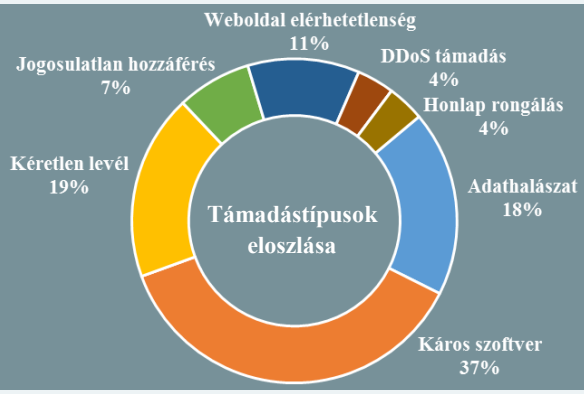
Incidens adatok: 2018.19. — 2018.01.25.



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

A Gmail felhasználók csupán 10%-a használja a kétfaktoros azonosítást

(www.forbes.com)

A Gmail az egyik legnépszerűbb levelező szolgáltatás, mely több millió felhasználóval rendelkezik. Sok felhasználó a Gmailt használja elsődleges e-mail címnek, valamint egyéb online szolgáltatások elérésére, többek között a Facebook és a különböző online banki szolgáltatások. A széleskörű elterjedése miatt különösen fontos a felhasználói fiókok megfelelő védelme. A Google már évek óta rendelkezésre bocsátotta a kétlépcsős azonosítás lehetőségét, melynek köszönhetően a jelszavakon kívül lehetőség van egy SMS-ben érkező biztonsági kód megadására, így növelve a felhasználói fiókok védelmét. Ennek ellenére a felhasználók 90%-a nem alkalmazza a biztonsági szolgáltatást, melynek leggyakrabban említett okai, hogy túl bonyolult elvégezni a szükséges beállításokat, valamint néhányan aggódnak a lehetséges adatvédelmi problémák miatt is. Tapasztalatok alapján erősen ajánlott a kétlépcsős azonosítás bekapcsolása, melyhez segítséget nyújt a Google Súgó oldalán található tájékoztató leírás, mely magyar nyelven is elérhető. **Bővebben...**

DuckDuckGo Privacy Essentials

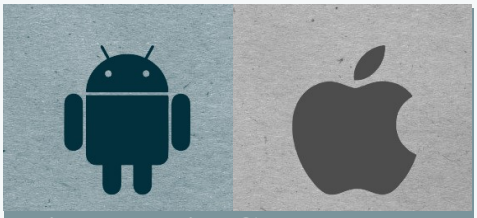
(www.helpnetsecurity.com)

Új böngészőbe telepíthető bővítménnyel és mobilalkalmazással jelentkezik a DuckDuckGo internetes kereső vállalata, a DuckDuckGo Privacy Essentials-al. Az újítások szerint a DuckDuckGo mostantól alapértelmezett keresőmotornak is beállítható, erősíti a weboldalak titkosított (HTTPS) verziójának használatát, valamint tiltja az összes harmadik féltől származó adatgyűjtő tevékenységet, melyről egy listát is készít a felhasználók számára. Információt gyűjt a felhasználó által felkeresett weboldalak felhasználási feltételeiről és adatvédelmi irányelveiről, melyeket a Terms of Service Didn't Read (TOSDR) weboldal eredményei alapján értékel. A DuckDuckGo alapítója Gabriel Weinberg megjegyezte, hogy az új bővítmény használatának következtében hamar észre lehet venni, hogy jelenleg nagyon kevés weboldal kapott „A" minősítést a TOSDR weboldalán. Az új bővítmény és alkalmazás Firefox-on, Safari-n, Chrome-n, iOS-en és Android-on is elérhető, továbbá a forráskód megtalálható a GitHub-on. **Bővebben...**

Így reagál a Facebook a GDPR-ra

(www.reuters.com)

Sheryl Sandberg, a Facebook közösségi hálózat vezérigazgatója egy brüsszeli Facebook eseményen jelentette be, hogy a cég a májusban hatályba lépő Európai Unió Általános Adatvédelmi Rendeletének (GDPR) személyes adatok védelmére vonatkozó követelmények megfeleléséhez egy új, globális szintű adatvédelmi központot hoz létre, melyben a Facebook adatvédelmi beállításait egy helyen tárolja, ezzel egyszerűbbé téve az adatkezelést a több mint 2 milliárd Facebook felhasználó számára. "Az alkalmazásaink régóta arra fókuszálnak, hogy átláthatóságot és ellenőrizhetőséget nyújtsanak az embereknek, mely megfelelő alapot biztosít számunkra a GDPR megfelelési kötelezettségeihez, valamint arra ösztönöz bennünket, hogy továbbra is olyan termékekbe és oktatási eszközökbe invesztáljunk, amelyek hozzájárulnak a magánélet védelméhez." - mondta Sandberg. Sandberg azt is elárulta, hogy a cég azt tervezi, megduplázza a biztonsági terület munkatársainak számát év végéig, valamint a jövőben nagyobb hangsúlyt kívánnak fektetni a hamis hírek és a gyűlöletbeszéd megakadályozására is. **Bővebben...**



Biztonsági PCI szabványt kap a mobil Point of Sale

(www.theregister.co.uk)

A PCI SSC (Payment Card Industry Security Standards Council) biztonsági szakemberei aggodalmukat fejezték ki amiatt, hogy a mobil point-of-sale (MPOS) rendszerek nem felelnek meg a kereskedelmi forgalomban használt bankkártya terminálok szigorú hardver követelményeinek, ezért bejelentettek egy új szabványt a kereskedők számára, ami javaslatot tesz arra vonatkozóan, hogy a fogyasztók kompromittálódás nélkül legyenek képesek fizetni a PIN kód használatával mobil eszközeiken keresztül is. A szabvány négy kulcsfontosságú alapelve: a szolgáltatás folyamatos monitorozása; a PIN kód más számlaadatoktól történő elkülönítése; a szoftver és a PIN-beviteli alkalmazás integritásának biztosítása a common off-the -shelf (COTS) eszközön; valamint a PIN - és fiókadatok védelme a PCI által jóváhagyott biztonságos kártyaolvasó (SCRP) használatával, mely titkosítja a tranzakciós kapcsolatokat. A szabvány tartalmaz egy vizsgálati követelményekre vonatkozó dokumentumot is, melynek közzététele februárra várható. **Bővebben...**

IT biztonsági Tanács

A laptopok működés közben hőt termelnek, mely ha meghaladja az optimális üzemi hőmérséklet szintjét, a készülékek lassulásához, illetve lekapcsolásához vezethet, amely adatvesztéssel járhat.

Ennek elkerülése érdekében javasoljuk a laptopok legalább évenkénti belső tisztítását, valamint hőmérséklet ellenőrző szoftverek használatát. A készüléket igyekezzünk egy egyenes, sík felületen használni.

Az Egyesült Királyságban is gondot okoz a titkosítás

(www.theregister.co.uk)

Theresa May brit miniszterelnök ismételten felszólította az IT szakembereket, hogy dolgozzanak ki egy olyan titkosítási eljárást, amellyel a bűnüldöző szervezetek hozzáférhetnek a felhasználók titkosított kommunikációjához. A Svájcban megrendezésre került Világgazdasági Fórumon (WEF) a miniszterelnök a technológia előnyeiről és hátrányairól tartott beszédében, megemlítette a különféle platformok szélsőséges tartalmaira vonatkozó szabályzás kidolgozásának szükségességét. A probléma középpontjába a végponttól végpontig terjedő titkosítást alkalmazó szoftverek állnak, ahol még az alkalmazás fejlesztői sem képesek dekódolni és olvasni a felhasználók közötti titkosított üzeneteket. Christopher Wray az Amerikai Egyesült Államok Szövetségi Nyomozó Irodájának (FBI) igazgatója a hónap elején szintén arról beszélt, hogy olyan törvénymódosításra és eszközkialakításokra van szükség, amelyek lehetővé teszik az adatbiztonságot amellett, hogy – bírósági végzéssel – a hatóságok számára hozzáférést biztosítanak az adatokhoz. A biztonságtechnikai szakemberek szerint az ilyen titkosítási eljárás kialakításában az okoz nehézséget, hogy nem képesek olyan hátsó ajtót biztosítani, amelyet csak és kizárólag a hatóságok vesznek igénybe, mert idővel a hackerek és bűnözők is felhasználhatják káros tevékenységeik során. **Bővebben...**

Kétfaktoros azonosítás a Reddit fiókokhoz

(www.bleepingcomputer.com)

Napjainkban egyre gyakoribb az adatok illetéktelenek számára való megismerése, a jelszavak újbóli felhasználása, illetve a gyenge jelszavak alkalmazása, ezért a felhasználói fiókok biztonságának növelése érdekében, a Reddit kétfaktoros azonosítással (2FA) plusz védelmi vonalat biztosít felhasználói számára. A korábban már béta verzióban működő hitelesítés (2FA), most minden felhasználó számára elérhetővé vált, amelynek köszönhetően a felhasználóknak a Reddit fiókba történő belépése során jelszavukon kívül, egy mobil hitelesítési alkalmazásban megjelenő kódot is szükséges megadniuk. Ennek aktivitására a regisztrációt követően van lehetőség. **Bővebben...**

Innovatív együttműködés az IoT eszközök biztonsága érdekében

(www.iotbusinessnews.com)

Az Entrust Datacard és a Schneider Electric partnerségének eredménye, hogy ügyfeleik számára lehetőség van az IoT (tárgyak internete) eszközöknél az identitás alapú biztonság használatára. Az Entrust Datacard – a megbízható identitás és biztonságos tranzakciós megoldások vezető szállítója – bejelentette, hogy csatlakozik a Schneider Electric együttműködési automatizálási partner programjához (CAPP - Collaborative Automation Partner Program). Ez az együttműködés lehetővé teszi a Schneider Electric – az automatizálás és energiagazdálkodási rendszerek piacvezetője – számára, hogy ügyfelei részére elérhetővé tegye az Entrust Datacard ioTrust biztonsági megoldását. Az ioTrust biztonsági megoldás megbízható infrastruktúrát hoz létre az M2M (machine to machine) adatok továbbításához, így csökkenti a biztonsági kockázatot, és növeli az átláthatóságot az ipari környezetekben. A CAPP további előnye a Schneider Electric számára, hogy a cég EcoStruxure for Industry architektúráján keresztül teljes vállalati biztonságtechnikai üzleti megoldásokat szállíthat a partnerei részére. **Bővebben...**