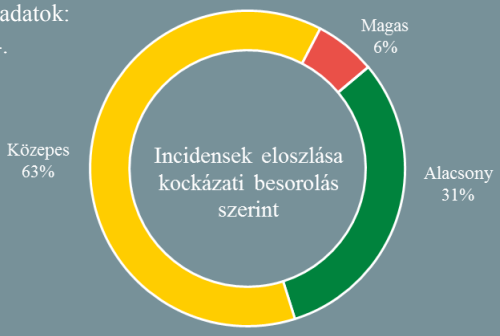
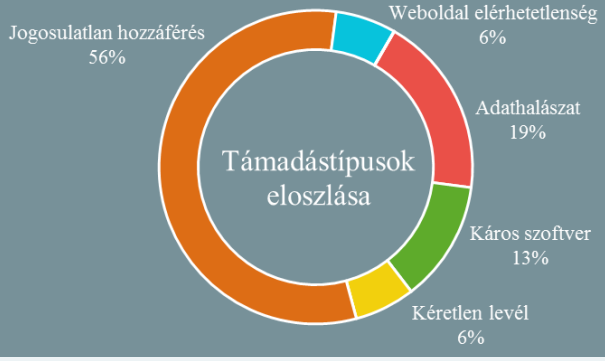
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.02.08. - 2019.02.14.





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

A GDPR első nyolc hónapja számokban

(www.bleepingcomputer.com)

A GDPR hatálybalépése óta több, mint 59 000 adatsértést jelentettek az adatvédelmi hatóságoknak (DPA) az Európai Gazdasági Térségben ─ beleértve Norvégiát, Izlandot és Lichtensteint is ─ hozza nyilvánosságra a DLA Piper jelentésében. A listavezetők Hollandia 15 400, Németország 12 600 és az Egyesült Királyság 10 600 bejelentéssel. Összesen 91-szer került sor pénzbírság kiszabásra, amelyek közül a legmagasabb értékű a Google számára 2019. január 21-én kiszabott 50 millió eurós bírság volt. Több tech vállalat is vizsgálat alá került, a Youtube-ot például a GDPR 15. cikkének (Az érintett hozzáférési joga) megsértésével vádolja az adat- és fogyasztóvédelemmel foglalkozó NOYB (None of Your Business) nonprofit vállalat, amelynek következtében a Google akár 3,87 milliárd eurós büntetésre is számíthat. A hozzáférési jog megsértésének okán mindazonáltal jóval több cég ellen ─ például az Apple, az Amazon, a Netflix, a Spotify, a SoundCloud, a Flimmit és a DAZN ─ nyújtottak be panaszt.

Svájc nyilvános tesztelés alá vonja e-szavazórendszerét

(www.zdnet.com)

A svájci kormány jövőbeli e-szavazási rendszerét nyilvános sérülékenység vizsgálatnak (Public Intrusion Test ─ PIT) veti alá 2019. február 25. és március 02-a között, amelyre bárki jelentkezhet. A felfedezett sebezhetőségekért pénzjutalom jár, amelynek összege attól függően változik, hogy a rendszer milyen fokú kompromittációja valósítható meg általa. Eszerint egy sikeres jogosulatlan hozzáférés 1 000 dollárt, azonban a szavazatok nem detektált manipulációja már 30-50 000 dollárt is érhet. **Bővebben...**

Lengyelország új kiberhadműveleti szervezet létrehozását jelentette be

(thenews.pl)

Mariusz Błaszczak lengyel védelmi miniszter a varsói Cyber.mil.pl konferencián nyilvánosságra hozta, hogy Lengyelország új kibervédelmi katonai szervezetet hoz létre az ország informatikai támadásokkal szembeni ellenálló képességének növeléséhez, ennek megalakításáért pedig Karol Molenda ezredes felel, a lengyel katonai elhárítás egy korábbi információbiztonsági szakértője. Błaszczak hangsúlyozta, hogy az intézkedés a NATO elvárásaival összhangban kerül megvalósításra.

Népszámlálás Németországban: A szövetségi alkotmánybíróság engedélyt adott az éles adatokkal való tesztre

(heise.de)

Karlsruheban helyi bírósági szinten elutasításra került az az indítvány, amelyet egy jogvédő szervezet (GFF) nyújtott be annak érdekében, hogy megakadályozzák a 2021-ben esedékes összeírás valós neveket felhasználó informatikai tesztüzemét. Az ügy folytatásaként a szövetségi alkotmánybíróság is vizsgálódott, azonban nem talált kivetnivalót a szóban forgó teszt kapcsán. Az indoklás szerint a népszámlálás megfelelő előkészítéséhez fűződő jogalkotói érdek erősebb, mint az esetleges kockázatokat jelentő teszteljárás elhagyása az adatvédelemre tekintettel. Figyelemmel arra, hogy Németország köteles az Európai Bizottság felé statisztikai adatokat szolgáltatni a tervezett népszámlálás kapcsán, a tesztüzem realizálása elengedhetetlen a bíróság szerint, még akkor is, ha az ennek során megvalósuló adatkezelés neveket, lakcímeket, nemi besorolást, családi állapotot, felekezeti hovatartozást, valamint ehhez kapcsolódóan két éves adattárolást tartalmaz. **Bővebben...**

Beépített VPN-t kap az Opera böngésző Androidon

(www.theverge.com)

Az Opera androidos verziója beépített VPN funkcióval gazdagodik, védelmet nyújtva a felhasználók webes böngészésének harmadik fél általi monitorozásával szemben ─ nem csupán ─ nyilvános Wi-Fi hálózaton. A jelenleg még béta verzióban lévő VPN funkció több manuális beállítási lehetőséggel rendelkezik, például megadható, hogy melyik kontinensen lévő szerveren keresztül haladjon a forgalom, beállítható, hogy csak a privát böngészés során megnyitott weboldalakon kerüljön alkalmazásra, valamint opcionálisan kikapcsolható az internetes keresések során, a találati relevancia növeléséhez. A cég közleménye szerint nem fogják logolni a felhasználók tevékenységét, mindazonáltal felhívják a figyelmet arra, hogy a szolgáltatás igénybevétele a böngészés sebességére hatással lehet. Egyelőre iOS-es verzió lehetőségére nem tértek ki.

IT biztonsági Tanács

Kutatók demonstrálták, hogy megfelelő ─ az Amazon felhőben körülbelül 25 dollárért bérelhető ─ számítási kapacitás mellett a nyílt forráskódú HashCat jelszótörő program a 8 karakter hosszú, Windows környezetekben potenciálisan még mindig alkalmazott NTLM hash jelszavakat körülbelül 2,5 óra alatt töri fel, függetlenül azok komplexitásától. Habár a NIST ajánlásában továbbra is a minimum 8 karakteres, bonyolult jelszavak használata szerepel, és a modernebb titkosító algoritmusok nehezebben törhetőek, javasolt inkább több (ideálisan 4-5) szóból álló jelszómondatok alkalmazása. *(Forrás: TheRegister)*

A Brave böngésző nem blokkolja a Facebook és a Twitter nyomkövető szkriptjeit

(www.bleepingcomputer.com)

Az Y Combinator Hacker News blogbejegyzésében arról ír, hogy a ─ magát a nyomkövető kódok blokkolásával reklámozó ─ Brave Browser a Facebook és Twitter kódjaival kivételt tesz. A Brave böngésző fejlesztői egy GitHub-os bejegyzés tanúsága szerint még 2016 augusztusában döntöttek így, egy későbbi hibajegyben arra hivatkozva, hogy a kérdéses nyomkövető szkriptek blokkolása számos webhely működésére hatással lehet, például a facebookos bejelentkezési funkciók nem működnek. **Bővebben...**

Több, mint 14 millió Instagram felhasználó profiladatait tartalmazó adatbázist fedeztek fel

(cyberscoop.com)

Oliver Hough, biztonsági kutató a Shodan segítségével felfedezett egy nyíltan hozzáférhető adatbázist, amely instagramos felhasználók adatait (nevek, azonosítók, képekre mutató linkek) tartalmazta ─ adja hírül a Cyberscoop. Hough szerint az adathalmazt célzott marketing tevékenységre, vagy ─ gyakran használt jelszavakkal párosítva ─ akár a fiókok elleni támadásokhoz is felhasználhatják. A Cyberscoop publikációjának megjelenéséig az Instagram nem reagált az esetre.

ENISA-s online felület a biztonságos mobilalkalmazás fejlesztés támogatásáért

(www.enisa.europa.eu)

Az ENISA interaktív felületet hozott létre a még 2017. február 10-én közzétett „Biztonságos fejlesztői útmutató okostelefonokhoz" című kiadványa alapján, amelyben a kritikus fontosságú biztonsági intézkedések ─ felhasználói hitelesítés, szenzitív adatok védelme, biztonságos szoftver disztribúció, stb. ─ kerültek megjelenítésre. A SMAShiNG elnevezésű online eszköz a fejlesztőknek nyújt kellő támogatást a biztonságos mobilalkalmazások létrehozásában, platformtól függetlenül. **Bővebben...**

Új közösségi platform a NATO szövetséges tagállamok kibervédelmi felelősei számára

(nato.int)

A NATO szövetség tagjai információcserére, legjobb gyakorlatok megosztására és további együttműködésre használhatják az új, biztonságos közösségi platformot, amelyet 2019. február 12-én állított élesbe a NATO technológiai fejlesztésekért felelős szervezete, az NCI Agency. Eddig öt ország (Belgium, Franciaország, Hollandia, Egyesült Királyság, és az Egyesült Államok) számítógépes vészhelyzeti reagáló csoportja (CERT) tartozik a hálózathoz, azonban az ígéretek szerint még idén minden tagország lehetőséget kap a csatlakozásra. **Bővebben...**

Kibertámadás érte a máltai Bank of Vallettát

(securityweek.com)

Málta legnagyobb bankja informatikai támadás áldozatává vált, amelynek során a támadók mintegy 13 millió eurónyi összeget igyekeztek megszerezni ─ jelentette be az ország miniszterelnöke. A többségében állami tulajdonban lévő Bank of Vallettának a biztonsági esemény következtében le kellett állítania rendszereit, beleértve a pénzkiadó automatákat, valamint a mobil és internetes bankolást is. **Bővebben...**