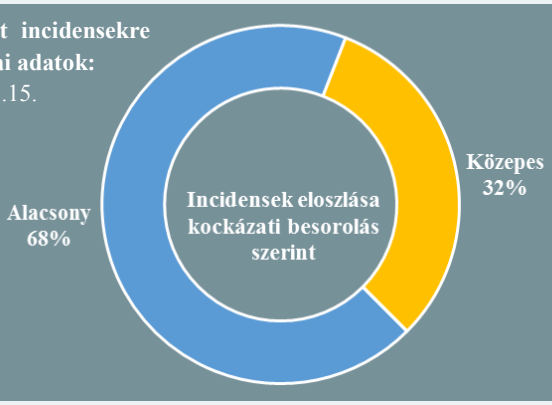
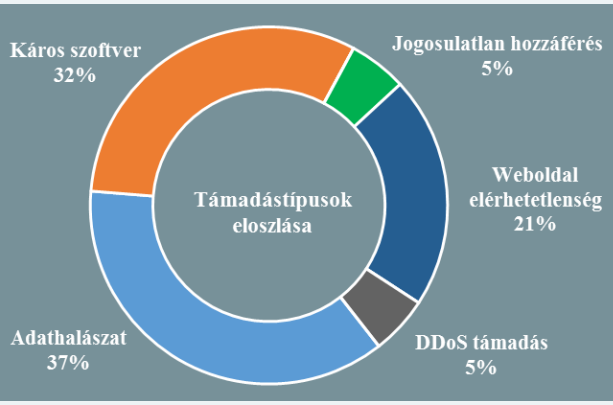
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2018. 46. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.11.09. - 2018.11.15.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!

A holland kormány szerint a Microsoft Office telemetrikus adatgyűjtése sérti a GDPR-t

(zdnet.com)

Egy, a holland hatóságok által lefolytatott vizsgálat nyolc adatvédelmi problémát tárt fel az Office 2016 és Office 365 programok telemetrikus adatgyűjtése kapcsán; az elemzők szerint a Microsoft „jelentős mértékű felhasználói adatgyűjtést" végez. Az egyik lényeges kritika azért érte a vállalatot, amiért az véleményük szerint nem tájékoztatja megfelelően ügyfeleit a tevékenységről, ugyanis hivatalos dokumentáció nem érhető el arra vonatkozóan, hogy a cég pontosan milyen adatokat gyűjt, sem arról, hogy a telemetriát hogyan lehet kikapcsolni. Az elemzés során ráadásul megállapítást nyert, hogy a szoftverfejlesztők által gyakorta gyűjtött diagnosztikai adatok mellett az Office alkalmazások konkrét felhasználói tartalmakat is rögzítettek, mint például az e-mail tárgy mezőben szereplő szövegek, és olyan dokumentumokból származó mondatok, amelyeken a cég fordító és helyesírás-ellenőrző programjait használták. A holland kormány aggodalmának oka, hogy attól tartanak, az adatgyűjtés során szenzitív kormányzati adatok kerülhettek amerikai szerverekre, mivel legalább 300 000 kormányzati gépen futtatnak Office alkalmazásokat. Minderről tájékoztatták a Microsoftot, akik a jelentés szerint már részben módosítottak is a beállításokon, lehetővé téve az adatgyűjtés teljes korlátozását, ugyanakkor nem egyértelmű, hogy ez minden ügyfél számára elérhető-e. A tech óriás emellett ígéretet tett arra vonatkozóan, hogy a jövőben nagyobb átláthatóságot biztosítanak a telemetrikus adatgyűjtés kapcsán.

Szofisztikált kiberkémkedési kampány zajlik Pakisztán ellen

(securityweek.com)

A Cyclane kutatói szerint egy korábban nem azonosított csoport pakisztáni kormányzati és katonai célpontok ellen szokatlanul komplex kiberkémkedést hajt végre. A biztonsági cég által „The White Company"-ként elnevezett hacker csoportról feltételezik, hogy állami támogatással bírhat, több 0. napi sérülékenységet kihasználó kóddal is rendelkezik, a felhasznált malware-eket és technikákat folyamatosan fejleszti, valamint azokat az adott küldetésre szabva célirányosan alkalmazza. A már egy éve zajló, „Operation Shaheen" néven azonosított kampány során a támadók ─ az elemzők szerint egyedülálló módon ─ több neves vírusirtó cég termékét (például Sophos, ESET, Kasperksy, BitDefender, Avira, Avast!, AVG, Quick Heal) is képesek voltak kijátszani, valamint a felhasználó ellen fordítani. A Cylance szerint a kampány még nem zárult le, mivel egy, a támadásokhoz köthető IP továbbra is aktív.

Routolási hiba miatt vált átmenetileg elérhetetlenné a Google több szolgáltatása

(arstechnica.com)

A ThousandEyes szerint egy BGP route szivárgási hiba következtében hétfőn egyes felhasználók több Google-ös szolgáltatás ─ például a Google kereső, vagy a G Suite ─ elérhetetlenségét tapasztalhatták. A hiba 21:13-kor (UTC) kezdődött, amikor a MainOne Cable Company ─ egy kis nigériai internetszolgáltató ─ 212 db, a Google-höz tartozó IP tartomány esetében téves útválasztási információkat kezdett hirdetni, miszerint ezek az ő ún. autonóm rendszerén (AS37282) keresztül érhetők el. A fals routing információt röviddel ezt követően a China Telecom rendszere elfogadta és tovább hirdette, csakúgy, mint az orosz Transtelecom és más nagyobb szolgáltatók, ezzel világméretűvé téve a hibás konfigurációt. Az útvonal probléma 74 percig tartott, az érintett szolgáltatások felé irányuló forgalom ezen időszakban nem ért célba, hanem eldobásra került. **Bővebben...**

Mobil platformon is használhatjuk a Cloudflare publikus DNS szolgáltatását

(bleepingcomputer.com)

A Cloudflare és az APNIC által tavaly áprilisban útjára indított, az 1.1.1.1 címen elérhető publikus DNS-e most már Androidon és iOS-en is elérhető egy alkalmazás segítségével. A cég szerint szolgáltatásuk nem csak, hogy rendkívül gyors, de anonim DNS névfeloldást biztosít, mivel egyetlen IP címet sem rögzít, és az összes keletkező logot 24 órán belül törli. A most megjelentetett applikáció telepítés és bekapcsolás után egy VPN profilt hoz létre, ami ettől kezdve automatikusan a Cloudflare szerverei felé irányítja a DNS feloldási forgalmat. Épp, hogy csak megjelent, az alkalmazást máris kritika érte, egyes felhasználók ugyanis azt kifogásolják, hogy az androidos verzió hozzáférést kér a mobil eszköz mikrofonjához, a készüléken tárolt médiatartalmakhoz, valamint az USB háttértárhoz. A cég szerint ezek a hibariportok generálásához szükségesek és csakis ekkor kerülnek használatra.

IT biztonsági Tanács

A Pwn2Own nemzetközi hacker versenyen került napvilágra egy, az iOS legújabb verzióján felfedezett biztonsági rés, amely illetéktelen távoli hozzáférést nyújthat azon, a felhasználó által már törölt képekhez, amelyek még nem kerültek felülírásra.

A biztonsági hiba befoltozásáig az iPhone felhasználók számára javasolt egy második, immár végleges törlési lépés elvégzése: a „Photos” alkalmazás „Recently Deleted” alatt listázott elemeken.

Az e-ügyintézés és az elektronikus igazolványok továbbra sem népszerűek Németországban

(heise.de)

Idén a németek csupán negyven százaléka használta az elektronikus ügyintézési szolgáltatásokat, ismételten egy százalékponttal kevesebben mint az előző évben, és öt százalékponttal kevesebben mint 2016-ban; emellett az elektronikus személyi igazolványok terén sem jelentkezett áttörés. Az ezen számokat bemutató tanulmány arra is felhívta a figyelmet, hogy az amúgy is alacsony számúnak mondható felhasználói kör 58 százaléka elégedett a szóban forgó szolgáltatásokkal. A statisztika azt is kimutatta, hogy mind Ausztriában, mind pedig Svájcban – tehát a hegyvidékibb területekkel rendelkező országokban – magasabb arányú a digitális ügyintézés. A németországi internet-használók több, mint egyharmada még mindig problémásnak ítéli az elektronikus ügyintézéssel összefüggő adatvédelmi, információbiztonsági kérdéseket, ezért nem is használja az említett digitális ügyintézési felületeket. Szintén problémát jelent, hogy az adóbevalláson túlmenően nagyon kevés elektronikus közszolgáltatás ismert az állampolgárok körében; és az elektronikus ügyintézéssel együtt járó előnyöket sem sikerült tudatosítani az emberekben. Az elektronikus személyi igazolványok kapcsán elmondható, hogy a népesség csupán hat százaléka tudja használni az ezzel járó szolgáltatások teljes körét.

Több nagyhatalom sem írta alá a francia kiber-paktumot

(zdnet.com)

Az „Öt Szem” országok közül egyedül Kanada írta alá Emmanuel Macron francia köztársasági elnök „Digitális Genfi Egyezményként” is hivatkozott kiber-paktumát, további 51 országgal, 224 vállalattal, valamint 92 non-profit csoporttal egyetemben. Az Egyesült Államok, Nagy-Britannia, Oroszország és Kína mellett azonban olyan jelentős kiber arzenállal rendelkező államok sem adták támogatásukat, mint Irán, Izrael és Észak-Korea. A megállapodás így ─ a ZDNet megfogalmazásában ─ hiábavalónak tekinthető, habár egyes vélemények szerint mindez eleve csupán szimbolikus jelentőséggel bírt, ugyanis nem ír elő büntetést azokkal szemben, akik megszegnék a dokumentumban vállaltakat. A „The Paris Call for Trust and Security in Cyberspace” egyezmény elsősorban olyan kötelezettségeket és célokat tartalmaz, mint például a kritikus rendszerek elleni, vagy magát az Internetet veszélyeztető támadások megelőzése, a kiberkémkedés, vagy a kiberbűnözés visszaszorítása.

Készül az új HTTP protokoll verzió, ami búcsút inthet a TCP-nek

(arstechnica.com)

A weboldalak megjelenítéséért felelős HTTP eddigi verziói (1.0, 1.1, és 2) mind az adatok megbízható, sorrendhelyes, hibamentes átviteléért felelős TCP hálózati protokollra épültek, azonban az új, 3-as verzió már elképzelhető, hogy az UDP egy fejlesztett változatát használná. A Google a webes böngészés gyorsabbá tételének céljából már egy ideje dolgozik ezen a kísérleti jellegű hálózati protokollon, amelyet QUIC-nek (Quick UDP Internet Connections) neveztek el. A tervek szerint ez megtartaná a TCP megbízhatóságát és sorrendhelyességét, azonban gyorsabb kommunikációt tenne lehetővé. Az IETF már a QUIC standardizálásán dolgozik, amely azonban jelentősen eltér a Google eredeti javaslatától.