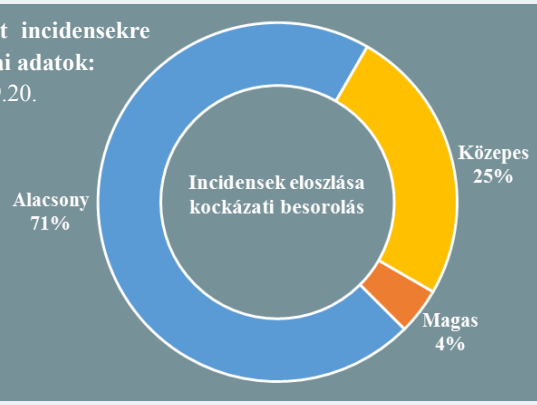
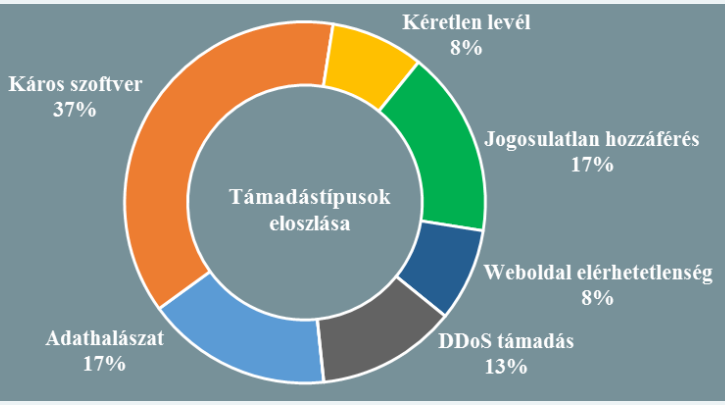
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.09.14. - 2018.09.20.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!

Elérhető a szervezett kiberbűnözésről szóló legfrissebb Europol jelentés

(www.europol.europa.eu)

Az Europol közreadta az internetes szervezett bűnözés 2017-ben tapasztalt jellegzetességeit összefoglaló IOCTA-jelentést (Internet Organised Crime Threat Assessment 2018). A tanulmány a káros kódokkal kapcsolatban megállapítja, hogy mára a zsarolóvírusok egy alapvető támadási formává váltak, amit a bűnözők egyre célzottabban használnak mind cégek, mind magánszemélyek ellen. Az elmúlt évben nőtt a mobil kártevők száma is, ahogy az online bankolás már inkább mobil platformon történik, a kártékony kódokat kínáló illegális piacokon pedig a fájlnélküli malware-ek már stabilan a portfólió részét képezik. **Bővebben...**

4.8 Gbps sávszélességű Wi-Fi hálózatot indít a dél-koreai SK Telecom

(www.zdnet.com)

A T Wi-Fi AX névre keresztelt hálózat már az új 802.11.ax szabvány alapján készült, ami közel négyszer akkora sávszélességet tesz lehetővé, mint a 2013-as 802.11ac Wave 1. Ugyanakkor a jelenleg kereskedelmi forgalomban kapható okostelefonok még nem rendelkeznek a szabványnak megfelelő chippel, így csak az 1 Gbps sebességet érhetik el, az első kompatibilis készülékek megjelenése legkorábban jövőre várható. A vállalat emellett bejelentette az 5G-s mobil hálózat kiépítéséhez preferált partnereket, amelyek a Samsung, az Ericson, és a Nokia lettek, a várakozásokkal ellentétben a Huawei végül kimaradt. **Bővebben...**

Bitkom: 43 milliárd eurós kár adatlopás, kémkedés és szabotázs révén

(www.heise.de)

A német vállalkozások az elmúlt két évben 43 milliárd eurós kárt szenvedtek el adatkémkedés miatt a Bitkom és a német alkotmányvédelmi hivatal (BfV) közös jelentése szerint, amely rámutatott, hogy különösen a kis- és középvállalkozások voltak a támadások áldozatai. Az elkövetői körben kimagasló arányt képviselnek az egykori, illetve éppen aktuális munkavállalók, ezen kívül például az adott cég vásárlói, beszállítói, valamint a hobbihekkerek; az említettek még a szervezet bűnözői köröknél is több kárt okoztak. A jelentés egyik fő következtetése, hogy a munkavállalók oktatása a legjobb védekezés az adatkémkedés- és szabotázs ellen. **Bővebben...**

Az egyre erőteljesebb felügyeleti kontroll paradox módon erősítheti a polgári szabadságjogokat Kínában

(www.heise.de)

A 2020-tól Kínában bevezetésre kerülő „társadalmi kreditrendszer” minősíteni fogja az egyes állampolgárokat megbízhatóságuk ─ azaz a rendszer által támasztott életmódbeli elvárásoknak való megfelelésük ─ alapján. Ezen értékelés minden rendelkezésre álló adatot figyelembe fog venni: a vásárlási szokásoktól kezdve egészen a baráti kör összetételéig. A metodika ideális eszköznek tűnik az állam számára, hogy a lakosságot ellenőrizhesse, mindazonáltal Yasheng Huang, az MIT Sloan School of Management professzora szerint ezáltal a kínai rezsim kevésbé maradhat elnyomó jellegű. Úgy véli, hogy az adatok egyre nagyobb mennyisége és a technikai fejlődés jóval nagyobb mértékben erősítette a magánszféra tudatosságát, mint bármely más gazdasági, társadalmi változás. Ennek oka abban keresendő, hogy az informatika fejlődésével az emberek előtt kinyíltak a lehetőségek a szélesebb körű kommunikációs kapcsolatok vonatkozásában, áttörve a konfuciánus kultúra intimitását, személyes zártságát. **Bővebben...**

Egy új támadás az iOS újraindulását és a macOS lefagyását eredményezheti

(www.bleepingcomputer.com)

A problémát a Wire egy biztonsági kutatója fedezte fel, aki szerint az a grafikus elemek megjelenítéséért felelős WebKit renderelő motor sérülékenységéből fakad. Mindez olyan speciálisan szerkesztett weboldalakkal használható ki, amelyek megadott CSS és HTML kódokat tartalmaznak, a felhasználónak elég betölteni egy ilyen weboldalt, hogy a rendszer összeomoljon. Minden iOS-en futó böngésző érintett ─ mivel az App Store szabályzata alapján az alkalmazás fejlesztők nem használhatnak más renderelő motort ─ macOSen pedig a Safari és a Mail. A hibát felfedező szakember szerint nincs megkerülő megoldás a problémára, így csak a gyártói javítás szüntetheti meg azt. **Bővebben...**

IT biztonsági Tanács

A Google és a Facebook példáját követve a Twitter is bevezetett egy új biztonsági funkciót; ezután a felhasználók megtekinthetik, hogy a fiókjukhoz milyen harmadik féltől származó applikációk férnek hozzá, és milyen eszközökről, történt bejelentkezés valamint, hogy azt honnan és mikor hajtották végre.

A gyanús applikációktól megvonhatjuk a jogosultságot, az ismeretlen eszközöket pedig azonnal kijelentkeztethetjük. Az aktuális bejelentkezések mellett 1 hónapra visszamenőleges adatok is hozzáférhetőek.

A funkció a Settings and privacy / Account / Apps and Sessions alatt érhető el.

Az ENISA támogatja a nemzeti kiberbiztonsági stratégiák fejlesztését

(www.enisa.europa.eu)

Az Európai Hálózat- és Információbiztonsági Ügynökség az EU-s tagállamok részére egy önértékelést segítő webes eszközt ad közre, ami a nemzeti kiberbiztonsági stratégiák kialakítását felügyelő hatóságokat kívánja támogatni azáltal, hogy a célkitűzések számbavétele mellett ajánlásokat és ötleteket is nyújt ezek eléréséhez egy gyors és könnyen kezelhető felületen. A segédlet a NIS irányelv követelményeinek megfelelően került kialakításra és a tervek szerint a jövőben újabb kérdéskörökkel fog bővülni. Az ügynökség emellett frissítette azt az interaktív online térképet is, amelyen a tagállamok felkészültségi állapotát lehet figyelemmel kísérni. **Bővebben...**

Zsarolóvírus támadás érte a bristoli repülőteret

(securityaffairs.co)

Mintegy két napig üzemen kívül voltak az utasinformációs digitális táblák a Bristoli Nemzetközi Repülőtéren (IATA:BRS) egy ransomware vírus támadás miatt, szerencsére a járatokat nem érintette az incidens. A cég szóvivője szerint a támadás egyes adminisztratív rendszereiket célozta, a fertőzés továbbterjedésének megakadályozása miatt pedig átmenetileg több rendszert is le kellett állítaniuk, például a járatinformációkat mutató kijelzőket, amelyek azóta a kulcsfontosságú helyeken már ismét működnek. **Bővebben...**

Megjelent a Pentagon új kiberstratégiája

(www.securityweek.com)

Az amerikai Védelmi Minisztérium elsősorban Kínát és Oroszországot tekinti az USA vetélytársának a kibertérben, azonban megemlíti Észak-Koreát és Iránt is. A Department of Defense Cyber Strategy 2018 többek között hírszerzési célú kiberműveleteket irányoz elő, valamint nagy ütemű kiber képességfejlesztést a hagyományos haderőnemek támogatásához krízishelyzetek és katonai konfliktusok során, emellett fontos célként jelenik meg a támadások elhárítása is. **Bővebben...**

Elképzelhető, hogy Amazon dolgozók felhasználói adatokkal kereskedtek

(www.afp.com)

Az Amazon elismerte, hogy vizsgálatot folytat azon vádak tisztázására, miszerint személyzetének egyes tagjai felhasználói adatokat és bizalmas információkat adtak el harmadik feleknek, köztük kínai cégeknek ─ adja hírül az AFP hírügynökség. A vállalat közleményében határozottan elítéli a visszaélést, és az elkövetők számára szigorú intézkedéseket ─ köztük jogi lépéseket ─ helyez kilátásba. A témáról először tudósító The Wall Street Journal szerint a belső vizsgálat kétes hitelű negatív felhasználói vélemények miatt indult, és már hónapok óta zajlik. **Bővebben...**

Hibrid háború a Balti térségben

(www.securityweek.com)

Németország katonai célú kiberképesség-fejlesztést végez a katonáit érő hibrid háborús támadások kezeléséhez ─ nyilatkozta Angela Merkel pénteken egy litván katonai bázison tett látogatása során. A német kancellár szerint folyamatos támadás éri a volt szovjet NATO tagországokba vezényelt német erőket Oroszország részéről, amit Németország nem kíván figyelmen kívül hagyni. **Bővebben...**