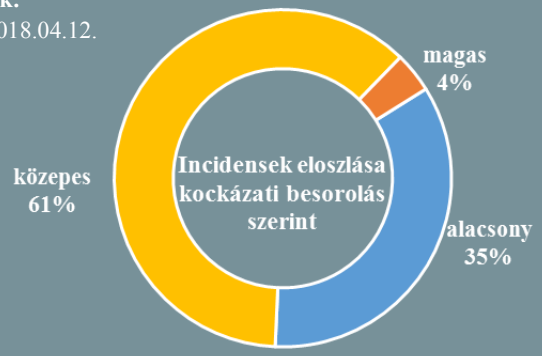
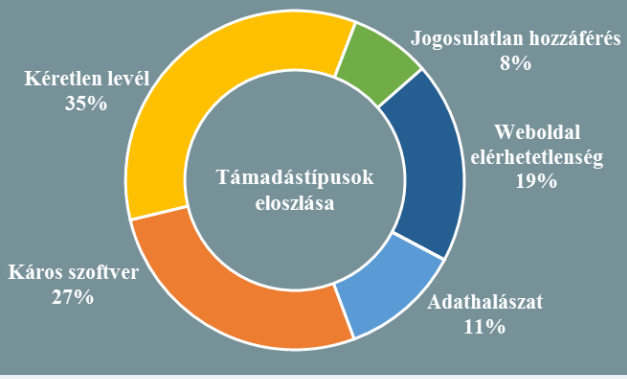
Nemzetközi IT-biztonsági sajtószemle

Incidens adatok:
2018.04.06. - 2018.04.12.





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

A Reddit is küzd az orosz propagandával

(www.theregister.co.uk)

A Reddit nyilvánosságra hozta, hogy az oldal az orosz befolyás kivizsgálása során 944 fiókot zárolt, amelyeket az orosz „troll gyárként" aposztrofált Internet Research Agency-hez (IRA) kötnek. Az átláthatósági jelentés szerint ezek közül csupán 13 rendelkezett 10 000 feletti „Karmával" – ami a Reddit felhasználók közösségi aktivitását jelző mérőszám – 662 azonban egyáltalán nem kapott ilyen, a hivatkozások megosztása és kommentelések után járó pontot, ami arról árulkodik, hogy ezek valószínűleg nem élő fiókok. A Karmával rendelkező fiókok több, mint fele (145) ugyanakkor a biztonsági házirend alapján már korábban tiltásra került, még az amerikai választás előtt. Összességében csupán 7 olyan fiók volt, ami magas pontszámmal rendelkezett és átjutott a szigorú szűrésen. A szóban forgó gyanús fiókok egy meghatározott ideig még elérhetőek lesznek az érdeklődők számára. **Bővebben...**

Ausztráliában is megkezdődött a kriptovaluta szolgáltatók szigorú felügyelet alá vonása

(www.in.reuters.com)

A pénzmosás, a terrorizmus és a kiberbűnözés finanszírozásának visszaszorításának érdekében az ausztrál kormány azonnali hatállyal kötelezi a kriptovaluta szolgáltatókat, hogy regisztráljanak az ausztrál üzleti hírszerző ügynökségnél (AUSTRAC). Az intézkedés a pénzmosás és terrorellenes finanszírozási törvény (AML/CTF) támogatását szolgálja, mely előírja a szabályzás alá eső pénzügyi szervezetek (pl.: bankok és egyéb pénzforgalmi szolgáltatók) számára a felhasználók személyazonosságának megállapítására szolgáló információ gyűjtését, a tranzakciók nyomon követését, valamint hogy, jelentsék a 10 000 AUD-t meghaladó készpénzfelvételeket és egyéb gyanús tevékenységeket. Az AUSTRAC az új szabályzással növelte a pénzügyi hírszerzés lehetőségeit, azáltal, hogy a bitcoin és más kriptovaluták felhasználásáról szóló információk is megosztásra kerülnek az iparág és a kormányzati partnerek között – nyilatkozta Nicole Rose, az AUSTRAC vezérigazgatója. A jogalkotási reform következő – nagy kihívást jelentő – lépcsőfoka a szabályok ügyvédekre, könyvelőkre, ingatlanügynökökre és viszonteladókra történő kiterjesztése lesz. **Bővebben...**

Minden eddiginél kiterjedtebb média monitoring rendszert vezetne be az USA

(www.gizmodo.com)

Az amerikai Belbiztonsági Minisztérium (DHS) világszerte több, mint 290 000 hírforrás nyomon követését kívánja megvalósítani, egy olyan adatbázis létrehozásával (Media Intelligence and Benchmarking Platform), mely az újságírók, szerkesztők, bloggerek, valamint egyéb közösségi médiaszereplők adatait, és az általuk közzétett publikációkat gyűjti össze és kategorizálja, ezáltal beazonosíthatóvá válnak a médiát leginkább befolyásoló „véleményvezér" személyek. A felhívásban a DHS közzétette a monitorozó rendszer megvalósítására vonatkozó követelményeket, melyre a vállalatok április 13-ig jelezhetik, amennyiben rendelkeznek a megfelelő képességgel. A követelmények szerint az adatbázisnak képesnek kell lennie a legtöbb médiumon keresztül terjesztett tartalom monitorozására. Annak ellenére, hogy az FBI már régóta figyelemmel kíséri az újságírókat, ilyen széles körű koordinált gyűjtésre eddig nem volt példa. **Bővebben...**

A vállalatok túlnyomó többségét a mobil eszközök biztonságával kapcsolatban a túlzott magabiztosság jellemzi

(www.forbes.com)

Az amerikai Verizon telekommunikációs óriás 2017 végén egy több szektort is átfogó felmérést végzett a vállalati mobil eszközök használatával kapcsolatban, amely több problémára is fényt derített. Eszerint, bár a cégek egyértelműen felismerik az ezekben rejlő biztonsági kockázatot (85% szerint ez közepes szintű, 26% gondolja jelentősnek), sőt annak folyamatos növekedésével is számolnak, ennek ellenére az üzleti célokat kiszolgáló hatékonyság érdekében háttérbe szorítják a biztonsági megfontolásokat. A válaszadó szakemberek mintegy 89%-a úgy nyilatkozott, hogy a mobil eszközök védelme érdekében a vállalatuk csupán egy biztonsági mechanizmust valósít meg, ráadásul sok helyen az alapvető megoldásokat sem alkalmazzák, például 39%-uk továbbra sem gondoskodik a alapértelmezett jelszavak cseréjéről. **Bővebben...**

IT biztonsági Tanács

Amennyiben elfelejtette az Apple ID -hoz tartozó jelszavát, de korábban aktiválta az Apple ID kétlépéses hitelesítését, visszaállíthatja a jelszót bármilyen megbízható Apple készülékről egy jelszóval vagy jelkóddal. Lehetősége van egy ún. „helyreállítási kulcs" generálására is, amely nem kötelező, azonban nagyobb biztonságot nyújt. Ugyanakkor, hogy ha ezt elveszíti, abban az esetben többé nem fog tudni belépni az Apple ID-fiókjába, ezért célszerű a kulcsból több példányt, megbízható helyen tárolni.

A T-mobile osztrák leányvállalatánál plaintext-ben tárolják a jelszavakat?

(www. motherboard.vice.com)

A kérdés annak kapcsán merült fel, hogy a vállalat egy munkatársa egy, a Twitteren küldött üzenetben felfedte, hogy a felhasználói jelszavak első 4 karaktere hozzáférhető az ügyintézők számára – írja a Motherboard. Ezt követően vita alakult ki több felhasználó és az ügyfélszolgálat között, miszerint a jelszavak egyszerű szövegként történő tárolása mennyire veszélyes az esetleges informatikai támadások miatt. A cég egyik képviselője ugyanakkor igyekezett árnyalni a képet, miszerint az ügyintézők számára megjelenített információk és az adatok tárolási módjának összekeverése okozta a félreértést, és jelezte, hogy a biztonsági felelőssel való egyeztetés után bővebb információt közöl a témáról, ám ez a publikáció elkészültéig nem történt meg. **Bővebben...**

Egy lépéssel közelebb a Telegram betiltásához

(www.engadget.com)

Múlt hét pénteken az orosz kormányzat pert indított annak érdekében, hogy korlátozza a Telegram üzenetküldő alkalmazást az országban, mivel a cég nem felel meg a törvényi előírásoknak. A csevegő platform és a Roskomnadzor közötti vita még 2017 során kezdődött, amikor az orosz médiafelügyeleti szervezet betiltással fenyegette meg a népszerű csevegő platformot, amiért a cég nem működött együtt a Szövetségi Biztonsági Szolgálattal (FSB) egy terrortámadás kivizsgálásában. A még 2016-ban elfogadott jogszabályok alapján ugyanis az országon belül működő üzenetküldő szolgáltatásoknak biztosítaniuk kell a hatóságok számára az üzenetek visszafejthetőségét, a Telegram alapítója ugyanakkor ezt etikai és – a végponttól végpontig terjedő titkosítás miatt – technikai korlátokra hivatkozva elutasította. **Bővebben...**

Egyszerűbb és biztonságosabb webes autentikáció

(www.engadget.com)

A tech cégek évek óta igyekeznek kiváltani a jelszavak használatát a weben, a FIDO Szövetség és a World Wide Web Konzorcium ennek kapcsán kidolgozott egy új webes hitelesítési szabványt (Web Authentication: An API for accessing Public Key Credentials - WebAuthn), amely lehetővé teszi valóban egyedi titkosított hitelesítő adatok használatát minden webes szolgáltatáshoz. Mindemellett a megszokott technológiák, mint az ujjlenyomat olvasók, a kamerák és az USB kulcsok továbbra is használhatók lesznek, és akár a jelszavakat is megtarthatjuk. A Google, a Microsoft, a Mozilla és az Opera mind jelezték, hogy elkötelezettek az új technológia implementálásában, sőt, a Firefoxban már jelenleg is támogatott. **Bővebben...**

További adatelemző cég kereskedhetett a Facebook-ról gyűjtött személyes adatokkal

(www.cnbc.com)

A CNBC hívta fel a Facebook figyelmét a CubeYou (CY) nevű szervezetre, akik a Cambridge Analytica-hoz hasonlóan szintén a Cambridge-i Egyetemmel közreműködve online kvízkérdések során gyűjthettek felhasználói adatokat, amelyeket azután harmadik félnek adtak át. Az amerikai hírcsatorna szerint, a többek között megtévesztő módon "tudományos, non-profit kutatásnak" címkézett kérdéssorok által nyert privát, személyazonosításra alkalmas információkat (nevek, e-mail címek, telefonszámok, IP címek, mobil eszköz és böngésző azonosítók, stb.) reklámügynökségeknek adták el, amiket azután célzott reklám kampányok során hasznosíthattak. **Bővebben...**