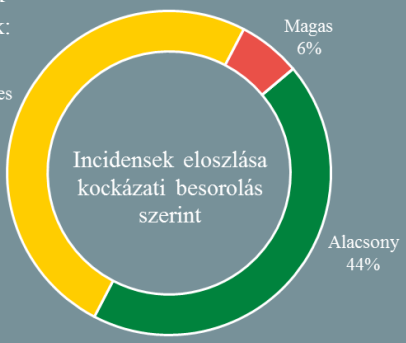
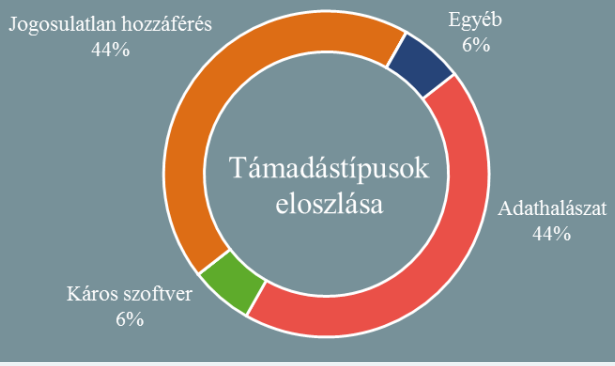
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.02.28. - 2019.03.07.





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

Irán állhat az ausztrál parlament elleni támadás mögött?

(www.scmagazine.com)

A Resecurity vizsgálatot indított az ausztrál parlament számítógépes rendszere ellen irányuló kibertámadás kapcsán, amely minden bizonnyal az Iridium hackercsoport nevéhez köthető. Az offenzíva első szakaszára még 2018. december 23-án, a második szakaszra pedig 2019 februárjában került sor, amelynek eredményeként a támadók hozzáférést szereztek a kormányzati hozzáférési listához (GAL). Bár a cég nem állítja, hogy a csoport egyértelmű kapcsolatban áll Iránnal, minderre csupán közvetett bizonyítékokat tártak fel, többek között azt, hogy a kollektíva által alkalmazott támadási technikák szinte teljesen megegyeznek a Mabna (iráni állami hackercsoport) és más, az Iszlám Forradalom Gárdájának hadserege által alkalmazott módszerekkel. **Bővebben...**

Kanada: Szigorúbb szabályzás a politikai hirdetésekre vonatkozóan

(www.engadget.com)

A szövetségi választások előtt a Google az összes politikai témájú hirdetést letiltja Kanadában. A kanadai kormány még 2018 decemberében fogadta el azt a törvényjavaslatot, amely arra kényszeríti az online platformokat, hogy nyilvántartást vezessenek a választási időszakban közvetve vagy közvetlenül megjelenített politikai hirdetésekről. A törvényjavaslat elfogadását megelőzően a tech óriás módosítási javaslattal élt, arra hivatkozva, hogy a hirdetések nyomkövetése jelentős változtatásokat követelne a valós idejű Google Ads hirdetésaukciós rendszerben, ezért a megfelelés érdekében inkább tiltják az összes politikai tartalommal bíró hirdetést. A tavaly év végén elfogadott törvényjavaslat 2019. június 30-án, vagy még az előtt lép hatályba, így várhatóan a Google – amennyiben még nem tette meg – hamarosan módosításokat fog eszközölni hirdetési rendszerében.

Haditengerészeti információkat gyűjtenek kínai hackerek

(www.bbc.com)

Az iDefence biztonsági kutatócég elmondása szerint kínai hackerek célzott kampányt folytatnak amerikai, kanadai és délkelet-ázsiai felsőoktatási intézmények ellen. Bár az érintett egyetemek teljes listáját nem fedték fel a kutatók, összesen 27 intézmény, például a Massachusettsi Műszaki Egyetem (MIT) is érintett volt a támadásban, amely során főleg a tengeri hadviseléssel összefüggő – például a tengeralattjáró rakéta – technológiával kapcsolatos információk megszerzése volt a cél. A támadás során – látszólag más egyetemekről érkező – olyan káros kódokat tartalmazó adathalász e-mailek kerültek kiküldésre, amelyekkel a támadók hozzáférést szereztek a tárolt kutatási eredményekhez, például az USA haditengerészetével szoros együttműködésben álló Woods Hole Óceanográfiai Intézet adataihoz. **Bővebben...**

Választási folyamatokat támogató kiberbiztonsági javaslatok az ENISA-tól

(www.enisa.europa.eu)

Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) múlt héten kiberbiztonsági ajánlásokat fogalmazott meg az európai parlamenti választásokkal kapcsolatban, amelyben felsorolásra kerültek az Unió demokratikus folyamatait potenciálisan veszélyeztető tényezők. Ilyen például azon kibereszközök köre, amelyek lehetővé teszik a választási folyamatokba történő beavatkozást. Udo Helmbrecht, az ENISA ügyvezető igazgatója arra bíztatja az uniós tagállamokat, hogy minél több kiberbiztonsági gyakorlatban vegyenek részt, valamint készítsenek incidens reagálási tervet arra az esetre, ha egy esetleges adatszivárgás áldozatává válnának. **Bővebben...**

A beállítások ellenére sem voltak védve az Android felhasználók tweetjei

(www.engadget.com)

A Twitter egy még január 14-én kijavított programhibáról tájékoztatja androidos felhasználóit, amely öt éve jelen volt az alkalmazásban. A közösségi oldal szerint azokat a felhasználókat érintett a hiba, akik az androidos Twitter alkalmazásban 2014. november 3. és 2019. január 14-e között megváltoztatták fiókadataikat, beleértve az e-mail címeket is. A felhasználói módosításokat követően, amennyiben az alkalmazáson belül korábban engedélyezték a védett módot (Protect your tweets), a Twitter automatikusan letiltotta a funkciót. Egyelőre az ügy kapcsán nem indítottak vizsgálatot a közösségi platform ellen, amely már korábban is szembesült a GDPR megsértésének vádjával. Tavaly év végén az ír Adatvédelmi Bizottság indított vizsgálatot a Twitter ellen, miután a cég elutasította a t.co webes linkkövető adatok átadását, majd biztonsági kutatók fedeztek fel egy olyan biztonsági hibát, amellyel engedély nélküli szöveges tweet bejegyzéseket lehetett közzétenni a platformon. Ez a hiba kizárólag angol twitterfiókokat érintett.

IT biztonsági Tanács

Androidos mobilkészülékek esetén a már nem kívánatos applikációk törlését ne az alkalmazásikon hosszan tartásával és a képernyő tetején megjelenő „Eltávolítás" feliratú sávba húzással végezzük el.

Ennél célravezetőbb megoldás a Google Play Alkalmazásboltján belül, vagy az eszköz *„Beállítások", „Alkalmazás"* menüjében megjelenő listából kiválasztani, majd az „Eltávolítás" gombra kattintva törölni a programokat.

Amazon szervereken kerülnek tárolásra a német rendőrség testkamera felvételei

(www.securityaffairs.co)

A német rendőrség az Amazon felhőszolgáltatását használja a testkamerák felvételeinek tárolására, derült ki a Neue Osnabrücker Zeitung egy szombati cikkéből. A német Belügyminisztérium állítása szerint az állami infrastruktúra nem felel meg a német adatvédelmi törvényeknek, így jelenleg az Amazon az egyetlen olyan szolgáltató, aki - a német Szövetségi Információbiztonsági Hivatal (BSI) által hitelesített - felhőszolgáltatást képes nyújtani az országban. A szövetségi Rendőr-főkapitányság elmondása szerint az adatok kizárólag az Amazon németországi szerverein kerülnek tárolásra titkosított formában. **Bővebben...**

Több száz katonai bevándorló került veszélybe az amerikai hadsereg e-mailje miatt

(www.engadget.com)

Az amerikai hadsereg véletlenül több mint 4200 bevándorló adatait hozta nyilvánosságra egy olyan táblázat e-mailben való kiküldésével, amely a MAVNI (Military Accessions Vital to the National Interest) katonai toborzási programban résztvevők adatait - többek között nevet, társadalombiztosítási számot és a szolgálatteljesítés kezdetének dátumát - tartalmazza. A kiszivárgott listán több mint 900 mandarin és több tucat orosz nyelvű, katonai szolgálatra jelentkező szerepel, akik közül egyesek vízumengedélyének érvényességi ideje már lejárt, így ők - a listára alapozva - benyújtották menedékjogi kérelmüket arra hivatkozva, hogy az országukba való visszatérésük során büntetésben részesülhetnek az amerikai hadseregben vállalt szolgálatteljesítés miatt.

Windows és Linux alapú gépekből áll az önmagát építő botnet hálózat

(www.bleepingcomputer.com)

Windows és Linux platformok ellen irányuló kampányt fedezett fel a FortiGuard Labs kutatólabor, amely során egy próbálgatás-alapú (brute force) rosszindulatú jelszótörő programot használnak a támadók. A Malwarebytes még februárban fedezte fel a StealthWorker, vagy GoBrut elnevezésű szoftvert, amely képes a Magento, a phpMyAdmin és a cPanel tartalomkezelő szerverek (CMS) számos sebezhető pontjának kihasználására és brute force módszerrel a rendszerbe történő beszivárgásra. **Bővebben...**

Elfogadták az orosz államiságot vagy kormányzati hivatalos személyeket online sértő tartalmak elleni törvénytervezetet

(www.bleepingcomputer.com)

Az Orosz Állami Duma 327 képviselői szavazattal (40 ellenző és 1 tartózkodó szavazat mellett) elfogadta a 606596-7-es számon benyújtott új törvényjavaslatot, amely lehetővé teszi a hatóságok számára, hogy büntetésben részesítsék azokat, akik sértő, tiszteletlen internetes tartalmakat tesznek közzé a kormány, illetve állami szervezetek vonatkozásában. Az Orosz Föderáció közigazgatási bűncselekményekről szóló törvény 20.1 cikkének módosítása szerint tiszteletlen tartalmak interneten történő közzététele az orosz társadalommal, a kormánnyal és a közhatalmat gyakorló állami szervezetekkel összefüggésben legfeljebb 15 nap elzárással és maximum 100.000 rubel (körülbelül 1.509 dollár) pénzbírsággal büntethető. **Bővebben...**