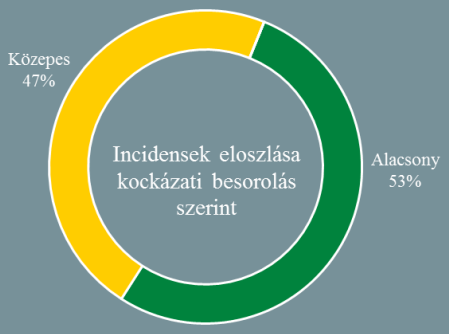
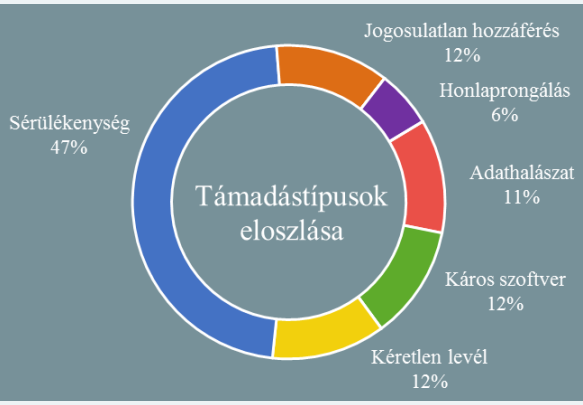
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.04.12. - 2019.04.17.





Kövessen minket megújult weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

Szofisztikált dezinformációs kampány irányult a litván védelmi miniszter ellen

(securityaffairs.co)

A litván védelmi minisztérium közleménye szerint komplex információs támadás érte Raimundas Karoblis védelmi minisztert, akiről olyan álhírek kezdtek terjedni, hogy korrupciós vádak miatt nyomozás folyik ellene. A támadás első fázisában egyes kormányzati hivatalok dolgozóihoz érkeztek hamis információkat és káros hivatkozást tartalmazó e-mailek, amelyek látszólag a védelmi minisztérium egy munkatársától származtak. A támadók ezzel párhuzamosan sikeresen bejuttatták a hírt a „Kas vyksta Kaune“, valamint a „Baltic Times“ nevű litván hírportálokhoz, ami ezeken kívül megjelent még az „OpEdNews“ nevű amerikai illetőségű véleményközlő weboldalon is. Utóbbi esetben a bejegyzés szerzőjeként a litván DELFI hírportál vezérigazgatóját, Vytautas Benokraitist tüntették fel, aki valójában soha nem publikált az OpEdNews-on ilyen témában. A litván Nemzeti Kiberbiztonsági Központ (National Cyber Security Centre) jelenleg is vizsgálja az esetet, illetve arra kéri a lakosságot, hogy legyenek kritikusak a hírekkel szemben, hogy ne válhassanak a manipuláció áldozatává.

Kvantumkriptográfiai fejlesztésekbe fog a NATO

(nato.int)

A kvantumtechnológia a közeljövőben számos területre fog komoly hatást gyakorolni, a lehetséges pozitív hatások mellett ugyanakkor számolni kell a potenciális veszélyekkel is. Lényeges problémát jelent például, hogy a kvantumszámítógépek hatalmas számítási kapacitásával a hagyományos titkosítási megoldások ─ amelyek a digitális kommunikációk biztosításának alapjául szolgálnak ─ feltörhetőek lesznek. A problémakör kezeléséhez a NATO Science for Peace and Security (SPS) programja két projektet is indít. **Bővebben...**

Hirdetésekbe rejtett vírussal támadják az iOS-es Chrome felhasználókat

(zdnet.com)

Kizárólag iOS felhasználókat céloz egy malvertising (reklámalapú vírusterjesztés) kampány, amelynek során a támadók online hirdetésekbe rejtett káros kódokkal rosszindulatú webhelyekre irányítják át a felhasználókat. A támadók az iOS Chrome mobilböngésző egy sérülékenységét kihasználva képesek megkerülni a Chrome beépített sandboxát is. A Google megkezdte a biztonsági rés vizsgálatát, amelyről már kiderült, hogy a Google Chrome más platformokon futó verzióit és a Safarit sem érinti. **Bővebben...**

Több száz VPN alkalmazást érinthet egy súlyos sérülékenység

(bleepingcomputer.com)

Az Egyesült Államok nemzeti kiberbiztonsági ügynöksége (National Cybersecurity and Communications Integration Center – NCCI) riasztást adott ki egyes VPN alkalmazásokat sújtó sérülékenységről, amelynek kihasználásával átvehető az irányítás a támadott rendszer felett. A Carnegie Mellon Egyetem kiberbiztonsági eseménykezelő csoportja (CERT/CC) által felfedezett biztonsági hiba – szerintük – a Palo Alto Networks, a Pulse Secure, a Cisco és az F5 Networks VPN alkalmazásait biztosan érinti, azonban potenciálisan több száz további VPN szoftvert is veszélyeztethet. A probléma hátterében az áll, hogy a hitelesítő adatok, valamint a session cookie-k titkosítás nélkül kerülnek tárolásra a memóriában és a naplóállományokban. Amennyiben ehhez illetéktelenek hozzáférnek az adatokat felhasználhatják a hitelesítés megkerülésére, ezzel pedig jogosultság-kiterjesztést érhetnek el. Az F5 és a Cisco ezidáig nem reagált a biztonsági rés hírére, a Palo Alto Networks és a Pulse Secure ellenben már adott ki hibajavítást. **Bővebben...**

A Google helyadatok átadásával segíti a bűnüldözést

(thehackernews.com)

Ismert, hogy a Google folyamatosan gyűjti a felhasználók helyadatait, még akkor is, ha a „Helyelőzmények” (Location History) tiltott az eszközökön. Azt is tudni, hogy a tech óriás ─ bírói határozat ellenében ─ meg is osztja ezeket az adatokat az amerikai hatóságokkal. A The New York Times egy, a napokban publikált mélyrehatató vizsgálata azonban egy olyan tevékenységre világított rá, amely sokkal kevésbé kapott publicitást eleddig. Mint kiderült, a cég a bűncselekményekben gyanúsított személyek azonosításában is közreműködik azáltal, hogy a szövetségi nyomozó hatóságok számára rendelkezésre bocsátja az adott időben a bűntények körzetében tartózkodók helyzeti adatait. Minderre a Google egy SensorVault nevű adatbázist tart fent, amelyből képes kikeresni, hogy egy adott virtuális határvonallal ellátott földrajzi területen (geofence), milyen eszközök haladtak át. **Bővebben...**

IT biztonsági Tanács

A hamis hírkampányok (Fake news) sikere sok esetben a felhasználók figyelmetlenségének köszönhető. Néhány dolog, ami kételyt ébreszthet bennünk a hír valódiságával kapcsolatban: túlzó, hatásvadász címek; egy valós portál nevéhez hasonlító webcím; forrás, szerző megjelölésének hiánya; hibás, vagy hiányzó dátummegjelölés; elgépelések a szövegben; halmozott írásjelek használata; igénytelen, összecsapott webdesign.

Bemutatták az amerikai fogyasztók személyes adatainak védelmére vonatkozó törvénytervezetet

(www.bleepingcomputer.com)

Edward J. Markey amerikai szenátor április 11-én törvényjavaslatot nyújtott be az amerikai fogyasztók személyes adatainak védelmére vonatkozóan. Az S.1214-es számú, magánélethez való jogról szóló törvényjavaslat (Privacy Bill of Rights Act) többek között tiltaná a személyes adatok diszkriminatív módon történő felhasználását, kötelezné a vállalatokat a birtokukban lévő személyes felhasználói adatok megfelelő védelmének biztosítására, valamint kizárólag a szolgáltatások igénybevételéhez szükséges fogyasztói adatokra korlátozná az adatgyűjtést. A fogyasztókat egy központosított holnapon tájékoztatná jogairól, ahol megkövetelné a vállalatoktól, hogy a fogyasztókat közvetlenül érthető formában értesítsék, továbbá lehetővé tenné mind az államügyészek, mint a magánszemélyek számára, hogy keresetet nyújtsanak be az egyének magánélethez való jogait sértő vállalatok ellen. **Bővebben...**

A Kaspersky szerint a kibertámadások 70%-a Microsoft Office sebezhetőségeket használ ki

(www.zdnet.com)

A Kaspersky Lab szerint az elmúlt negyedévben az általuk azonosított informatikai támadások 70%-a a Microsoft Office sebezhetőségei ellen irányult, ami négyszer annyi, mint amennyit a biztonsági cég két éve mért ugyanezek kapcsán. A Kaspersky hozzáteszi, hogy a leginkább kihasznált sérülékenységek nem közvetlenül az Office termékeket érintik, hanem azok valamely komponensét. A két leggyakrabban támadott biztonsági rés (CVE-2017-11882, CVE-2018-0802) például az Equation Editor kapcsán áll fenn, amely a Microsoft Word újabb verzióiban már csupán visszafelé kompatibilitási okokból van jelen. **Bővebben...**

Agresszív DNS eltérítéses támadási kampányt azonosított a Cisco Talos

(blog.talosintelligence.com)

A Cisco Talos fenyegetéselemző csapata egy agresszív DNS (Domain Name System) eltérítéses támadási műveletet azonosított, amely már nagyjából két éve zajlik, és eddig körülbelül 40 szervezetet érint. A „Sea Turtle”-re keresztelt művelet hátterében egy állami támogatású APT csoport állhat, azonban konkrét nemzetállamot eddig nem neveztek meg. Az összetett támadások célja a kiszemelt weboldalak felé irányuló hálózati forgalom elterelése a támadók irányítása alatt álló káros weboldalak felé, amelyet a DNS rekordok módosításával érnek el. A kampány célpontjában ezért számtalan szervezet állhat: domain nyilvántartók és regisztrátorok, DNS gyökérzóna szerver üzemeltetők, webtárhely szolgáltatók, stb. **Bővebben...**

Németországban elektronikus személyazonosító nyilvántartást állítanak fel az EU polgárai vonatkozásában

(www.heise.de)

A német szövetségi parlament (Bundestag) elé került azon törvényjavaslat, amelynek értelmében az Európai Gazdasági Térséghez tartozó személyek elektronikus személyazonosító igazolványt igényelhetnek majd a jövőben. Az említett döntés értelmében a német személyi igazolványok online funkciói – egy erre szolgáló chipkártya révén – a későbbiekben szélesebb személyi körhöz juthatnak majd így el, lehetővé téve az egyes szerveknél történő online személyazonosítást. **Bővebben...**