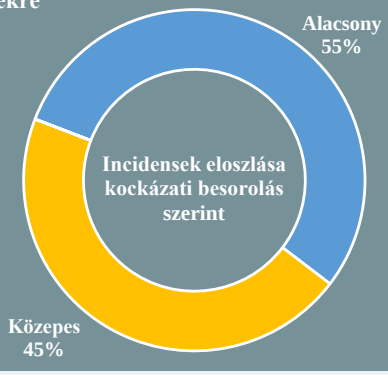
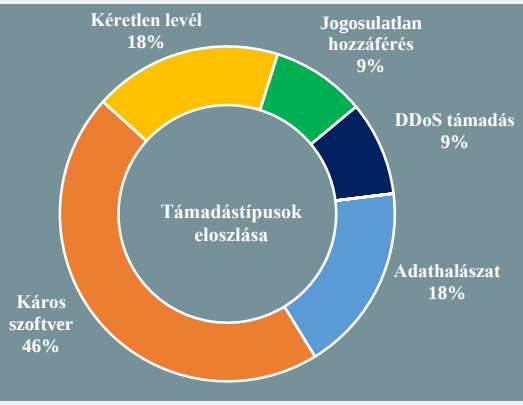
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.07.27. - 2018.08.02.





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

Cenzúrázó keresőt indít a Google Kínában

(www.reuters.com)

A kínai cenzúra szabályokra szabott webes kereső kivitelezése „Dragonfly" kódnév alatt 2017 tavasza óta zajlik, azonban csak év végén kapott lendületet, miután a Google vezérigazgatója, és egy magas rangú kínai tisztségviselő a témában megbeszélést folytatott. Információk szerint ─ többek között ─ emberi jogokkal, demokráciával, vallással és béketüntetésekkel kapcsolatos kifejezések szerepelnek majd a kereső motor feketelistáján, amit a The Intercept szerint már be is mutattak a kínai kormánynak. A kereső élesbe állása valamikor a következő hat és kilenc hónap között valószínűsíthető, a kínai hatóságok engedélyezési eljárásától függően. Sem a Google, sem Kína internetes szabályozó szerve (Kibertér Adminisztrációs Iroda) nem reagált a Reuters megkeresésére. **Bővebben...**

Tanulmány az Onion szolgáltatások használatáról

(hci.princeton.edu)

A Princeton Egyetem kutatói tanulmányukban azt vizsgálták, hogy a felhasználók mennyire értik az online anonimitást biztosító Tor (The Onion Router) hálózat működését, hogyan használják azt, és eközben milyen nehézségekbe ütköznek. A felmérés eredményei szerint a megkérdezettek több, mint fele nem volt tisztában a Tor néhány alapvető működési elvével, valamint kiderült, hogy a felhasználóknak gondot okoz az onion-os domain formátum értelmezése, és az ilyen címek felderítése, mivel ezeket nem indexelik a webes keresők. Ennek oka, hogy valójában nem is hagyományos DNS nevekről van szó, hanem a szerverek publikus kulcsából több lépcsőben generált hash-ekről, amelyek azonban fontos részét képezik a rendszernek. **Bővebben...**

Fontos újításokat vezetett be a ProtonMail

(securityaffairs.co)

A ProtonMail 3.14-es verziójával több újítást is bevezetett, az egyik ilyen a címellenőrzés, ami azon támadásokat kívánja megakadályozni, amelyek során a támadó a saját nyilvános kulcsát juttatja el az áldozatnak, hogy aztán az ehhez tartozó privát kulcs birtokában a kommunikációba ékelődve (man-in-the-middle) el tudja olvasni a titkosított üzeneteket. A ProtonMail új webes verzióján ugyanis lehetőség van a publikus kulcsokat megbízhatónak minősíteni, amit ekkor a rendszer titkosít és digitális aláírással lát el, amivel egyszer s mindenkorra elkerülhető, hogy harmadik fél ezt manipulálja. Egy második fontos újdonság, hogy a PGP kulcsok immáron szabadon importálhatóak, valamint exportálhatóak, így lehetőség van nem ProtonMail-es fiókkal rendelkezőkkel is PGP-zett üzeneteket váltani. **Bővebben...**

Digitális bizonyíték, bűnüldözés

(www.csis.org)

A washingtoni (USA) székhelyű Stratégiai és Nemzetközi Tanulmányok Központja (CSIS) által júliusban kiadott tanulmány szerint az amerikai bűnüldöző szervek még soha sem néztek szembe olyan jelentős akadályokkal a digitális bizonyítékok gyűjtése során, mint napjainkban. A kutatás során megkérdezésre kerültek szövetségi, állami, és helyi bűnüldöző hatóságok képviselői, de ügyvédek, szolgáltatók és civil csoportok is. A tanulmány célja az volt, hogy a különböző szereplők szemszögéből megvilágításra kerüljenek azok a problémák, amikkel a hivatalos szervek szembesülnek a digitális bizonyítékok beszerzése során. A kutatás rámutatott, hogy a szolgáltatóik által tárolt digitális bizonyítékokhoz való hozzáférés – melynek túlnyomó többsége nem titkosított – a legnagyobb kihívás. A tanulmány szerint „minden rendőrnek és ügynöknek képesnek kell lennie bizonyítékok gyűjtésére és azok megőrzésére, mint például az ujjlenyomatok, vagy a DNS minták, de nem minden hivatástól várják el, hogy ezeket a bizonyítékokat értelmezze – ez a szakértők feladata. Ugyanennek az elvnek kellene érvényesülnie a digitális bizonyítékok esetében is." **Bővebben...**

Windowsos malware-t találtak a Google Play Store-on

(researchcenter.paloaltonetworks.com)

A Palo Alto szerint több, mint 145 applikáció került törlésre a Play Store -ból, amiért azok káros Windows-os binárisokat tartalmaztak. A különböző témájú alkalmazásokat még 2017 októbere és novembere között töltötték fel a Google áruházába, volt köztük olyan, ami ruházkodással („Learn to Draw Clothing"), volt amelyik kerékpár átalakítással („Modification Trail") foglalkozott, egyesek több ezres letöltéssel rendelkeztek, és jó (4-es) minősítést kaptak a felhasználóktól. A biztonsági cég szerint a káros kódok Androidos rendszeren hatástalanok voltak, a felhasználókra nézve veszélyt elsősorban akkor jelenthettek, ha a fertőzött APK fájlokat Windows-os környezetben nyitják meg, ekkor a beágyazott futtatható fájl ugyanis egy key loggert telepít a rendszerre. A cég szakemberei felhívják a figyelmet a fejlesztői környezetek biztonságának fontosságára, mivel a szoftveres ellátási lánc kompromittálása napjainkban a malware támadások egyik leghatékonyabb módja ─ a példánál maradva, a fejlesztők különböző platformok számára is készíthetnek szoftvereket. **Bővebben...**

IT biztonsági Tanács

Kísérjék figyelemmel a szervezet által alkalmazott szoftverek támogatási idejéről szóló gyártói információkat. Ennek segítségével a támogatás megszűnéséről időben értesülhetnek és tervezhetővé válik a helyettesítő eszközök beszerzése. Célszerű minderről egy saját nyilvántartást vezetni és időközönként felülvizsgálatot tartani.

A munkafolyamatokat támogató szoftverek mellett ne feledkezzenek meg a IT-biztonsági infrastruktúra elemeiről sem (például a Gemalto autentikációs menedzsment termékek, amelyek támogatása tavaly év végén megszűnt).

Az NCSC biztonsági útmutatót adott ki az Ubuntu 18.04 LTS kiadásához

(blog.ubuntu.com)

Az Egyesült Királyság Kiberbiztonsági Központjának (NCSC) ─ a brit kormányzat információbiztonságáért felelős szervezeteként ─ egyik alapfeladata legjobb gyakorlatok és útmutatók készítése a köz-, valamint a magánszféra számára. E minőségében készítette legutóbbi anyagát is, amely az egyik legnépszerűbb Linux disztribúció, az Ubuntu legújabb kiadásának javasolt biztonsági beállításait tartalmazza. Az összefoglaló többek között érinti a távoli hozzáférés VPN-en keresztüli beállítását, az erős jelszó házirend alkalmazását, az UEFI megfelelő konfigurálását, a Kernel Livepatch engedélyezését, vagy a tűzfal megfelelő konfigurálását. **Bővebben...**

Sokkal beszédesebbek a közösségi média oldalakról származó metaadatok, mint korábban gondolták

(www.ucl.ac.uk)

A londoni University College kutató által nemrégiben publikált, 5 millió Twitter felhasználói fiókot alapul vevő tanulmány szerint az olyan jelentéktelennek tűnő adatok is, mint például a metaadatok, lehetőséget teremtenek arra, hogy a közösségi hálózatokon belül az egyedi felhasználókat szinte 100%-os pontossággal azonosítani lehessen. A metaadatokat gyakran a nem érzékeny adatok körébe sorolják, ennek ellenére a tanulmány szerzői 96,7%-os pontossággal képesek voltak kizárólag ezek alapján azonosítani az egyedi felhasználókat egy 10 000 fős csoporton belül. A kutatók megállapították továbbá, hogy a jelenleg alkalmazott adatködösítő, adatmanipulációs technológiák sem hatékonyak a metaadatok esetében, a tesztadatok több, mint felének összekeverését követően is 95%-os pontossággal lehetett az egyedi felhasználókat azonosítani. **Bővebben...**

Kiberbiztonság az űrben

(www.belfercenter.org)

Amikor a kritikus infrastruktúrákra gondolunk, legtöbbünknek az elektromos hálózat, a vízellátás, vagy a közlekedés jut eszébe. A fogalmat jobban kifejtve eszünkbe juthat még a mezőgazdaság, a honvédelem, vagy a pénzügyi szektor is, azonban ritkán gondolunk azokra a szolgáltatásokra, amik mindezek működését lehetővé teszik. Az Amerikai Egyesült Államokban a legtöbb kritikus infrastruktúra az űrben lévő eszközök által biztosított szolgáltatásokon nyugszik, legyen az telekommunikáció, meteorológia vagy GPS. Egy közelmúltban megjelent kutatás szerint ezeknek az (űrben lévő) eszközöknek a biztonságával kapcsolatban jelentős hiányosságok tapasztalhatóak: Bár a kritikus infrastruktúrára vonatkozóan léteznek szabályok és eljárások, ezek a szabványok alig kerülnek átültetésre az űriparban. Hovatovább, ezek a rendszerek technológiai szempontból jóval összetettebbek, illetve a tulajdonjog és a management kérdésköre is több kérdést vet fel. **Bővebben...**

Egyelőre mégsem vetheti meg a lábát a Facebook Kínában

(www.zdnet.com)

A tech óriás a múlt hét során egy leányvállalat bejegyzésére kapott engedélyt Kínában, ám végül csupán néhány óráig szerepelt a kínai cégjegyzékben, mivel nem sokkal a hivatalos bejelentést követően törölték onnan. A Facebook szóvivője szerint a cég a kínai fejlesztők és startupok számára szeretett volna egy tréningekre és workshopokra koncentráló innovációs központot nyitni az Alibaba főhadiszállásának is otthont adó Hangcsouban, ahogy tette azt korábban a világ számos pontján, például Brazíliában, Franciaországban, Indiában és Dél-Koreában. A Zdnet úgy tudja, hogy helyi tisztviselők és az internetes felügyeletet ellátó Kibertér Adminisztrációs Iroda közötti nézeteltérés vezetett az engedély visszavonásához. **Bővebben...**