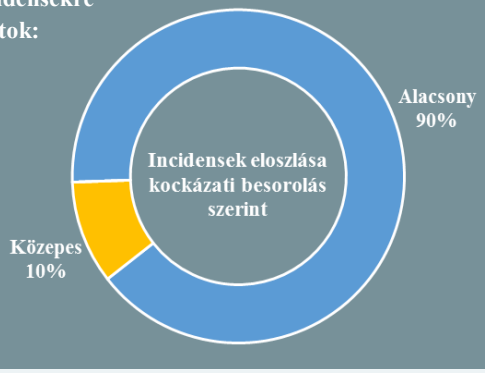
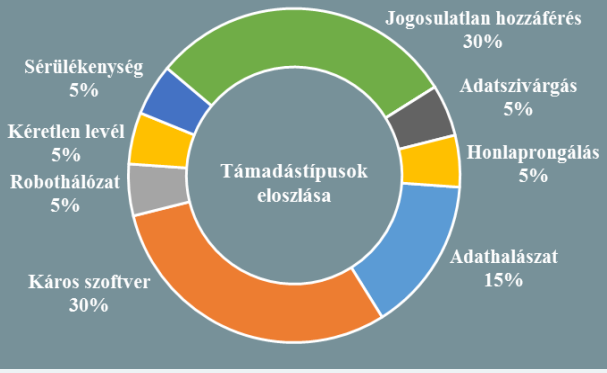
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.06.15. - 2018.06.21.





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

A hatóságok felszámolták Franciaország legnépszerűbb illegális weboldalát

(www.ehackingnews.com)

A francia hatóságok június 12-én felszámolták a több mint két éve működő „Black Hand" kábítószer- és fegyverkereskedelemre, valamint adatbázisok és hamis dokumentumok értékesítésére használt hírhedt darknetes fórumot. A weboldalhoz – melyet csak egy speciális szoftver segítségével lehetett elérni – több mint 3 000 felhasználó rendelkezett hozzáféréssel. A francia Vámügyi Nyomozóigazgatóság (DNRED) több mint 40 ügynök bevetésével végzett intenzív házkutatásokat több francia városban, ennek során sikerült letartóztatni az oldal állítólagos üzemeltetőjét, egy 28 éves nőt, valamint három további személyt. **Bővebben...**

Az Europol felszámolta az egyik legrégebbi hacker csoportot

(www.bleepingcomputer.com)

Az Európai Rendőrségi Hivatal nemzetközi összefogással nyolc embert tartóztatott le, akik a hírhedt Rex Mundi („A világ királya") nevű hacker csoporthoz tartoztak. A csoport legalább 2012 óta volt aktív, munkamódszerük pedig a vállalatok informatikai magánhálózatába történő betörések során szenzitív információk zsákmányul ejtése volt. Ezt az áldozattal való kapcsolatfelvétel követte, amelynek során igyekeztek váltságdíjat kikényszeríteni annak fejében, hogy az adatokat nem hozzák nyilvánosságra. Esetenként

egy magasabb összegért a biztonsági rést is felfedték, amin keresztül a betörést megvalósították. A csoport azonban az utóbbi években – hála a bűnüldöző hatóságok intenzív letartóztatásainak – már egyre kevesebb támadást intézett. A vesztüket jelentő esetre végül 2017 júniusában került sor, melynek során egy brit vállalatot támadtak meg, és zsaroltak a szokásos módon, ezúttal viszont jóval magasabb összegért. **Bővebben...**

Nemzetbiztonsági aggályok a Google-Huawei együttműködés kapcsán

(www.cyberscoop.com)

A hónap elején öt amerikai törvényhozó szólította fel a Google-t, hogy vizsgálja felül partneri együttműködését a kínai Huawei gyártóval, mellyel szemben nemzetbiztonsági aggályok miatt egyre erősödik a kongresszus kritikája. A szenátorok által szerdán megfogalmazott nyílt levélben említésre került, hogy a Google utóbb visszautasította a Védelmi Minisztériummal kötött, „Project Maven" névre keresztelt kutatási együttműködés meghosszabbítását, így a szerzők szerint a cégóriás nagyobb hajlandóságot mutat a Kínai Kommunista Párt támogatására, mint az amerikai hadsereggel való együttműködésre. A Google szóvivőjének válasza szerint cégük - ugyanúgy, mint számos más amerikai vállalat -, több tucat OEM gyártóval köt partneri megállapodást világszerte, beleértve a Huawei-t is. A megállapodás nem biztosít speciális hozzáférést a Google felhasználói adatokhoz, sőt adatvédelmi és biztonsági kitételeket tartalmaz a felhasználói adatokra vonatkozóan. **Bővebben...**

A Facebook oktatással segíti az SMB-ket

(www.engadget.com)

A Facebook a TeachPrivacy-vel együttműködésben 10 konkrét, adatvédelemmel kapcsolatos témakörben szervez képzéseket kis- és középvállalkozásoknak (SMB). Az alkalmakra Baltimoreban, New Orleansban, San Diegoban, Palo Altoban és Edisonban kerül sor, de a Promontory tanácsadói csoport segítségével Európában is terveznek képzéseket. A közösségi oldal egy FbStart nevű programot is létrehozott a kezdő mobilalkalmazás-fejlesztők oktatására. **Bővebben...**

Automatikusan tudatja majd az iOS, hogy honnan hívják a segélykérő vonalat

(www.bleepingcomputer.com)

Az Apple bejelentése szerint az iOS új (12-es) verziója automatikusan továbbítani fogja a 911-es hívóközpontokhoz beérkezett sürgősségi hívások helyadatait az Egyesült Államokban. Ehhez a cég két technológiát alkalmaz, az egyik a saját fejlesztésű HELO (Hybridized Emergency Location), ami a mobiltelefon-átjátszó tornyok, a GPS és a Wi-Fi hozzáférési pontok segítségével beméri a készülékek körülbelüli helyzetét, a másik pedig a RapidSOS által fejlesztett internet alapú protokoll, ami gyorsan és biztonságosan osztja meg a HELO adatokat. Az Apple új funkciója az FCC szabályok szerint készül, ami előírja, hogy a mobilszolgáltatóknak 2021-re képesnek kell lenniük az idő 80%-ban, 50 méteren belüli pontossággal bemérni a 911-hez beérkező hívásokat. **Bővebben...**

IT biztonsági Tanács

Ne gondoljuk, hogy minden alkalmazás megbízható, ami magas letöltési számmal rendelkezik, egyes rosszindulatú fejlesztők ugyanis éppen ezáltal tévesztik meg a jóhiszemű felhasználókat. Tartsuk észben, hogy a letöltésre vonatkozó hiteles adat az "Olvass tovább" menü alján található, bármilyen erre vonatkozó, de ettől eltérő helyen elérhető információ jó eséllyel megtévesztés céljából került feltüntetésre.

A Labdarúgó-világbajnokság idején a futball témájú káros alkalmazások is elszaporodnak, ezért legyünk körültekintőek az ilyen témájú programok használata során.

Újabb eszközzel figyelheti állampolgárait a kínai kormány

(www.cnet.com)

A Wall Street Journal információi szerint jövő hónaptól a kínai piacon megjelenő autókat RFID (Radio Frequency IDentification) chipekkel fogják ellátni. A program hivatalosan a forgalom csökkentése céljából indul, azonban kritikusai szerint csak egy újabb eszköz az állampolgárok nyomon követéséhez. A gépkocsikba integrált RFID chipeket az út szélére telepített szenzorok olvassák majd le a jármű áthaladásakor, az így keletkezett helyadatok pedig a kínai Közbiztonsági Minisztériumhoz kerülnek továbbításra. Bár a módszer kevésbé pontos a GPS alapú nyomon követésnél, a profilalkotáshoz így is bőséges információval szolgálhat, hiszen általa meghatározhatók az egyének által rendszeresen használt útvonalak. **Bővebben...**

Televíziós vita közben érte kibertámadás az éppen hivatkozott weboldalt

(www.securityweek.com)

2018. június 13-án – mintegy két héttel a mexikói parlamenti választások előtt – a jobboldali National Action Party (PAN) politikai párt weboldalát egy kibertámadás során több órára elérhetetlenné tették. A DDoS támadást egy televíziós vita idejére időzítették, a weboldal pedig éppen azt követően vált elérhetetlenné, mikor az érintett párt képviselője közzétette a site címét, amin egy korrupciós vád bizonyítékait tették elérhetővé. A támadás mögött a korrupcióval vádolt elnökjelöltet, Andres Manuel Lopez Obradort sejtik. A szervert túlterhelő kérések orosz és kínai IP címekről érkeztek, azonban azok valós eredetének felderítése közel lehetetlen. **Bővebben...**

Hiába Trump közbelépése, mégis tilthatják a ZTE-vel történő kereskedelmet

(www.bleepingcomputer.com)

Az USA szenátusa elfogadta a National Defense Authorization Actet (NDAA), amely visszaállítaná a ZTE kínai hardver gyártó elleni kereskedelmi tilalmat. Egy korábbi rendelkezés ugyanis megtiltotta az amerikai vállalatok számára, hogy hardver és szoftver termékeket adjanak el a ZTE-nek, amit azzal indokolt az amerikai Kereskedelmi Minisztérium, hogy a cég a szóban forgó termékekkel olyan harmadik felekkel folytat további kereskedelmi tevékenységet, amelyek ellen amerikai szankciók vannak érvényben, emellett nemzetbiztonsági kockázatot jelent, hogy amerikai vásárlók adatait is megosztják ezekkel a partnerekkel. Mivel a kínai cég a saját előállítású termékeiben nagymértékben hagyatkozik az amerikai Qualcomm chipekre, a tiltás komoly visszaesést hozott a vállalatnak. **Bővebben...**

Újabb kibertámadási kampány során használják az Olympic Destroyert

(www.securityaffairs.co)

Az Olympic Destroyer malware-t ismeretlen támadók 2018. február 11-én, a dél-koreai rendezésű téli olimpiai játékok nyitóceremóniája idején történt kibertámadás során alkalmazták, amivel többek között átmenetileg megszakították a televízió adást a helyszínen lévő sajtóközpontban. A Kaspersky jelzése szerint a malware-t egy új támadássorozat során most ismét bevetették, ezúttal orosz pénzügyi szervezetek, valamint Ukrajnában és más európai országokban található vegyi laboratóriumok ellen. A szakértők szerint egyes e-mailek tökéletes orosz nyelvezete arra enged következtetni, hogy a támadásban orosz nemzetiségű személyek is közreműködnek. **Bővebben...**