, hogy adataikat kivel, és milyen módon osztják meg. Az AdGuard szakértői az eset nyilvánosságra hozásától azt várják, hogy a problémáról való értesülést követően az érintett platformok el fogják távolítani az alkalmazásokat **Bővebben...**

Immár utazás közben is biztonságban lehetnek a jelszavaink

(www.blog.agilebits.com)

A kellően bonyolult és hosszú jelszavak megjegyzésére legtöbbször egy jelszókezelő program alkalmazását javasolják több fórumon is, például a SANS hírlevél is dedikált egy számot a témával kapcsolatban. A 1Password jelszókezelő ebben a témában is szintet tudott lépni, az „utazás üzemmód” bevezetésével. Az üzemmódot kifejezetten a felhasználói visszajelzések alapján fejlesztették ki, célja, hogy elrejtse a jelszókezelő alkalmazás meglétét a kíváncsi hivatalos szervek előtt. Például, az Amerikai Egyesül Államok területére való beutazás során a bevándorlási hivatal tisztje kérheti, hogy a belépni szándékozó oldja fel a telefonját vagy laptopját, ezzel felfedve az elmentett jelszavakat és belépési adatokat is. Az új funkció nemcsak elrejti ezeket az adatokat, hanem – az utazásra biztonságosnak megjelölt széfek kivételével – teljes egészében eltávolítja a telepített széfeket az eszközökről mindaddig, míg az utazás üzemmód engedélyezve van. A csoport mód ehhez képest még olyan többletfunkcióval is rendelkezik, hogy a csoport adminisztrátora határozhatja meg azon adatok körét, amelyek az üzemmód aktiválását követően is elérhetőek maradnak. **Bővebben...**