

Az NKI által kezelt incidensek-
re vonatkozó statisztikai adatok:
2019.03.08. - 2019.03.13.



Kövessen minket megújult [weboldalunkon](#), ahol friss IT-biztonsági hírek kerülnek publikálásra!

Venezuela szerint az Egyesült Államok a felelős a múlt hét óta tartó áramszünetért ([securityaffairs.co](#))

Jorge Rodriguez, Venezuela kommunikációs minisztere szerint egy Egyesült Államok által indított kibertámadás okozta a Guri erőmű múlt heti súlyos meghibásodását, amelynek következtében az ország 23 államából 22-ben jelenleg is áramszünet van, a vád alátámasztására pedig bizonyítékokat kíván a napokban a helyszínrre látogató emberi jogi ENSZ főbiztos elé tární. Mike Pompeo amerikai külügyminiszter Twitter üzenetben reagált a vádra, amelyben úgy fogalmaz, hogy nem az USA, vagy más állam a felelős a Venezuelában uralkodó krízis állapotokért, hanem a Maduro-rezsim inkompetenciája.

A felhasználói engedélyek kikényszerítése nem felel meg a GDPR-nak ([www.bleepingcomputer.com](#))

A holland Adatvédelmi Hatóság (DPA) múlt heti közleményében arra hívta fel a figyelmet, hogy azok a weboldalak, alkalmazások, illetve szolgáltatók, akik kizárólag a nyomkövető cookie-k (sütik) elfogadásával engednek hozzáférést tartalmukhoz, nem felelnek meg az EU általános adatvédelmi rendeletének (GDPR). A GDPR egyértelműen meghatározza, hogy adatkezelés kizárólag a felhasználók egyértelmű és önkéntes engedélyével végezhető, egyes szolgáltatók viszont csak akkor engednek hozzáférést tartalmaikhoz, ha a felhasználó elfogadja a weboldal működéshez nem feltétlenül szükséges sütik (például a nyomkövető cookie) használatát. Mivel ilyen esetekben a felhasználó nem tagadhatja meg az engedélyt bizonyos következmények (például a tartalom megtekintésének korlátozása) nélkül, nem valósul meg a GDPR követelményei szerint meghatározott felhasználói önkéntesség.

A Facebook adatlopással vádolja ukrán fejlesztőit ([www.theverge.com](#))

A Facebook pert indított két ukrán férfi – Gleb Sluchevsky és Andrey Gorbachov – ellen, mivel Facebook adatokhoz felhatalmazás nélküli hozzáférés megvalósításával megsértették a számítógépes csalásról és visszaélésről szóló törvényt, valamint megszegtek a Facebookkal kötött szerződést azáltal, hogy jogszerű Facebook-fejlesztőknek adták ki magukat. 2017 és 2018 között, mintegy 63 000 Facebook felhasználót vettek rá káros kódokat tartalmazó böngészőbővítmények telepítésére. A két férfi állítólag négy webalkalmazást működtetett, köztük a Supertest-et és az FQiuzt, amelyek olyan személyiségi tesztek ajánlottak főleg orosz és ukrán felhasználók számára, mint a „Ki vagy a modern vámpírok közül?” vagy a „Ki a Te múltbéli hasonmásod?”, hasonlóan a „Mennyi királyi vér csörgedezik az ereidben?” kvízekhez. **Bővebben...**



Mostantól a Windows 10 automatikusan eltávolítja a problémát okozó frissítéseket ([thehackernews.com](#))

Egy nappal a márciusi hibajavító csomag közreadása előtt a Microsoft [közleményben](#) tudatta, hogy a Windows 10 kapcsán egy új biztonsági megoldást vezet be, miszerint automatikusan törölni fogja a rendszerindítási problémákat okozó frissítéseket, azonban mindezt csak abban az esetben kerül majd sor, amennyiben minden más helyreállítási folyamat kudarcot vallott. A törlés mellett a funkció 30 napig meg is akadályozza majd a kérdéses frissítés telepítését, időt adva a Microsoftnak a hiba kijavítására.

A WhatsApp új funkcióval segítené a manipulált képek felismerését

(www.engadget.com)

A WhatsApp egy beépített képkereső bevezetésén dolgozik, amely jelenleg csak a csevegő alkalmazás 2.19.73-as (béta) verziójában érhető el, és lényegében a Google képkeresőjének integrálása. Célja, hogy a felhasználók egyszerűen rákereshessenek egy üzenetben kapott képre, a találatok alapján pedig könnyebben dönthessenek annak eredetiségéről. Még nem tudni, hogy az álhírek és dezinformációk elleni küzdelemben hasznosnak ígérkező funkció mikortól válhat élessé.

Adatvédelmi hiánypótlások várhatóak az új Androidban

(www.engadget.com)

Már elérhető az Android Q béta verziója, az Engadget szerint pedig a funkcionális újítások mellett a Google végre az adatbiztonságra is nagyobb hangsúlyt fektet. A következő Android kiadásban többszintű korlátozási lehetőség lesz elérhető a felhasználók számára, például a helyadatok alkalmazások által történő gyűjtésére, vagy az alkalmazások média tartalmakhoz, valamint eszközazonosítókhoz (IMEI, sorozatszám) történő hozzáférésére vonatkozóan.

IT biztonsági Tanács



A Google nem várt módon [bővítette](#) az alapértelmezett elérhető internetes keresőmotorok listáját a Chrome böngésző új, 73-as verziójában. Ennek köszönhetően a privát adatok biztonságát szem előtt tartó [DuckDuckGo](#) alapértelmezett keresőmotorként történő beállítása a korábbiakhoz képest jóval egyszerűbbé vált, csupán egy kattintás a <chrome://settings/searchEngines> alatt.

Kutatók kritikus sérülékenységet találtak a svájci online szavazórendszerben

(motherboard.vice.com)

Még zajlik a nyilvános hibakereső program, egy nemzetközi kutatókból álló csoport máris komoly biztonsági problémát fedezett fel a svájci elektronikus szavazórendszerben, amellyel a szavazatok a rendszeren belülről észrevétlenül manipulálhatóak. A biztonsági kitétség egy korszerű kriptográfiai koncepció (Zero-knowledge proof) hibás implementálásából fakad, amely a szavazatok eredetiségét hivatott garantálni a többlépcsős feldolgozás során. A biztonsági rést felfedező kutatók értesítették a rendszert fejlesztő Swiss Postot, akik közleményükben megerősítették ugyan a sérülékenység tényét, azonban a biztonsági kockázatot alacsonyabbnak ítélték, arra hivatkozva, hogy egy kihasználó támadáshoz a támadóknak előbb a Swiss Post IT infrastruktúráján kellene irányítást szerezniük, ráadásul speciális ismeretekkel rendelkező belső munkatársak segítségre is szükségük lenne. **Bővebben...**

1,37 millió euró a Windows 10 biztonsági elemzésére a német Sisyphus projekt keretében

(www.heise.de)

A német szövetségi információtechnikai-biztonsági hivatal (BSI) 1,37 millió euró költséggel részletes biztonsági vizsgálatokat végzett a Microsoft Windows 10 tekintetében annak érdekében, hogy felmérjék, mennyire nyújt biztonságos alkalmazási feltételeket a szóban forgó operációs rendszer. Az első eredményeket már tavaly novemberben nyilvánosságra is hozták, amely több komponenselemzést tartalmazott (TPM, PowerShell, Update-funkció, stb.); ezen adatok különösen fontosak a közigazgatásban alkalmazott programok használatát tekintve. **Bővebben...**

A ProtonMail is felkerült az orosz tiltólistára

(techcrunch.com)

Egy orosz nyelvű blog [információi szerint](#) a Szövetségi Biztonsági Szolgálat (FSB) elrendelte számos e-mail szolgáltató – köztük a ProtonMail – tiltását, arra hivatkozva, hogy a szolgáltatások megkönnyítik a robbantásos fenyegetések kivitelezését. Az intézkedés hátterében az áll, hogy januárban jelentősen nőtt a rendőrséghez e-mailek keresztül beérkezett névtelen bombafenyegetések száma, amelyek miatt a hatóságoknak több iskolát és kormányzati építményt is evakuálniuk kellett. Az FSB rendelete szerint összesen 26 internetes cím került blokkolásra azonnali hatállyal, köztük Tor szerverek is, amelyeket a felhasználók a cenzúra megkerülésére használtak. **Bővebben...**

Szigorítanak a gyermekek online adatvédelméről szóló törvényt az Egyesült Államokban

(engadget.com)

Ed Markey and Josh Hawley amerikai szenátorok módosítási javaslatot nyújtottak be a gyermekek online adatvédelméről szóló törvény (COPPA – Children's Online Privacy Protection Act) vonatkozásában, amellyel szigorúbb ellenőrzés alá vonnák a kiskorúak adatainak kezelését. A törvénymódosítással tiltanak a gyermekek számára célzott hirdetések alkalmazását, lehetővé tennék a gyermekek és szülők adatainak törlését, valamint továbbra is tiltanák a 13 éves kor alatti gyermekek adatainak szülői engedély nélküli, illetve a 13-15 év közötti gyermekek adatainak felhasználói beleegyezés nélküli gyűjtését. **Bővebben...**