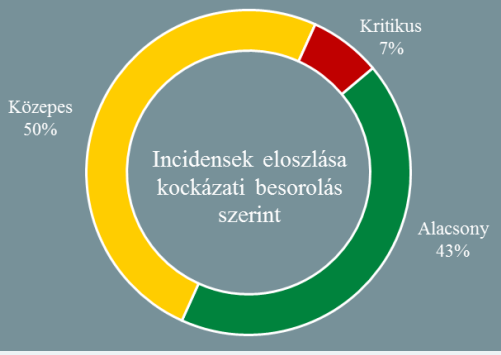
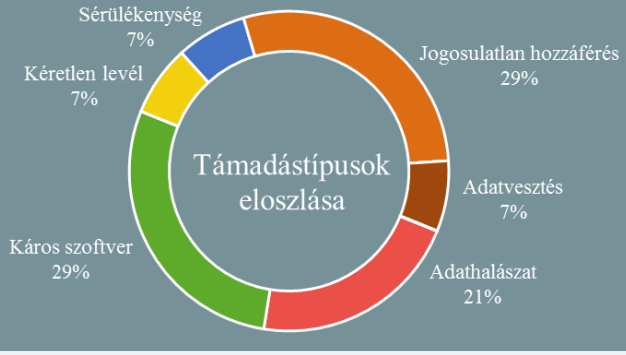
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.01.25. - 2019.01.31.





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

A német politikai pártok tartományokon átívelő, egységes minimumkövetelményeket szeretnének a kiberbiztonság terén

(heise.de)

A német CDU és CSU pártok az állampolgárok, a vállalkozások, illetve az állam vonatkozásában egyaránt egységesebb kibervédelmi stratégiát akarnak elérni a kibertámadások növekvő száma okán. EU-s képviselők, a német szövetségi parlament, azaz a Bundestag, továbbá a tartományi parlamentek képviselői egységes, mihamarabbi és szigorúbb fellépést sürgetnek a szenzitív adatok védelme, a gazdasági kémkedés, valamint a kiberbűncselekmények büntetési tétele terén, alkalmazkodva ezáltal az EU egyre határozottabb elvárásaihoz is. Ezzel kapcsolatosan már el is készült az a javaslat, amely megfogalmazza az ehhez szükséges jogszabály-módosítások koncepcióját. **Bővebben...**

Egy új, Iránhoz köthető APT csoportról számol be a FireEye

(www.cyberscoop.com)

A FireEye kedden nyilvánosságra hozott jelentésében egy új, kiberkémkedést végző APT csoportról számol be, amely főként a telekommunikációs és utazási ipar terén működő, közel-keleti vállalatok között szedi áldozatait. Az összefoglaló szerint az „APT39” néven hivatkozott kollektíva intenzív adatgyűjtési tevékenysége Irán geopolitikai céljainak megfelelően történik, emellett a támadásokhoz felhasznált eszközök tekintetében is tapasztalható átfedés egyéb iráni kötődésű csoportokéval, mint például az APT33, az APT34, a Newscaster és a Chafer. **Bővebben...**

Január 28. az adatvédelem nemzetközi napja

(www.us-cert.gov)

2019. január 28-a ─ az Európai Tanács kezdeményezésére 2007 óta ─ az adatvédelem napja, amelynek apropóján az adatvédelmi tudatosság népszerűsítésére irányuló programok kerülnek megrendezésre világszerte. Az idei adatvédelmi nap fő témája „az adatvédelem új korszaka” volt, ezzel összhangban az amerikai Nemzeti Kiberbiztonsági Szövetség (NCSA) az adatvédelem jövőjével foglalkozó előadássorozatot szervezett, amelyet élőben figyelemmel lehetett kísérni a Stay Safe Online weboldalon keresztül. **Bővebben...**

Névfeloldási problémák jelentkezhetnek a „DNS flag day” után

(securityweek.com)

Habár az eredeti DNS specifikációt kibővítő Extensions to DNS (EDNS) szabvány előírásai 1999 óta érvényben vannak, azok implementációja nem ment végbe megfelelőképpen DNS kiszolgálói oldalon, emiatt a DNS resolver szoftverek fejlesztői inkább kerülő megoldásokat kezdtek alkalmazni a DNS rendszer zavartalan működésének biztosításához. A legnépszerűbb DNS szoftver (BIND) fejlesztését végző nonprofit szervezet, az Internet Systems Consortium (ISC) álláspontja szerint azonban mindez negatívan befolyásolja többek közt a DNS kérések feldolgozási idejét, illetve megnehezíti az új védelmi megoldások bevezetését. 2019. február 1-je, a „DNS flag day” fordulópontnak ígérkezik e téren, ugyanis egyes DNS resolver gyártók (ISC, CZ NIC, NLNET, PowerDNS), valamint publikus DNS szolgáltatók megállapodtak, hogy ezen időpontot követően ─ a hosszú távú fejlődés érdekében ─ elvetik a fent nevezett megkerülő megoldásokat és megkövetelik az EDNS-megfelelőséget, ami azonban egyúttal azt is jelenti, hogy egyes elavult rendszerek által kiszolgált domain nevek feloldásában problémák jelentkezhetnek. **Bővebben...**

Anti-phishing mobil-alkalmazást ad ki a Netcraft

(www.securityweek.com)

A Netcraft bejelentette, hogy mobilalkalmazást (Netcraft Phishing and Malware Protection) ad ki, amely az adathalászat és egyéb, káros tartalmú weboldalak elleni védelem növelését célozza. A vállalat úgy véli, a népszerű mobil böngészők nem biztosítanak az asztali verziókkal azonos szintű védelmet, ezért a cég úgy döntött, hogy a már 2005 óta működő anti-phishing rendszerét ─ amely több, mint 56 millió egyedi adathalász weboldalt azonosít ─ most a mobilböngészők számára is elérhetővé teszi 28 napig ingyenes, majd havi, vagy éves díj ellenében. Az androidos verzió már letölthető a Google Play Store-ból, és a tervek szerint a közeljövőben iOS-en is megjelenik az applikáció. *(Szerk. megjegyzés: asztali platformon a cég böngésző kiegészítője ingyenesen elérhető.)*

IT biztonsági Tanács

A Microsoft a vállalatoknál dolgozó IT-biztonsággal és kockázatkezeléssel megbízott szakemberek munkájának megkönnyítése érdekében két új platformot hozott létre: a Microsoft 365 security centert, valamint a Microsoft 365 compliance centert. Az előbbi a rendszergazdák számára nyújt lehetőséget a Microsoft 365 intelligens biztonsági megoldásainak használatához, beleértve például az identitás- és hozzáférés-felügyeletet és a fenyegetettség védelmet. A megfelelőségi központ pedig a különböző szabványoknak és szabályoknak (GDPR, ISO 27001, NIST 800-53) való megfelelőség nyomon követését és központi menedzselését teszi lehetővé.

Kibertámadások keresztтüzében az ukrán elnökválasztás

(securityaffairs.co)

Az ukrán kormányzat szerint infrastruktúráik ellen egyre intenzívebb támadásokat indít Oroszország, amelyek a márciusban esedékes ukrán elnökválasztás megzavarására törnek. Serhiy Demedyuk, az ország kiberrendőrségének vezetője a Reutersnek elmondta, jelenleg a támadók célja választási tisztségviselők hitelesítési adatainak megszerzése célzott adathalász támadások útján, illetve sötét webes piacokon keresztül. A hatóságok információi szerint a nemzeti választási rendszerek ellen ugyanakkor még direkt hozzáférési kísérletek nem történtek. Az orosz kormányzati szóvivő kategorikusan cáfolta a vádakat.

Japán feltörheti a lakossági IoT eszközöket, hogy kiderüljön azok mennyire biztonságosak

(zdnet.com)

Japánban jóváhagyták azt a törvénymódosítást, amely lehetővé teszi, hogy az ország Nemzeti Információs és Kommunikációs Technológiai Intézetének (NICT) munkatársai japán felhasználók IoT eszközein ─ például otthoni és vállalati környezetben található routereken és webkamerákon ─ sérülékenység vizsgálati céllal bejelentkezést kíséreljenek meg ismert és könnyen kitalálható jelszavak felhasználásával. A tervek szerint a jövő hónapban induló vizsgálat célja egy nem biztonságos eszközökről készült lista elkészítése, és ennek átadása az illetékes hatóságoknak, valamint az érintett internet szolgáltatóknak, hogy azok értesíthessék a felhasználókat a megfelelő ellenintézkedések megtételéről. **Bővebben...**

Az ENISA szerint Irán fokozni fogja kiber-kémkedési tevékenységét

(www.reuters.com)

Az Európai Unió a 2015-ös atomalku óta első alkalommal érvényesített szankciókat Iránnal szemben, amelynek kapcsán az Európai Unió Hálózat- és Információbiztonsági Ügynöksége (ENISA) arra hívja fel a figyelmet, hogy a közel-keleti ország reakcióként fokozhatja kibertevékenységét geopolitikai és stratégiai célkitűzéseinek elérése érdekében. Az ENISA az európai térség digitális biztonságára nézve az állami támogatású hacker csoportokat értékeli a legnagyobb fenyegetésnek, a gazdasági célú kiberkémkedés kapcsán pedig Irán mellett Kínát és Oroszországot tartja a leginkább potens és aktív szereplőknek. Egy iráni tisztviselő határozottan visszautasította a vádakat, amelyek szerinte illeszkednek az USA és szövetségesei által folytatott Irán ellenes pszichológiai hadviseléshez.

Elkészült a 2018-as év kibereseményeinek értékelése

(www.enisa.europa.eu)

Az ENISA immár hetedik alkalommal készítette el éves fenyegetettségi jelentését, amely a tavalyi év kibereseményeinek tapasztalatait összegzi. A beszámoló kiemelten foglalkozik a 2018-as trendekkel, köztük a káros szoftvereket terjesztő adathalász e-mailekkel ─ mint elsődleges fenyegetési vektorral ─ a kiberbűnözői körökben népszerű kriptovaluta-bányász műveletekkel, illetve az államilag szponzorált hacker csoportok egyre gyakrabban pénzintézeteket célzó támadásaival, valamint az IoT eszközök védelmével kapcsolatban fennálló kérdésekkel. **Bővebben...**