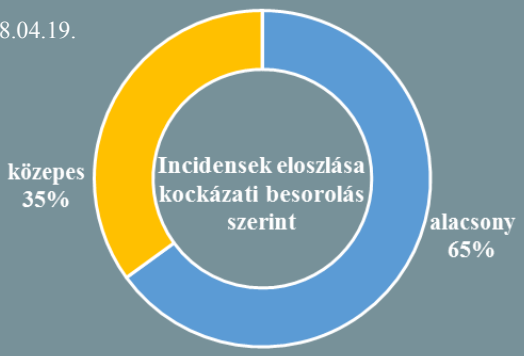
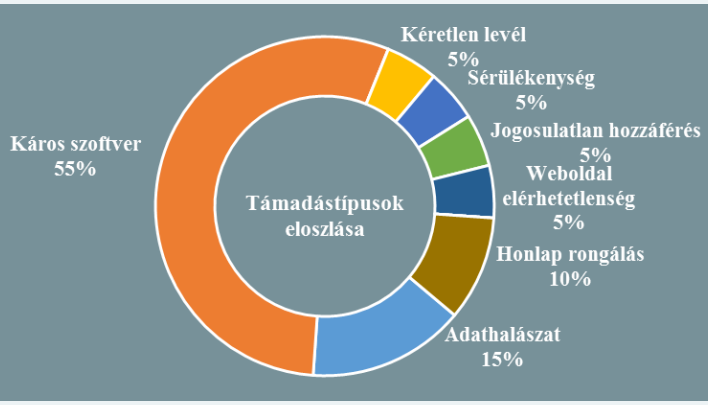
Nemzetközi IT-biztonsági sajtószemle

Incidens adatok:
2018.04.13. - 2018.04.19.





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

A Telegram miatt legitim oldalakat is kitiltottak Oroszországban

(www.bleepingcomputer.com)

A Roskomnadzor mintegy 1.8 millió, az Amazon, illetve a Google felhő infrastruktúráihoz tartozó IP címet tiltatott ki az orosz internetszolgáltatóknál. Mindezt azért, mert a Telegram csevegő szolgáltatása – a jogerős tiltás ellenére – továbbra is elérhető maradt, azt a cég ugyanis a tech óriások felhőparkjaiba „menekítette". Sok felhasználó a közösségi oldalakon fejezte ki felháborodását a médiafelügyeleti szerv döntésével szemben, mivel a tömeges IP tiltásnak köszönhetően több legitim webes szolgáltatás (játékok, mobil applikációk, kriptovaluta alkalmazások, stb.) elérése is megszűnt. **Bővebben...**

Pusztító kibertámadástól tart az Egyesült Királyság – szakértők szerint teljes joggal

(www.mirror.co.uk)

Elemzők szerint Oroszország előreláthatólag kibertámadást indít az Egyesült Királyság ellen, válaszul a múlt heti szíriai bombázásra. Bár az orosz elnök korábban egy rakéta válaszcsapást irányozott elő az amerikai haderő ellen, szakértők szerint egy informatikai támadás sokkal valószínűbb. Egy ilyen online támadást vélhetően nagy volumenű online propaganda egészíthet ki, emellett számítanak a szigetországban végzett orosz hírszerzési tevékenység élénkülésére is. Mindezt a napokban Ciaran Martin, az NCSC vezetője is megerősítette, aki szerint egy kibertámadás lehetősége még soha nem volt ennél valóságosabb. Michael Clark, a RUSI (Royal United Services Institute) védelmi tanácsadó szervezet volt vezérigazgatója az elkövetkezendő 2-3 hetet tartja a legvalószínűbbnek a támadásra, amiről úgy véli, hogy „a teljes társadalomra hatással lehet". A potenciális célpontok között említette az egészségügyi ellátórendszert, a szállítási szektort, vagy a légi közlekedésirányító rendszereket, mások az energia és a pénzügyi szektort tartják a leginkább veszélyeztetettnek. **Bővebben...**

Harmadik fél szivárogtatott ki közösségi oldalakról származó privát információkat

(www.zdnet.com)

A Localblox nevű, profilalkotással foglalkozó amerikai cég mintegy 48 millió, weboldalakról és különböző közösségi platformokról (többek között Facebook, LinkedIn, Twitter) származó személyes adatot szivárogtatott ki – adja hírül a ZDNet. A bárki számára hozzáférhető Amazon tárhelyen „felejtett" 1.2 terabyte méretű fájlra a jól ismert biztonsági szakember – és az UpGuard vezetője – Chris Vickery talált rá, aki szerint az adatok jelszóval sem voltak védve. A felfedezés után azonnal felvette a kapcsolatot a céggel, akik néhány órával később már elérhetetlenné is tették az állományt. Az eset komoly adatvédelmi aggályokat vet fel, mivel a Localblox által épített adatbázis olyan érzékeny, személyazonosításra is alkalmas információkat tartalmaz, mint például nevek, postai címek, munkahelyi és családi információk, melyeket a cég a felhasználók tudta és hozzájárulása nélkül gyűjt. Az UpGuard által az incidensről készített jelentésben Vickery úgy fogalmaz, hogy azok „háromdimenziós képet" festenek minden érintett személyről, amelyek kapcsán az a gyanú is felmerült, hogy az adatok nem csupán publikus forrásból származhattak. **Bővebben...**

Új szolgáltatással bővül a Google Play Protect

(www.blog.chromium.org)

A Chrome biztonságos böngészés funkciója 2007 óta érhető el, ami egy figyelmeztető üzenetet jelenít meg még azelőtt, hogy a felhasználó egy feltételezhetően rosszindulatú vagy adathalász weboldalt keresne fel. A cég a hét folyamán jelentette be, hogy 2018 áprilisától – a WebView 66 megjelenésével – a Google Play Protect alapértelmezetten lehetővé teszi a biztonságos böngészés használatát. A funkció az Android 8.0 és annál magasabb verziókon érhető el, ugyanazt a technológiát és piros hátterű üzenetet alkalmazva, mint az Android Chrome esetén. A WebView-t használó Android alkalmazásfejlesztőknek nem szükséges változásokat eszközölniük a funkció aktiváláshoz, ugyanakkor a 27. API szinten már lehetőség van a személyre szabott működtetésre is. **Bővebben...**

IT biztonsági Tanács

Online vásárlás előtt mindig informálódjunk az adott webshopról az interneten.

- A boltra vonatkozó sok negatív vásárlói vélemény általában jelzi, ha egy cég nem megbízható.
- Adataink biztonsága miatt fontos, hogy az oldal SSL tanúsítvánnyal rendelkezzen, figyeljünk a https meglétére a webhely címében.
- Ellenőrizzük, hogy az adott cég rendelkezik-e Általános Szerződési Feltételekkel (ÁSZF), ha ez nem érhető el, inkább álljunk el a vásárlási szándéktól.

Az amerikai CLOUD törvény európai változata

(www. engadget.com)

Az Egyesült Államokban nemrégiben elfogadott CLOUD törvény lehetővé teszi a szövetségi hatóságok számára, hogy egy bírói határozat birtokában hozzáférhessenek az amerikai állampolgárok tengeren túli szervereken tárolt adataihoz is. Ennek kapcsán most az Európai Bizottság tett javaslatot a CLOUD törvény uniós változatának létrehozására, aminek alkalmazásával gyorsíthatják az adatokhoz való hozzáférést. Az EU-s törvényjavaslat értelmében az online szolgáltatóknak 10 napon belül – vészhelyzet esetén 6 órán belül – kell válaszolniuk a hatóságok megkeresésére, mely a meglévő európai nyomozási határozatban szereplő 120 napos határidőnél lényegesen gyorsabb eljárási folyamatot eredményezhet. **Bővebben...**

Megszülethetett a „Digitális Genfi Egyezmény”

(www.securitynewspaper.com)

A Microsoft kezdeményezésére mintegy 34 prominens tech vállalat írt alá egy nyilatkozatot, melynek értelmében mindenek felett kiállnak a felhasználók kiberbűnözők, valamint állami támogatású hacker csoportokkal szembeni védelme mellett. A „Cybersecurity Tech Accord”-ot aláírók között neves hardver (pl.: HP, Dell, Cisco, Juniper), valamint szoftver gyártók (pl.: Oracle, SAP) is megtalálhatók, csakúgy, mint biztonsági cégek (pl.: Symantec, F-secure) valamint olyan platformok is, mint a GitHub, a Facebook vagy a LinkedIn. Brad Smith, a Microsoft vezető jogásza már közel két éve küzd azért, hogy a kormányzatok a magánszektort ne tekintsék hadszíntérnek a nemzetek ellen indított kiber műveleteik során. Az áttörést végül a 2017 során milliárdos károkat okozó WannaCry támadás jelenthette, ami után több szakember is kiállt az ügy mellett. **Bővebben...**

A Facebook a következő a Roskomnadzor listáján

(www.securityweek.com)

Az orosz médiafelügyeleti hatóság még az év vége előtt vizsgálatot indít a közösségi oldal ellen – nyilatkozta Alexander Zharov, a Roskomnadzor vezetője az Izvestiának. A cég már több figyelmeztetést is kapott, miszerint ha nem tesz eleget az orosz nemzetiségű személyek adatainak kezelésére vonatkozó hatályos jogszabályoknak, úgy – a Telegramhoz hasonlóan – blokkolni fogják az oldal Oroszországból való elérését. A hivatkozott 2014-es törvény a külföldi csevegő szolgáltatást nyújtó vállalatok számára előírja, hogy az orosz állampolgárok adatai kizárólag az ország határain belül tárolhatók. A jogszabály kritikusai szerint azonban félő, hogy a felhasználók adatai ily módon az orosz hírszerzés számára könnyen hozzáférhetővé válnának. **Bővebben...**

Németország aggódik a kínai felvásárlások miatt

(www.reuters.com)

Hans-Georg Maassen, a német elhárítás (BfV) vezetője szerint aggasztó, hogy Kína igyekszik egyre több német technológiai vállalkozásban érdekeltséget szerezni. Maassen szerint Németország nyitott a külföldi befektetésekkel szemben – beleértve Kínát is –, azonban a kulcsfontosságú technológiák védelmében intézkedéseket kell hozni, ugyanis ezek elvesztése az ország gazdaságára negatív hatással lesz. Biztonsági szempontból különösen kockázatosnak ítélte például az ipari robotok gyártásával foglalkozó KUKA vállalat 2016-os kínai felvásárlását, de ilyen, széles körben vitákat kiváltó esemény volt az is, amikor a múlt hónapban a Sate Grid Corporation of China megpróbált 20%-os részesedést szerezni az 50Hertz villamosenergia-szolgáltató vállalatban. **Bővebben...**