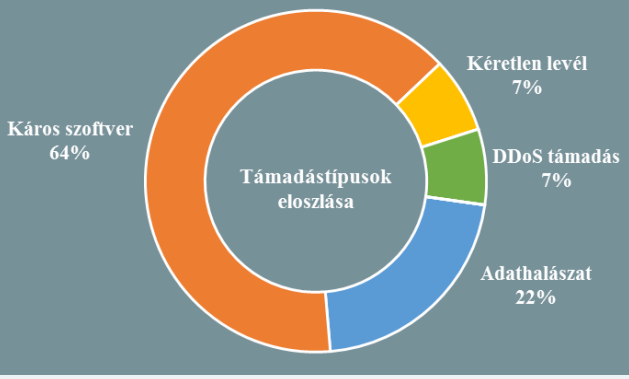
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.05.11. - 2018.05.17.



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

Hogyan kezeli az Amazon a gyermekek adatait?

(www.engadget.com)

A törvényhozók levélben kértek tájékoztatást arról, hogy a cég Echo Dot nevű, személyi asszisztens funkcióval bíró okoshangszórójának gyerekeknek szánt verziója gyűjt-e adatokat a gyermekekről, és azt megosztják-e harmadik féllel, valamint arra is kíváncsiak voltak, hogy az eszköz fejlesztése során egyeztettek-e kis- és fiatalkorúaknak készült szoftverekre specializálódott alkalmazásfejlesztési szakértőkkel. Az Amazon a CNET-nek tett válasznyilatkozatában reagált néhány kérdésre. Eszerint a cég komolyan veszi a magánélet védelmét, így a rendszer csak adott hangutasítás elhangzásakor kezd rögzíteni, ráadásul a szülők ezt ki is kapcsolhatják egy gombnyomással. Emellett képesek törölni is a gyermekekről készült hangfelvételeket az eszközről és a szerverekről egyaránt, amikhez a vállalaton kívül más nem férhet hozzá. A nyilatkozatban az is kifejtésre került, hogy a cég a gyermekek online adatvédelméről szóló törvénynek (Children's Online Privacy Protection Act) is megfelel. Josh Golin, a Campaign for a Commercial-Free Childhood csoport ügyvezető igazgatója szerint a válasz ennek ellenére nem kielégítő, az eszközt pedig egy újabb felesleges, potenciálisan káros terméknek tartja, aminek célja, hogy a gyermekek függővé váljanak a használatától. Az Amazonnak június 1-ig az összes feltett kérdésre válasszal kell szolgálnia. **Bővebben...**

Rendszerkritikusok elleni támadásokkal vádolják a török kormányt

(www.motherboard.vice.com)

Az Acces Now digitális jogvédő szervezet jelentése szerint a török kormányzat kiterjedt kampányt folytatott török aktivistákkal és ellenzékiekkel szemben – írja a Motherboard. A kutatók vizsgálatai szerint a 2017 júniusa és júliusa közötti „Igazság menete" ellenzéki tüntetéseken résztvevőket a Twitter-en keresztül igyekeztek kompromittálni a kormányzatok számára kémszoftvereket gyártó FinFisher cég FinSpy elnevezésű malware-ének egy új variánsával. A jelentés emellett kitér arra is, hogy további hat FinSpy mintát is azonosítottak, amelyek Ukrajnában, Líbiában, Venezuelában és Indonéziában kerültek felhasználásra. **Bővebben...**

A British Telecom összefog az Europollal

(www.europol.europa.eu)

A BT vállalatcsoport együttműködési szándéknyilatkozatot írt alá az Európai Rendőrségi Hivatallal, miszerint információt cserélnek egymás között a főbb kiberfenyegetésekről és támadásokról. Kevin Brown, a BT Security Threat Intelligence alelnökének nyilatkozata szerint nem ez az egyetlen bűnüldöző szervezet, akikkel közreműködnek, emellett idén – telekommunikációs cégként a világon elsőként – a Malware Information Sharing Platform (MISP) nevű, ingyenes online portálon is információmegosztásba kezdtek. **Bővebben...**

Ellenőrzés alatt a Google adatkezelési elvei Ausztráliában

(www.reuters.com)

Az Oracle által készített jelentés szerint – mely a Google és a Facebook reklámpiaci hatásait vizsgálta – a keresőóriás részletes információt kap az Android felhasználók internetes kereséseiről és a tartózkodási helyadatairól, melyek nagyságrendileg több gigabájtot is jelenthetnek, és ezek a Google-höz való eljuttatása az adott felhasználó internetszolgáltatójától igénybevett adatkeret terhére történik. Az ausztrál Versenyjogi és Fogyasztói Bizottság (ACCC), valamint az ausztrál adatvédelmi biztos felülvizsgálják a jelentés állításait. **Bővebben...**

Az Apple tiltja a helyadatokkal visszaélő alkalmazásokat

(www.nakedsecurity.sophos.com)

Az Apple – vélhetően a GDPR közelgő hatálybalépése miatt– kitiltja áruházából azokat a fejlesztőket, akiknek alkalmazásai olyan kódokat, keretrendszereket, illetve SDK-kat tartalmaznak, melyekkel az alkalmazások képesek megosztani a felhasználók helyadatait. A cég számos alkalommal emlékeztette fejlesztőit, hogy alkalmazásuk sértheti az App Store felülvizsgálati irányelv 5.1.1 és 5.1.2 szakaszait, melyek az adatok gyűjtésére, tárolására, felhasználására és megosztására vonatkoznak. Emellett nyomatékosan kérték a fejlesztőket, hogy a felhasználók kapjanak pontos tájékoztatást arra vonatkozóan, hogy az alkalmazás milyen típusú adatokhoz férhet hozzá, beleértve a helyadatokat is. **Bővebben...**

IT biztonsági Tanács

Drupal tartalomkezelő használata esetén az alábbiak segítségül szolgálhatnak a biztonság növeléséhez:

- A People > Permissions alatt korlátozzuk az „authenticated user” és az „anonymous user” felhasználói csoportok számára kiosztott jogosultságokat.
- Ügyeljünk rá, hogy kizárólag az adminisztrátor hozhasson létre felhasználói fiókokat.
- Kövessük nyomon a Drupal-t érintő biztonsági közleményeket, például a Drupal és a Drupal Security Twitter fiókok üzeneteit.
- Tiltsuk le a Testing (korábban SimpleTest) modult, mivel az támadásra is felhasználható.

Megjelent Luxemburg új nemzeti kiberbiztonsági stratégiája

(www.enisa.europa.eu)

Az új verzió a megelőző – 2015. és 2017. közötti időszakra vonatkozó – stratégiáról kapott visszajelzések figyelembevételével készült, és olyan intézkedéseket fed le, amelyek javítják a számítógépes rendszerek és hálózatok informatikai támadásokkal szembeni védelmét, illetve általánosságban a digitális technológiák ellenálló képességét. Ennek részeként a kormányzat a szabályozhatóság fenntartásához, valamint a stratégiában megfogalmazott célok megvalósításának megkönnyítése érdekében egy tárcaközi koordinációs bizottságot is létrehozott. **Bővebben...**

Az Egyesült Államok Belbiztonsági Minisztériuma (DHS) bemutatta új kiberstratégiáját

(www.reuters.com)

Kirstjen Nielsen, a minisztérium vezetője úgy véli, a fenyegetések már a köztársaság szerkezetét veszélyeztetik. A Reuters hozzájutott egy még nem publikált, 35 oldalas jelentéshez, amely szerint az Egyesült Államokat egyre több kifinomult technikákat alkalmazó rosszindulatú szereplő fenyegeti, akik motivációi között elsősorban a kémkedés, politikai és ideológiai érdekek, illetve gazdasági előnyszerzés áll, ami nem csak az állami támogatású hacker csoportokra érvényes. A jelentés kitér arra is, hogy 2020-ra több, mint 20 milliárd internethez csatlakoztatható eszközre lehet számítani, ami jelentős biztonsági kockázatot jelent. Mindemellett amerikai hírszerzők szerint Oroszország – a 2016-os elnöki kampányhoz hasonlóan – valószínűleg a 2018-as időközi kongresszusi választásokba is be fog avatkozni. Ezzel kapcsolatban Nielsen még márciusban azt nyilatkozta, hogy a szervezet a választások védelmét jelenleg minden más kritikus rendszer elé helyezi. **Bővebben...**

WikiLeaks-es szivárogtatással gyanúsítanak egy volt CIA ügynököt

(www.securityweek.com)

A The New York Times és a The Washington Post szerint Joshua Adam Schulte-t, egy 29 éves szoftver mérnököt vádolnak a „Vault 7” szivárogtatással, melynek során a CIA-től származó titkos hacker eszközökről közölt információkat a WikiLeaks. A vádlott 2010-ben az NSA-nél is dolgozott, mielőtt a CIA alkalmazásába került volna, ahol 2016 novemberéig szoftvermérnökként tevékenykedett. Annak ellenére, hogy a hatóságok már egy héttel a 2017. márciusi szivárogtatás után gyanúsították Schulte-t, nem emiatt emeltek vádat ellene, hanem gyermekpornográf tartalmú anyagok birtoklása miatt. Schulte jelenleg börtönbüntetését tölti, amiért megszegte a számítógépes rendszerek használatától, valamint New York város elhagyásától való eltiltását. **Bővebben...**

Hollandia is korlátozza a Kaspersky termékek használatát

(www.bleepingcomputer.com)

Hasonlóan az Egyesült Államokhoz, a holland kormány is kitiltja hálózatából a Kaspersky antivírus szoftvereit – derült ki a holland igazságügyi miniszter leveléből. Ferdinand Grapperhaus mindezt „óvintézkedésnek” nevezte, arra hivatkozva, hogy a cég az orosz kormányzat befolyása alatt állhat, és Hollandia a múltban már vált az orosz kiberkémkedési tevékenység célpontjává. A kitiltás a kormányzati hálózatokon kívül a létfontosságú szolgáltatásokat és folyamatokat ellátó szervezeteket is érinti. **Bővebben...**