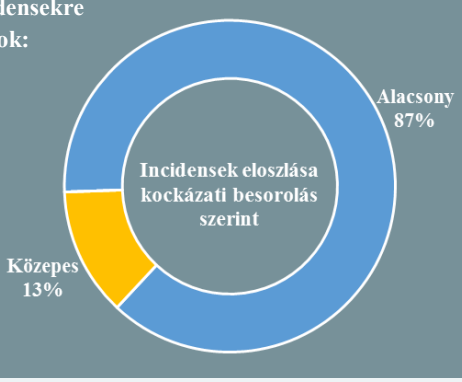
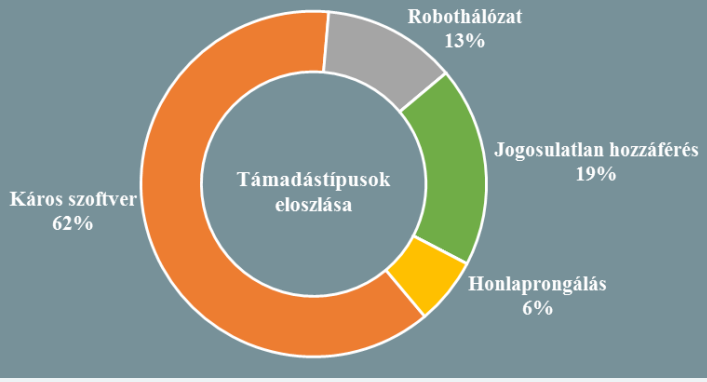
Nemzetközi IT-biztonsági sajtószemle

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.06.08. - 2018.06.14.





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

Az internetes kereséseket is cenzúrázza Oroszország

(www.securityaffairs.com)

Egy új törvényjavaslat szerint pénzbírságra számíthatnak azok az internetes keresők, akik a keresési találatok között megjelenítik a feketelistán szereplő domaineket, valamint a VPN szolgáltatásokat és egyéb olyan eszközöket, amelyekkel hozzáférhetők a tiltólistán szereplő tartalmak. Az orosz parlament 2017-ben szavazta meg az illegálisnak minősített webhelyek elérését lehetővé tévő VPN szolgáltatások betiltását. A Duma akkor azt is elfogadta, hogy az online csevegő szolgáltatásokat csak telefonszám regisztrálásával lehessen igénybe venni, mostantól pedig a VPN és proxy szolgáltatóknak is regisztrálni kell magukat a hatóságoknál. **Bővebben...**

Komoly aggodalmak kísérik az Egyesült Államok új kormányzati biometrikus azonosító rendszerét

(www.nakedsecurity.sophos.com)

A magánszféra védelmében fellépő szervezetek figyelmét egyre jobban felkelti az amerikai Belbiztonsági Minisztérium 2017-ben bejelentett Homeland Advanced Recognition (HART) programja, ami a biometrikus azonosítók tárolására szolgáló Automated Biometric Identification System (IDENT) egy kibővített verziójaként értelmezhető. A HART bővített képességei egyrészt a rendszer kapacitásában mutatkoznak meg, ugyanis ez már több, mint 500 millió azonosító tárolására lesz alkalmas. Másrészt jóval több féle biometrikus adatot lesz képes gyűjteni, például írisz mintákat, tenyér lenyomatokat, hangmintákat és DNS-t is, amit kiegészítenek majd az alanyok közigazgatási adatai, (név, cím, gépjármű azonosító, stb.) illetve a közösségi hálózatok alapján a személy kapcsolatira vonatkozó információk. **Bővebben...**

Kiderült mennyi adatot loptak el kínai hackerek az amerikai haditengerészettől

(www.csoonline.com)

Az Egyesült Államok Haditengerészetét (USN) 2018 január-február között érte az incidens, amelynek hátterében kínai állami hackereket sejtenek. A The Washington Post információi szerint ennek során mintegy 614 GB-nyi érzékeny adatot tulajdonítottak el, köztük egy szuperszonikus hadihajó elhárító rakétarendszerről készült minősített anyagokkal, amit az amerikaiak 2020-ra terveztek hadrendbe állítani. Ugyan nem nevezik néven, annyi azonban ismert, hogy a támadás célpontja egy, a haditengerészet víz alatti fegyverrendszerek fejlesztésével foglalkozó Rhode Island-i kutatóközpontjának szerződéses partnere volt. **Bővebben...**

Egyes termékeivel kapcsolatban nem nyújt több segítséget a Microsoft

(www.bleepingcomputer.com)

A Microsoft 2018. július 1-től nem reagál majd a Windows 7, 8.1, 8.1 RT és néhány régebbi alkalmazásával kapcsolatban feltett kérdésekre a Microsoft közösségi fórumon (Microsoft Community), a cég közleményében azonban jelezte, hogy a felhasználók ettől függetlenül megválaszolhatják egymás kérdéseit. A topikok közül lesz olyan, ami teljesen megszüntetésre kerül majd, néhányat pedig zárolnak, azonban továbbra is böngészhetőek maradnak. **Bővebben...**

Mégis lesz USB port korlátozás az iOS-ben

(www.reuters.com)

A Reuters információi szerint az Apple változtatásokat vezet be az iOS új kiadásában, hogy hatástalanítsák azt a legutóbbi módszert, amellyel jelenleg az Apple készülékeihez hozzáférést biztosító — a bűnüldöző hatóságok között egyre népszerűbb — eszközök működnek. Az iOS-ben tervezett módosítás meg fogja szüntetni az USB porton keresztül történő kommunikációt, amennyiben a telefont 1 órája nem oldották fel. Ismert ugyanis, hogy a vezető forensic vállalatok – mint a GrayShift és a Cellebrite – eszközei ezen keresztül csatlakoznak, hogy megkerüljék a jelszó próbálgatás limitálását. Kutatók szerint azzal, hogy az érdekelt félnek maximum 1 órája lesz arra, hogy megkezdje a telefon feltörését, a hozzáférések körülbelül 90%-át meg fogják tudni akadályozni. **Bővebben...**

IT biztonsági Tanács

A nyári szabadságok idején legyünk különösen óvatosak az online szállás- és repülőjegy foglalások során, ugyanis ebben az időszakban jellemzően megnövekszik a csaló oldalak száma.

- Az e-mailben érkező ajánlatok esetén ne a levélben szereplő linkre kattintva nyissuk meg az adott foglalási oldalt, hanem külön keressünk rá.
- Amennyiben úgy dönt, hogy a foglalást egy harmadik fél weboldalán keresztül végzi, válasszon egy jól ismert és elismert céget.
- Mindenképp kérjünk telefonon megerősítést a foglalások leadása után.

Több céget is orosz titkosszolgálati kapcsolatokkal vádol az amerikai kormányzat

(www.cyberscoop.com)

Az Egyesült Államok szankciókat léptetett életbe öt szervezet és három magánszemély ellen az 13694-es elnöki rendelet erejénél fogva, ami még az Obama adminisztráció idején került elfogadásra, és olyan entitásokkal szemben alkalmazható, amelyek „jelentős káros kiber-tevékenységben vesznek részt”. Az érintett cégek és személyek a vádak szerint összefüggésbe hozhatók az orosz titkosszolgálattal (Szövetségi Biztonsági Szolgálat – FSB), és informatikai támadásokban működtek közre. A tiltás elsődleges célpontja a kiberbiztonsággal foglalkozó Digital Security vállalat, emellett annak állítólagos leányvállalatai, a sérülékenységvizsgálati profilú ERPScan és az Embedi. **Bővebben...**

A Google megelégelte, hogy sok a káros tartalmú Chrome bővítmény

(www.bleepingcomputer.com)

A Google úgy döntött, hogy fokozatosan kivezeti a Chrome bővítmények ún. inline – azaz távoli webhelyekről történő – telepítési lehetőségét, ami mellett a cég a harmadik felektől származó rosszindulatú bővítmények megszaporodott száma miatt döntött. Az elképzelések szerint 2018. végére a felhasználók kizárólag a Chrome hivatalos webáruházából tudnak majd bővítményeket telepíteni. **Bővebben...**

Nagyon valószínű, hogy mesterségesen befolyásolták a Bitcoin árfolyamát

(www.nytimes.com)

Egy, a Texasi Egyetem pénzügyi professzora és tanítványa által publikált tanulmány szerint koncentrált ármanipuláció a felelős a Bitcoin, valamint további kriptovaluták tavaly tapasztalt meredek árfolyam-emelkedésének legalább feléért – írja a The New York Times. Griffinék behatóan tanulmányozták a Bitfinex kriptovaluta-váltó tevékenységét, amelynek tisztaságával kapcsolatban iparági szereplők részéről már korábban is merültek fel kétségek. A vizsgálatok alapján olyan mintázatokat fedeztek fel, amelyek arra engednek következtetni, hogy a váltónál dolgozó ismeretlen személyek manipulálták az árat, amihez a Tether nevű virtuális valutát használták fel, amelynek kibocsátója maga a Bitfinex volt. **Bővebben...**

A Kaspersky átmenetileg felfüggeszti együttműködését az Europollal

(www.bleepingcomputer.com)

A Kaspersky Lab jelezte, hogy egy, az Európai Parlament 2018. június 13-ai plenáris ülésén elfogadott dokumentummal szembeni tiltakozásul bizonytalan időre megszakítják az Európai Rendőrségi Hivatallal történő kooperációt, és abban a NoMoreRansom projektben történő további részvételt, amelynek megalapításában is részt vettek. A szóban forgó tanácsadói dokumentumban ugyanis – amely átfogó felülvizsgálatot javasol az uniós intézmények teljes számítógépes infrastruktúráik vonatkozásában – káros szoftverekre hozott példaként név szerint említik a Kaspersky Lab-ot. A tény, hogy egy Európai Uniós hivatalos okiratban köztudomásúlag rosszindulatúként hivatkoznak a cégre, annak ellenére komoly presztízsveszteséget jelent az orosz vállalatnak, hogy a dokumentum önmagában nem bír kötelező erővel. **Bővebben...**