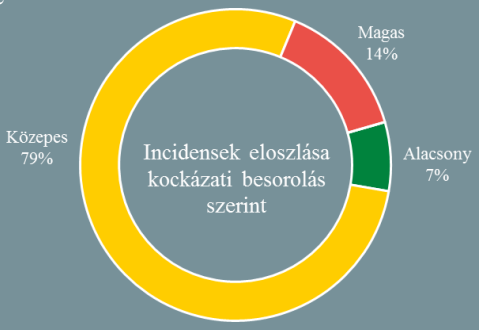
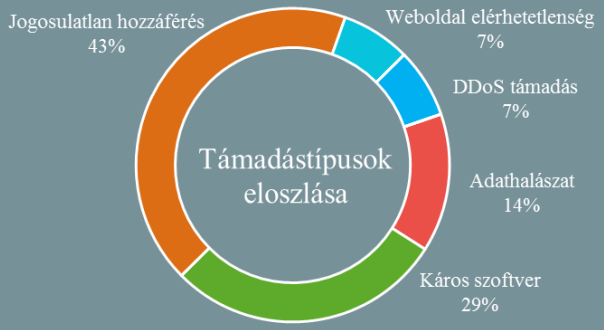
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 17. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.04.18. - 2019.04.25.





Kövessen minket megújult weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

Hatalmas biometrikus adatbázis létrehozásáról szavazott az EU

(zdnet.com)

Az Európai Parlament múlt héten szavazta meg a személyazonosításra alkalmas adatokat tartalmazó közös adatbázis (Common Identity Repository - CIR) létrehozását, amely több rendészeti adatbázis összekapcsolásából jön majd létre, és a személyazonosítási adatok (név, születési dátum, útlevélszám és egyéb azonosítók) mellett biometrikus azonosítókat is tartalmaz majd. A jövőben több mint 350 millió emberre vonatkozó információkat tartalmazó adatbázishoz az Uniós határrendészeti és a bűnüldöző hatóságok férnek majd hozzá, így a különböző nyilvántartások helyett egy egységes adatbázisból kereshetik ki a szükséges adatokat. Az összevonni kívánt nyilvántartások között szerepel a Schengeni Információs Rendszer (SIS), a határokon és a tagállamokban illegálisan tartózkodó menedékkérők és harmadik országbeli állampolgárok európai ujjnyomat-azonosító rendszere (EURODAC), az uniós szintű Vízuminformációs Rendszer (VIS), valamint további három új rendszer. Ezek a harmadik országbeli állampolgárok bűnügyi nyilvántartására vonatkozó európai információcsere-rendszer (ECRIS-TCN), az Európai Határregisztrációs Rendszer (EES), valamint az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS).

Az ASUS csak egy volt a „ShadowHammer” művelet célpontjai közül

(bleepingcomputer.com)

A Kaspersky szerint nem csak az ASUS-t érintette a nemrég felfedezett, „Operation ShadowHammer”-ként hivatkozott malware támadási kampány, biztonsági kutatók ugyanis további hat cégnél fedeztek fel nagyon hasonló káros kódokat és fertőzési mechanizmusokat. Az új áldozatok között szerepel három ázsiai játékgyártó cég (Electronics Extreme, Innovative Extremist és a Zepetto) valamint további három — mindeddig nem megnevezett — dél-koreai vállalat. **Bővebben...**

Hibát fedeztek fel a nemrég bemutatott francia kormányzati privát üzenetküldő alkalmazásban

(thehackernews.com)

A Tchap nevű, nyílt forrású és végponti titkosítást alkalmazó csevegő alkalmazást a francia kormányzat fejlesztette ki annak a kezdeményezésnek a részeként, hogy a kormányzati dolgozók adatai kizárólag az országon belüli szervereken kerüljenek eltárolásra — tartván a külföldi hírszerzéstől. Bár az alkalmazás androidos változata a Google Play Store-ból bárki számára letölthető, csak meghatározott hivatali e-mail címmel rendelkezők (pl.: @gouv.fr or @elysee.fr) regisztrálhatnak fiókot. **Bővebben...**

Adatszivárgásról tájékoztatja ügyfeleit a Bodybuilding.com

(www.bleepingcomputer.com)

Egy februári biztonsági eseményről tájékoztatta ügyfeleit a Bodybuilding.com, amely szerint 2018 júliusában illetéktelenek hozzáférhettek ügyfeleik egyes személyes adataihoz, mint például nevük, e-mail címük, szállítási és számlázási címük, rendelési előzményeik, illetve telefonszámuk. Hitelkártya adatok szerencsére nem szivárogtak ki, köszönhetően annak, hogy a weboldal csak a kártyaszám utolsó négy számjegyét őrzi meg, és ezt is kizárólag azoknál a felhasználói profiloknál, amelyeknél az ügyfelek engedélyezték azok tárolását. A Bodybuilding.com a hatóságok és egy eddig meg nem nevezett „piacvezető biztonsági cég” szakértőinek segítségével igyekszik felderíteni az incidenst, illetve azonosítani a kihasznált sérülékenységeket. **Bővebben…**

Az NSA már leállítaná a telefon lehallgatási programját

(www.engadget.com)

Az Amerikai Egyesült Államok Nemzetbiztonsági Ügynöksége (NSA) kész befejezni a telefonos kommunikációk tömeges megfigyelését, mivel a fenntartásával járó logisztikai és jogi nehézségek jelentősen meghaladják a programból származó hírszerzési előnyöket. A telefon lehallgatási program a 2001. szeptember 11-i támadások után kezdte meg működését, ekkoriban a terrorizmus utáni hajsza során naponta több milliárdnyi telefonhívásra és szöveges üzenetre vonatkozó adatot gyűjtött. A program Edward Snowden 2013-as szivárogtatása kapcsán kapott nagy nyilvánosságot, majd 2015-től alacsonyabb fokozatba kapcsolt, miután az Egyesült Államok Kongresszusa elfogadta a „USA Freedom Act”-et, amely néhány százmillióra redukálta az éves szinten begyűjthető adatok számát. Luke Murry, a Republikánus Párt nemzetbiztonsági tanácsadójának elmondása szerint az NSA különböző technikai és megfelelési problémák miatt az utóbbi fél évben pedig már gyakorlatilag nem is használta a rendszert. A program leállításával kapcsolatban a Fehér Ház határozhat, azonban a hírek szerint még a mögöttes jogszabály megújításáról sem született döntés.

IT biztonsági Tanács

A holland kibervédelmi intézet ajánlásokat adott ki a szervezetek számára a biztonságos webes kommunikációt megvalósító Transport Layer Security protokoll (TLS) implementálásához. Az anyag röviden bemutatja a TLS-sel kapcsolatos legfontosabb alapvető tudnivalókat és segítséget nyújt a megfelelő konfigurációk kiválasztásához.

Lényegesen több Instagram felhasználó jelszavához férhetnek hozzá a Facebook alkalmazottai

(theverge.com)

A Facebook egy márciusi közleményében arról adott tájékoztatást, hogy egyes ügyfeleinek jelszavai titkosítatlan formában kerültek tárolásra. Az érintett ügyfélkörről szólva eredetileg azt közölték, hogy több száz millió Facebook Lite, több tíz millió Facebook, valamint több tízezer Instagram felhasználót fognak kiértesíteni. A közleményt azonban a múlt héten frissítették, eszerint az érintett Instagram felhasználók száma jóval nagyobb, több millióra tehető. Az esetről először Brian Krebs biztonsági szakértő írt blogján, amelyből kiderült, hogy a probléma már 2012 óta fennállt, ahogy az is, hogy több, mint 20 000 Facebook alkalmazott férhetett hozzá a jelszavakhoz. A tech cég nem sokkal később kiadott közleménye sietett hangsúlyozni, hogy a jelszavak csak a vállalat belső rendszerein keresztül voltak elérhetőek, a problémát sikeresen elhárították, és nem találtak arra utaló nyomot, hogy a jelszavakhoz bárki illetéktelenül hozzáfért volna.

Zsarolóvírussal támadnak sérülékeny Confluence szerverekre

(csoonline.com)

Támadók a Confluence nevű kollaborációs szoftver kritikus biztonsági hibáját (CVE-2019-3396) kihasználva GandCrab zsarolóvírust kezdtek terjeszteni a sérülékeny szervereken, az Alert Logic elemzése szerint egy április 10-én nyilvánossá vált kihasználási módszert (proof-of-concept exploit) felhasználva. A tavaly feltűnt GandCrab zsarolóvírus jelenleg az egyik legnagyobb fenyegetést jelentő káros szoftver. Eddig ez a ransomware jellemzően e-mailek csatolmányában található fertőzött Office dokumentumokon keresztül okozott fertőzést, a most megfigyelt támadási módszer ─ azaz a szerver sérülékenységek kihasználása ─ pedig inkább kriptovaluta bányász programok terjesztésére volt használatos. **Bővebben...**

Korszerűbb titkosítási algoritmusra vált a ProtonMail

(protonmail.com)

A ProtonMail bevezeti az elliptikus görbékre épülő kriptográfia (Elliptic Curve Cryptography – ECC) használatát az e-mail üzenetek titkosítása során. Mindez azért lényeges, mert jelenleg az ECC számít a legfejlettebb titkosítási eljárásnak, amely az eddig leggyakrabban használt RSA-hoz képest gyorsabb műveletvégzést tesz lehetővé, megegyező, vagy magasabb biztonság garantálása mellett. Az RSA algoritmus nagy hátránya ugyanis, hogy az ECC-vel ellentétben a számítási kapacitások ugrásszerű növekedésével a titkosítás biztonságát csak nagyobb prímszámok alkalmazásával képes garantálni, ami azonban a titkosítási művelet idejét növeli. **Bővebben...**

Az Európai Parlament jobban kívánja védeni a botrányos esetek kiszivárogtatóit

(heise.de)

Egy, az Európai Parlament által nagy többséggel elfogadott új szabály szerint a korrupciós esetek, gazdasági visszaélések felfedői – alapos gyanú fennállta esetén – a jövőben könnyebben tudnának a nyilvánosság elé lépni a közérdek védelme érdekében. Az irányadó szabályozás értelmében minden uniós tagállamban közös alapnormák fogják szabályozni azon személyekkel összefüggő rendelkezéseket, akik az uniós normák megszegéseit bejelentik. Ennek keretében minden ilyen esetben, ha egy személyt a normaszegés jelentése okán bármilyen fenyegetés érné munkahelyén, akkor közvetlenül a sajtónyilvánossághoz fordulhat majd. **Bővebben...**