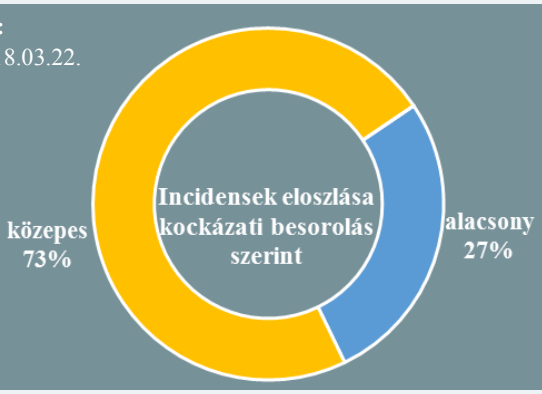
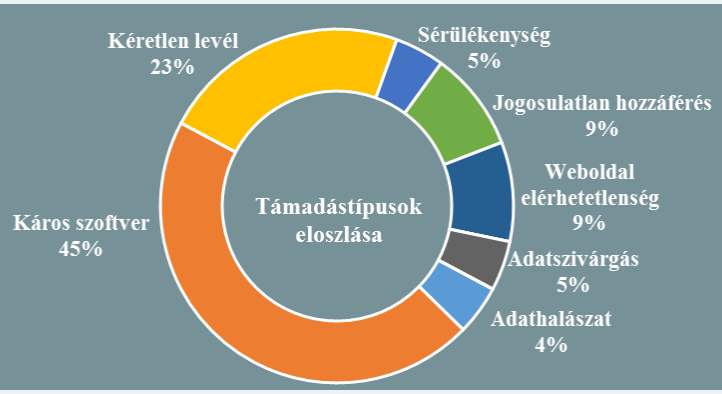
Incidens adatok:
2018.03.16. - 2018.03.22.





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

Egyre valószínűbb, hogy elfogadják a CLOUD törvényt

(www.geekwire.com)

Az Egyesült Államok Kongresszusa múlt hét csütörtökön elfogadta a 2018-as évre vonatkozó, mintegy 2 232 oldalas költségvetési rendeletet (Omnibus Spending Bill). Ez magába foglalja a még februárban bemutatott CLOUD (Clarifying Lawful Overseas Use of Data Act) törvényt is, mely lehetővé tenné a szövetségi hatóságok számára, hogy hozzáférjenek az amerikai állampolgárok külföldi szervereken tárolt adataihoz, ugyanakkor azt is biztosítaná, hogy a külföldi szervektől érkező, hasonló igények kiszolgálása is egyszerűsödjön. A Microsoft elnöke, Brad Smith üdvözölte a CLOUD törvény, a költségvetési rendeletbe való beemelését, amit „kulcsfontosságú előrelépésnek" titulált egy immár négy éve elhúzódó, a tech óriás és az Igazságügyi Minisztérium (DOJ) közötti jogvitával kapcsolatban. **Bővebben...**

A kriptopénz piac közös szabályozásáról is tárgyalnak a G20-ak

(www.bloomberg.com)

A kriptopénzek szabályozására világszerte egyre nagyobb hangsúlyt fektetnek a kormányzatok, ugyanakkor messze nem egységes elképzelések mentén. A legkeményebb intézkedéseket eddig Kína hozta a kriptovaluta kibocsátások (Initial Coin Offering – ICO) és a kriptovaluta váltás betiltásával, emellett támadva azokat a platformokat is, amelyek lehetővé teszik a belső kereskedelmet tengerentúli piacokon keresztül. Japán ehhez képest egy jóval megengedőbb megoldást választott, 16 kereskedési platform engedélyezésével, azonban azóta az ő hozzáállásuk esetében is szigorodás tapasztalható, ugyanis március elején 6 váltó cég is büntetést kapott. Az EU tagállamainak stratégiái között is sok az eltérés, míg Franciaország visszaszorítaná a virtuális fizetőeszközöket, Svájc egyenesen „kripto nemzetté" válna. Az Egyesült Államok még nem hozott átfogó szabályzatot a témában, eddig leginkább a kibocsátásra koncentrált, Oroszország pedig a pénzügyminiszter által januárban benyújtott törvénytervezet alapján a kriptovalutával való fizetést tiltaná, ugyanakkor engedélyezett maradna az ICO-k és a hagyományos valutára való átváltás. A G20-as nemzetek pénzügyminisztereinek, a héten esedékes csúcstalálkozóján a közös fellépés lehetőségét is napirendi pontra tűzik. **Bővebben...**

Kína a közösségi közlekedésben is korlátozhatja állampolgárait

(www.bleepingcomputer.com)

A kínai hatóságok a „közösségi kredit" adatbázis felhasználásával egy évre eltilthatják a repülő- és vonatjegy vásárlástól a szabálysértést elkövető kínai polgárokat. A Nemzeti Fejlesztési és Reformbizottság közleményei szerint mindez 2018. május 1-vel lép életbe és többek között olyan tevékenységeket szankcionálnak majd, mint például a hamis jegyekkel való üzérkedés, a hamis személyi okmányokkal történő jegyváltás, azonban akár a vonaton vagy repülőgépen való dohányzás, vagy a személyzettel szemben tanúsított nem megfelelő magatartás is büntetést vonhat maga után. A közösségi kreditrendszert először 2012-ben jelentették be, akkor még „Szezám kredit" néven, ami végül 2016-ban indult el ténylegesen. A rendszer a kínai polgárok magánéletéről gyűjt adatokat teljességre törekvően, amelyeket – folyamatosan bővülő – szempontok alapján (pl.: vásárlásaik, online aktivitásuk mértéke, közösségi kapcsolataik) elemeznek, ez alapján pedig egy 350 és 950 közötti pontszámot állítanak ki az érintettnek. Az alacsony pontszámmal rendelkező, személyekkel szemben ezután különböző retorziókat alkalmaznak, ugyanis nem csupán az utazási lehetőségektől tilthatják el őket, hanem egyéb téren is hátrányos megkülönböztetésben részesülhetnek. **Bővebben...**

A Siri kiszivárogtathatja a privát üzeneteinket

(www.nakedsecurity.sophos.com)

A brazil MacMagazine egy biztonsági rést fedezett fel az iOS 11-es verziójában, amely lehetővé teszi, hogy egy, a készülékhez hozzáférő személy, jogosulatlanul elérhesse a privát üzeneteket, hiába van a készülék zárolt állapotban. A probléma abból ered, hogy a hangvezérelt asszisztens alkalmazás (Siri) annak ellenére hozzá tud férni az üzenetküldő applikációk (pl.: a WhatsApp és a Skype) által a képernyőn megjelenített értesítésekhez, ha azok esetében a „Show Previews When Unlocked" beállítás az érvényes, azaz az üzenetek előnézete elvben csak feloldott készülék esetében lehetséges. Habár a hiba kihasználása csak bizonyos beállítások mellett lehetséges, a Sophos biztonsági szakemberei arra hívják fel a figyelmet, hogy ezeket széles körben alkalmazzák a felhasználók. Az Apple – amellett, hogy a hiba a saját fejlesztésű üzenetküldő alkalmazásánál (Messages) nem áll fenn – elismerte a biztonsági rés tényét és jelenleg a javításon dolgozik. Addig is javasolt a Siri, valamint az értesítések kikapcsolása. **Bővebben...**

IT biztonsági Tanács

Mobilalkalmazásaink védelme érdekében használhatunk alkalmazás zároló biztonsági applikációkat, melyeknél egy jelszó segítségével könnyen korlátozhatjuk az alkalmazásokhoz történő hozzáféréseket.

Egyes app zárolók esetén az alkalmazások jelszavas védelme mellett, akár bizonyos fájl típusok (pl.: képek, videók) hozzáférésének korlátozására is van lehetőségünk.

A Reddit törölte a darknet-es témájú aloldalát

(www.bleepingcomputer.com)

A Reddit közösségi weboldal letiltotta a legnépszerűbb (a tiltás előtt 180 000 feliratkozóval rendelkező) feketepiaci témájú aloldalát, a DarkNetMarkets-et. Ennek hátterében a tartalom politikában eszközölt szigorítás áll, mely megtiltja az illegális árucikkekkel történő kereskedést az oldalon, mint a lőszerek, robbanóanyagok, kábítószerek (beleértve az alkohol és dohánytermékeket is), szexuális szolgáltatások, lopott személyes adatok, valamint hamis dokumentumok vagy kriptopénzek. A teljes alreddit oldal tiltására azért volt szükség, mert a beszélgetések mellett olyan számban fordultak elő illegális üzletkötések, amiket a moderátorok már nem voltak képesek esetileg kezelni. **Bővebben...**.

Választás előtt a Telegram: együttműködik az FSB-vel vagy elhagyja az orosz piacot

(www.securityaffairs.co)

A Roskomnadzor, az orosz médiafelügyeleti szervezet először 2017 júniusában fenyegette meg betiltással a népszerű csevegő alkalmazást, arra hivatkozva, hogy az nem működik együtt a hatóságokkal és figyelmen kívül hagyja az új adatvédelmi törvényeket. Júliusban a Telegram beleegyezett ugyan, hogy bejegyezteti a céget az országban, azonban a felhasználók adataihoz továbbra sem adott hozzáférést, ehelyett fellebbezést nyújtott be a felszólítás ellen az orosz Legfelső Bírósághoz. A döntés azonban nem a Telegramnak kedvez, így most kötelesek elérhetővé tenni a felhasználók kommunikációjának titkosításához használt privát kulcsokat a Szövetségi Biztonsági Szolgálat (FSB) számára, melyek birtokában az üzenetek visszafejthetők. A Roskomnadzor ehhez 15 napos határidőt adott a cégnek, aminek elmaradása esetén kezdeményezni fogja a Telegram oroszországi szolgáltatásainak korlátozását. Pavel Durov, a Telegram alapítója korábban „technikailag kivitelezhetetlennek", valamint „alkotmányellenesnek" minősítette a felszólítást, majd tavaly szeptemberben elhagyta az országot. **Bővebben...**

Nyugati kritikus rendszerek támadásával vádolják Oroszországot

(www.securityweek.com)

Az Egyesült Államok a múlt hét során szankciókat vezetett be orosz kémügynökségek és több, mint egy tucat személy ellen, a 2016-os amerikai elnökválasztást befolyásoló tevékenységek, valamint kibertámadások – köztük a NotPetya ransomware kampány – indításának vádjával. Nem sokkal ezt követően az US-CERT frissítette az amerikai Belbiztonsági Minisztérium (DHS) és az FBI által kiadott korábbi figyelmeztetését, mely hivatalosan az orosz kormányzatot teszi felelőssé a 'Dragonfly' csoport (más néven Crouching Yeti/EnergeticBear) kritikus infrastruktúrák ellen intézett informatikai támadásaiért. A brit nemzeti kiberközpont (NCSC) a tavalyi év során szintén adott ki figyelmeztetést, miszerint ismeretlen hackerek energia szektorbeli dolgozók jelszavait próbálták megszerezni adathalász támadások útján. Az amerikai Cylance biztonsági cég által végzett vizsgálat ezzel kapcsolatban feltárta, hogy ezek a brit kritikus rendszerek elleni támadások mögött is a Dragonfly csoport állhat. **Bővebben...**