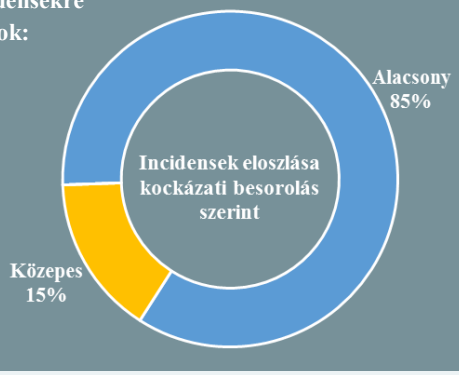
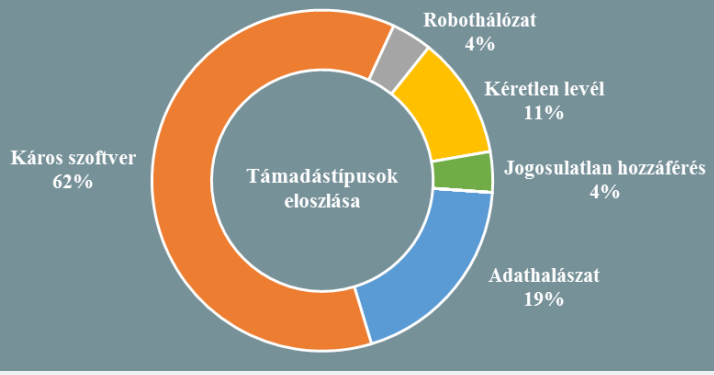
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.06.01. - 2018.06.07.





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

Mi változott a Snowden-ügy kirobbanása óta?

(www.theguardian.com)

Öt év telt el azóta, hogy Edward Snowden minősített dokumentumokat szivárogtatott ki az NSA-től, hogy felhívja a figyelmet az amerikai titkosszolgálatok és tech vállalatok törvénytelen adatgyűjtési eljárására. Az évforduló alkalmából a The Guardian telefonos interjút készített Snowdennel, melynek során érintették az elmúlt öt év főbb változásait. Kiemelendő, hogy 2015-ben az Egyesült Államok Kongresszusa elfogadta a Freedom Act nevű törvényt, amely megfékezte a telefonhívások adatainak tömeges gyűjtését. Az Egyesült Királyság parlamentje azonban egy évvel később jóváhagyta a nyomozati hatáskörök szabályozásáról szóló, számos vitát kiváltó törvényét. **Bővebben...**

Szigorúbb intézkedéseket javasol az amerikai külügy kibertámadások esetén

(www.cyberscoop.com)

Az amerikai külügyminisztérium kibővítené a Trump adminisztráció „kiber elrettentési stratégiája” által javasolt intézkedések körét. Az ajánlások egy publikus verziója szerint az USA kormányának a szövetségesek közreműködésével „gyors, költséges és átlátható következményeket” kell okoznia azon külföldi államoknak, akik „jelentős mértékű” káros internetes tevékenységet folytatnak az Egyesült Államok ellen. Az alkalmazható elrettentő eszközök nem kerültek részletesen felsorolásra, de egyes tisztségviselők szerint különböző szankciók, jogi lépések, nyilvánosan is felvállalt, valamint rejtett támadások mind elképzelhetőek, ehhez azonban elvárás az adott tevékenység nyilvános megjelölése. Javasolják azt is, hogy dedikált intézkedési tervek készüljenek minden egyes szembenálló állam részére**. Bővebben...**

Újabban kikerüli Amerikát az egyik legveszélyesebb észak-koreai hacker csoport

(www.securityweek.com)

A „Covellite”-ként hivatkozott csoport eddigi fő célpontjai európai és észak-amerikai civil energetikai vállalkozások voltak, utóbbiak ellen legutóbb 2017 szeptemberében folytattak kiterjedt támadásokat. A Dragos most publikált elemzésében arról számol be, hogy a csoport fókuszából az utóbbi időben kikerült az Egyesült Államok, azonban Európa és Kelet Ázsia ellen továbbra is folytatják a kiberműveleteket. A támadások hátterével kapcsolatban az elemzés ugyan direkt módon nem említi Észak-Koreát, azonban a felhasznált malware variánsok és az infrastruktúra tekintetében egyezéseket találtak a rezsimhez köthető két másik csoporttal („Lazarus”, és „Hidden Cobra”). **Bővebben...**

A német hírszerzés legálisan hozzáférhet a belföldi hálózati forgalomhoz is

(www.securityweek.com)

2018. 05. 30-án ítéletet hoztak a világ legnagyobb internetes forgalom kicserélési központjának üzemeltetője (a német DE-CIX) által benyújtott kereset kapcsán. A cég álláspontja szerint ugyanis jogellenes, hogy a BND a nemzetközi mellett a teljes belföldi hálózati forgalomhoz is hozzáfér. A Szövetségi Közigazgatási Bíróság azonban most úgy határozott, hogy az internetes csomópontok üzemeltetői kötelezettek a BND által végzett stratégiai célú megfigyelésben való közreműködésre. **Bővebben...**

Fordulat az Apple-Telegram ügyben?

(www.reuters.com)

Az Apple váratlanul elérhetővé tette a Telegram frissített verzióját, egy nappal azt követően, hogy Pavel Durov, a Telegram vezetője közölte, a tech óriás – vélhetően az orosz hatóságok nyomására – április óta visszatartja a chat alkalmazás javítását. Ennek hiányában azonban több funkció sem működik megfelelően a legutóbbi iOS verión (11.4), és ez az új európai adatvédelmi rendeletnek való megfelelést is hátráltatja. Az esettel kapcsolatban az Apple nem közölt információkat, Durov egy Twitter postban köszönte meg a frissítést. **Bővebben...**

IT biztonsági Tanács

Az ún. „fájl nélküli” rosszindulatú programokat az antivírus szoftverek nehezen tudják felismerni, mivel a támadás nem jár fájlletöltéssel. A káros kód jellemzően a PowerShell segítségével töltődik a memóriába, és azután igyekszik – valamilyen sérülékenységet kihasználva – legitim folyamatokat kompromittálni. Védekező intézkedésként javasolt, hogy:

- Tartson naprakészen minden használt szoftvert.
- Használja a PowerShell 5-ös verzióját és távolítsa el a 2-est.
- Aktiválja a PowerShell 5-ben a logolást.
- Tiltsa le a nem használt komponenseket a Windows framework-ben.
- Alkalmazza a legkissebb jogosultság elvét.

A VPNFilter jóval több eszközt fenyeget, mint amiről a kezdeti hírek szóltak

(www.cyberscoop.com)

A korábban már több, mint 500 000 hálózati eszköz fertőzését okozó VPNFilter malware-ről most új információkat közölt a Cisco Talos csapata. Eszerint egyrészt további gyártók termékei is veszélyeztetettek, így a Linksys, a MikroTik, a Netgear, a TP-Link, és a QNAP mellett már az ASUS, a D-Link, a Huawei, az Ubiquiti, az UPVEL és a ZTE egyes modelljei is. Ezzel a kezdeti 16 helyett összesen már 71-nél tart az érintett típusok száma. Másrészt a károkozó újabb tulajdonságai váltak ismertté, például közbeékelődve a webes forgalomba, képes lehallgatni és módosítani a webes forgalmat. **Bővebben...**

Megállapodás született az új EU-s távközlési szabályokról

(www.europa.eu)

Az Európai Parlament és az Európai Tanács a héten megállapodott az Európai Uniós telekommunikációs szabályok módosításáról. Az új Európai Elektronikus Hírközlési Kódex a tervek szerint ösztönözni fogja a nagyteljesítményű hálózatok tekintetében történő beruházásokat az EU peremterületein is. Fokozni kívánják az 5G hálózatok kiépítését, aminek célja, hogy az 5G-s rádiós-pectrum legkésőbb 2020 végére egységesen elérhető legyen az EU-ban. A szolgáltatóknak – többek között – javítaniuk kell majd a tarifacsomagok átláthatóságán, valamint sürgősségi vészhelyzet esetén pontosabb helymeghatározást kell biztosítaniuk. **Bővebben...**

Tervben az újgenerációs PGP

(www.cyberscoop.com)

Phil Zimmerman, az 1991-óta létező PGP (Pretty Good Privacy) atyja csatlakozott a StartPage.com vállalathoz, ahol a cég közleménye szerint fő feladata az e-mailes kommunikáció titkosítására szolgáló PGP eljárás egy új verziójának megalkotása lesz. Zimmerman nyilatkozatában elmondta, ő maga már évek óta nem használja a PGP-t, mivel elmondása szerint folyamatosan kompatibilitási problémákba ütközött az általa használt MacOS aktuális verzióival. A StartPage -hez azért csatlakozott, mert úgy látja, a cég elkötelezett a biztonság irányában. **Bővebben...**

Tömegesen kémkednek amerikai állampolgárok után a mobil hálózatokon keresztül

(www.cyberscoop.com)

Az amerikai Belbiztonsági Minisztérium (DHS) egy jelentése szerint a mobil kommunikációban használt SS7 protokoll régóta ismert sérülékenységét rosszindulatú szereplők aktívan kihasználják, hogy bármiféle jogi felhatalmazás nélkül amerikai állampolgárok után kémkedjenek. Az információ Chris Krebstől, a DHS egy magas rangú tisztségviselőjétől származik, aki minderről egy május 22-ei levélben tájékoztatta Ron Wyden amerikai szenátort. **Bővebben...**

A Google kihátrál egy katonai szerződésből

(www.techcrunch.com)

A Google vezetése úgy döntött, hogy – engedve a külső és belső nyomásnak – nem hosszabbítja meg az amerikai Védelmi Minisztériummal kötött, 2019-ben lejáró szerződését. A Project Maven névre keresztelt program során a tech cég például drónok által készített harctéri felvételek mesterséges intelligenciával történő elemzésében nyújtott segítséget a hadseregnek. **Bővebben...**