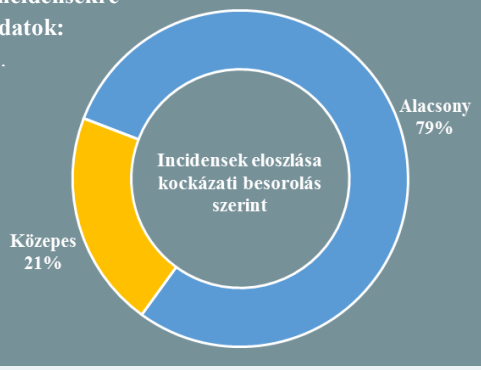
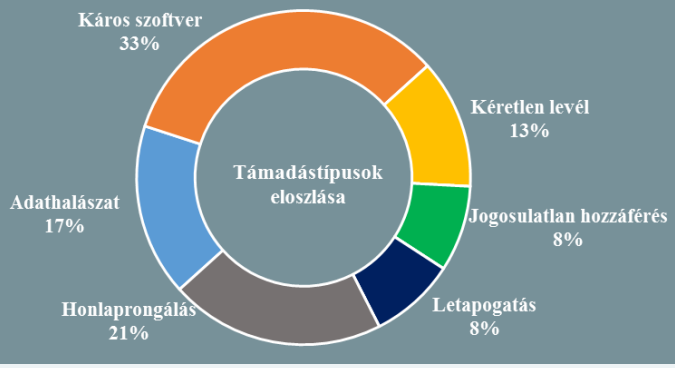
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.08.17. - 2018.08.23.





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

A LinkedIn megnyitja „adatkapuját” a kutatók előtt

(www.engadget.com)

A Bloomberg információi szerint a világ legnagyobb üzleti közösségi hálózata elérhetővé teszi adatait a kutatók számára, hogy ezzel segítse a munkaerőpiac, és a gazdaság terén folytatott kutatásokat. A vállalat olyan pályázatokat vár, amelyek valamilyen módon elemezésekkel, gazdasággal, vagy mesterséges intelligenciával foglalkoznak, ezek közül jövő év elején választják ki a támogatni kívánt projekteket. A LinkedIn számos védelmi intézkedést hozott ügyfelei adatainak biztosításához, így a kutatók csak aggregált, anonimizált adatokhoz férhetnek hozzá, azok saját kezű letöltésére pedig nem lesz lehetőségük, minden igényt előbb ellenőrizni fog a cég jogi és biztonsági osztálya. **Bővebben...**

Regionális kiberfenyegetések az „Új selyemút” körül

(www.securityaffairs.co)

A FireEye és a Recorded Future szakértői növekvő kiberkémkedési tevékenységre figyelmeztetnek a kínai „Új selyemút” (Belt and Road Initiative ─ BRI) projekt vonatkozásában, ami Délkelet-Ázsia, Közép-Ázsia, a Közel-Kelet, Európa és Afrika egyes országait összekötő infrastruktúra kiépítését célozza. A FireEye szerint a projekt jelentős stratégiai potenciállal bírhat bármely hírszerző szolgálat számára, ezért az ezzel kapcsolatos információgyűjtés jelentős megélénkülésére lehet számítani. Az egyik ilyen, jelenleg is zajló kampány a kínai kötődésű Roaming Tiger APT csoporté, akiket korábban orosz és belarusz célpontok elleni aktivitással is vádoltak, aktuálisan pedig ─ többek között ─ a BRI projektben érintett európai országok külügyminisztériumai ellen vetnek be káros kódokat, mint például a TOYSNAKE backdoort. Mindemellett az ázsiai és közel-keleti térségben egyre több feltörekvő csoport esetében tapasztalható nagyarányú kiber képességfejlesztés ─ jó példa erre Vietnám ─ akik a növekvő támadó potenciált nem félnek bevetni az országhatáraikon belül tevékenykedő külföldi vállalatokat ellen. **Bővebben...**

Inkompatibilis programokról figyelmeztet a Chrome

(www.bleepingcomputer.com)

A Google egy új biztonsági funkciót vezetett be a Chrome stabilitásának javítása céljából, miszerint figyelmeztető üzenetet küld a felhasználóknak azon „összeférhetetlen” alkalmazásokról, amelyek kódot fecskendeznek a Chrome folyamataiba. A három fázisra bontott intézkedésről már tavaly óta tudni, hogy végső célja az, hogy automatikusan blokkoljon minden, a böngészőbe történő kód befecskendezést. Mindezt csak 2019 januárja után tervezik bevezetni, a jelenlegi második fázisban még csak figyelmeztetik a felhasználókat, hogy távolítsák el a kérdéses programokat. A funkciót fokozatosan állítják élesbe, akinél már elérhető, az a chrome://settings/incompatibleApplications URL-en ellenőrizheti, hogy a rendszerén található-e ilyen program. A BleepingComputer információi szerint már több hír is érkezett arról, hogy sok esetben AV termékek kerülnek ily módon megjelölésre ─ például Malwarebytes, Bitdefender, ESET, Emsisoft, AVG, IOBit, Avast ─ több más, széles körben használt program mellett, mint a Dropbox, vagy a FileZilla. **Bővebben...**

Politikai tiltakozás kibereszközökkel

(www.securityaffairs.co)

Ellehetetlenítették Spanyolország több kormányzati honlapjának működését, a magukat a hírhedt Anonymus kollektíva tagjainak valló hackerek, akik a Twitteren közzétett bejegyzésük szerint az akcióval Katalónia függetlenségi törekvéseit kívánták támogatni. Az #OpCatalunya néven hivatkozott művelet során elérhetetlenné vált az Alkotmánybíróság, valamint a Gazdasági minisztérium, illetve a Külügyminisztérium weboldala is. **Bővebben...**

Adatgyűjtés miatt tiltott ki egy Facebookos alkalmazást az Apple

(www.engadget.com)

A Facebooknak el kellett távolítania az Onavo Protect nevű VPN alkalmazását az App Store-ból, mivel az sértette az Apple júniusban megszigorított irányelveit, amelyek korlátozzák, hogy a programok miként és milyen célból gyűjthetnek adatokat. Az Engadget információi szerint az Onavo Protect által végzett felhasználói adatgyűjtés és elemzés többszörösen áthágta ezeket a szabályokat, valamint sértette a fejlesztői megállapodás azon záradékát is, ami tiltja az adatok bármilyen, az alkalmazás működésével összefüggésbe nem hozható — például reklám — célra történő felhasználását. A Facebook például ezt az applikációt felhasználva értesült a Snapchat népszerűségének csökkenéséről, hónapokkal az információ nyilvánosságra kerülése előtt. A cég beleegyezett az alkalmazás törlésébe, így augusztus 22-e óta az már nem érhető el az Apple alkalmazásboltjában. Azon felhasználók, akik korábban telepítették az applikációt, továbbra is használhatják, azonban frissítés már nem érkezik hozzá. **Bővebben...**

IT biztonsági Tanács

A kétfaktoros azonosítás egy mindenképp javasolt biztonsági intézkedés, azonban alkalmazása előtt informálódjunk annak kockázatairól is. Hitelesítő applikáció használatakor készítsünk offline biztonsági másolatot a 2FA beállításakor az adott szolgáltatás (pl.: Gmail) weboldalán megjelenített QR kódról. A legegyszerűbb azt kinyomtatni, de egy megbízható személy (pl.: családtag) eszközén is tárolhatjuk backup gyanánt, így az azonosításra használt eszköz elvesztése esetén sem veszítjük el a kontrollt fiókjaink felett.

Külföldi cégek nem vehetnek részt az ausztrál 5G hálózat kiépítésében

(www.zdnet.com)

Ausztrália kormánya nemzetbiztonsági okokra hivatkozva kizárta a külföldi gyártókat az ország 5G-s mobilhálózatának kialakításából, ezzel többek között olyan, a technológia terén piacvezető tech óriásokat is, mint a Huawei, vagy a ZTE. Mitch Fifield kommunikációs és Scott Morrison belügyminiszter közös nyilatkozata szerint az ausztrál kormány komoly aggodalmakat táplál az olyan külföldi cégek bevonásával szemben, akik idegen államhatalmakhoz köthetőek. Az intézkedés kapcsán a tavaly előirányozott és 2018. szeptember 18-án hatályba is lépő Távközlési Ágazati Biztonsági Reformra (TSSR) hivatkoznak, ami jelentős szigorításokat fogalmaz meg a telekommunikációs cégek számára az ausztrál hálózatok elleni illetéktelen hozzáférések megakadályozása céljából. **Bővebben...**

A fogyasztók megtévesztésével vádolják a Trivagot

(www.zdnet.com)

Az Ausztrál Verseny- és Vásárlásfelügyeleti Bizottság (ACCC) eljárást kezdeményezett a Trivago online szálláskereső szolgáltatás ellen, arra hivatkozva, hogy a cég megsérti az ausztrál vásárlóvédelmi törvényt. Az ACCC vádja szerint a cég legalább 2013 decembere óta félrevezető árakat jelenít meg honlapján, valamint televíziós reklámjaiban, és azt a hamis illúziót kelti, hogy az összegyűjtött szállásajánlatok közül objektív szempontok alapján jeleníti meg a legjobb ajánlatokat. Az ACCC azonban úgy véli, a hirdetések aszerint priorizáltak, hogy a szállások mekkora összeget hajlandóak kifizetni a hirdetések után, a Trivago fő bevétele ugyanis abból származik, hogy nem a hirdetés megjelenítéséért, hanem az arra történt kattintások mennyisége alapján számít fel költséget (lásd: „cost per-click” modell). Ez az eljárás mind a fogyasztók, mind a hirdetők számára káros, a Trivagonak pedig egyértelműen a fogyasztók tudomására kell hoznia, hogy ez alapján állítja össze a sorrendet. **Bővebben...**

Több ezer hamis alkalmazást töröltek a kínai App Store-ból

(www.bleepingcomputer.com)

Az Apple hamis szerencsejáték alkalmazásokat távolított el az App Store-ból, valamint az ezeket értékesíteni próbáló fejlesztők is kitiltásra kerültek. A Wall Street Journal szerint a tech cég eddig már összesen 25 000 alkalmazást törölt annak érdekében, hogy megfeleljen a szigorú kínai jogszabályoknak. A mostani intézkedést Kína legnagyobb közszolgálati televíziója, a Kínai Központi Televízió (CCTV) kérelmezte, miután értesült egy kínai iPhone felhasználóról, aki egy hamis alkalmazáson keresztül vásárolt lottót 122 000 jüan (körülbelül 17,5 dollár) értékben. A férfi azóta kártérítési keresetet nyújtott be, amit egy sanghaji kerületi bíróság el is fogadott. A CCTV szerint a károsult korábban többször is hívta az Apple ügyfélszolgálatát, valamint személyesen is felkereste a vállalat sanghaji kirendeltségét, azonban nem kapott segítséget. **Bővebben...**

Adatszivárgás történt az amerikai T-Mobile-nál

(www.motherboard.vice.com)

A Motherboard információi szerint 2018. augusztus 20-án ismeretlenek egy API-n keresztül hozzáfértek a vállalat mintegy 2 millió ügyfelének adataihoz, köztük nevekhez, e-mail címekhez és egyes fiók, valamint számlázási adatokhoz, azonban szenzitív információkhoz — mint például jelszavak vagy kártyaszámok — nem. A támadást még aznap felfedezték, és sikeresen elhárították, azonban ennél több részletet eddig nem árultak el. A cég SMS üzenetben tájékoztatja az érintett felhasználókat. **Bővebben...**