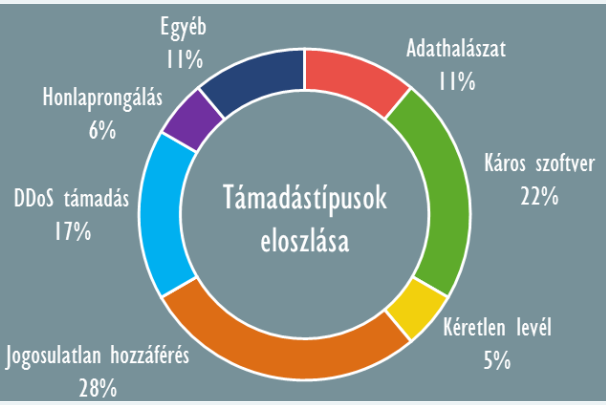
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.01.04. - 2019.01.10.



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

A Kaspersky segíthetett kézre keríteni az NSA-től adatokat szivárogtatót

(politico.com)

Bizalmas NSA dokumentumok ellopásának vádjával 2016 októberében amerikai hatóságok letartóztatták Harold T. Martint, akinek az azonosításában a Politico információi szerint lényeges szerepe volt a Kaspersky-nek. A biztonsági cég kutatói gyanús Twitter üzenetek miatt lettek figyelmesek a „HAL999999999" nevű felhasználóra, amelyek csupán 30 perccel a „The Shadow Brokers" csoport szivárogtatása előtt érkeztek a cég egyes kutatóihoz. **Bővebben...**

Ingyenes kódvisszafejtő programot ad közre az NSA

(zdnet.com)

Az amerikai Nemzetbiztonsági Ügynökség (NSA) a márciusi RSA konferencián ingyenes elérhetővé teszi a saját fejlesztésű disassemblerét (GHIDRA). A program segítségével a futtatható fájlok az ember által értelmezhető assembly nyelvű kóddá fejthetők vissza, amely többek között a malware-ek működésének elemzéséhez nyújthat hatékony segítséget. Az eszköz a WikiLeaks-es Vault7 publikálásával már 2017-ben ismertté vált, amelyből az is kiderült, hogy azt több amerikai kormányügynökség mellett például a CIA is használja. A moduláris felépítésű szoftver Java nyelven készült, grafikus felülettel rendelkezik és Windows, Linux vagy macOS környezetben is működik, az említettek mellett pedig mobil operációs rendszerek binárisait is képes elemezni. **Bővebben...**

Összehasonlító tanulmány öt európai katonai kiberparancsnokságról

(icds.ee)

Észtország biztonsági és védelmi kérdések terén vezető agytröszt (think tank) szervezete, az International Centre for Defence and Security (ICDS) összehasonlító tanulmányt készített öt európai nemzet ─ jelesül Észtország, Finnország, Németország, Hollandia és Norvégia ─ kiberparancsnokságának képességeiről, amely az első nyilvánosan elérhető kiadvány ebben a témában. Az anyag több szempontból vizsgálja a szerveket, többek között a stratégiai iránymutatások, a szervezeti felépítés, vagy például a parancsnoki lánc függvényében. A második rész elemzéseket tartalmaz minden egyes szervezeti felépítés tekintetében, számba véve az adott modell előnyeit és hátrányait, az utolsó szekció pedig szabályozási javaslatokat fogalmaz meg.

Már meg is történt 2019 első jelentős adatszivárgása

(scmagazineuk.com)

Mintegy 30 000 ausztrál állami dolgozó adata szivárgott ki ─ adja hírül egy helyi hírügynökség. Az incidens Victoria államot érintette, és a kompromittálódott adatok között elsősorban az alkalmazottak munkahelyi adatai szerepelnek, beleértve dolgozói kontakt információkat és belső levelezéseket is. A Melbourne-i Egyetem egy kutatója szerint elképzelhető, hogy az eset hátterében állami támogatású csoport áll, ugyanakkor nem zárható ki az sem, hogy az elkövetőket a haszonszerzés motiválta, ugyanis az eltulajdonított információk többféle visszaélésre is módot adhatnak.

Egy Skype hívással kijátszható volt az androidos eszközök zárolása

(theregister.co.uk)

Egy biztonsági rés kihasználásával a Skype alkalmazáson keresztül fogadott hívások lehetővé tették az androidos eszközök zárolásának megkerülését, így a feloldási művelet végrehajtása nélkül megtekinthetővé váltak az eszközökön tárolt fényképek, és névjegyek, valamint üzenet küldésére is mód nyílt. A sérülékenységre egy 19 éves, koszovói számítógépes programhiba-kutató hívta fel még októberben a Microsoft figyelmét, a december 23-án kiadott frissítésben pedig már javításra került a hiba. A sebezhetőségben minden 8.15.0.416 ─ és ennél alacsonyabb ─ verziószámú androidos Skype alkalmazás érintett.

IT biztonsági Tanács

Egyedi Android-hirdetésazonosítóját (GAID) a *Beállítások* ► *Google* ► *Hirdetések* menüpontban tekintheti meg, illetve iratkozhat le a személyre szabott hirdetésekről, amelynek kikapcsolását követően az Ön hirdetési ID-ját nem fogják felhasználni profilépítéshez, illetve személyre szabott hirdetések megjelenítéséhez.

Ugyanezen menüpontban lehetősége van a hirdetési azonosító visszaállítására is, azonban ennek végrehajtása előtt mindenképp jegyezze fel korábbi azonosítóját, ugyanis a GAID-hoz rögzített személyes adatai továbbra is a régi azonosítóval lesznek megtalálhatók, ellenőriztethetők és törölhetők.

Útmutatók a kiberbiztonsági kollaboráció erősítéséhez

(enisa.europa.eu)

Miután az elmúlt években számos sikert ért el a kiberbiztonsági együttműködések terén, a holland kibervédelmi központ (NCSC-NL) most négy útmutatót ad ki a témában. A központ álláspontja szerint a digitális ellenálló képesség növelése kizárólag a szektorokon belüli ─ valamint kiemelten a publikus és a magán szektor közötti ─ aktív kooperációval valósulhat meg. **Bővebben...**

A német internet szolgáltatók három hónapig tárolják az IP-címeket

(heise.de)

Egy jelentés szerint a német távközlési szolgáltatók a 2012-ben kiadott hivatalos állami ajánlásban foglaltak ellenére általánosságban nézve hat hónapos – ezen belül is például az IP-címek esetében három hónapos – adattárolást realizálnak a törvényes megőrzési kötelezettségtől függetlenül, önkéntes alapon, annak ellenére, hogy a hatóságilag irrelevánsnak minősülő adatokat legkésőbb hét napon belül törölniük kellene. **Bővebben...**

Modlishka ─ egy automatizált adathalász eszköz pentestereknek

(zdnet.com)

Piotr Duszyński lengyel biztonsági kutató közzétett egy Modlishka névre keresztelt sérülékenység vizsgálati eszközt a GitHubon, amellyel egyszerű módon automatizálhatóak az adathalász támadások, és még a kétfaktoros hitelesítéssel ellátott fiókok is sikeresen támadhatóak, azok kivételével, amelyek U2F -alapú hardverkulcsokkal védettek. A Modlishka lényegében egy módosított reverse proxy, amely a felhasználó és a támadott weboldal között helyezkedik el. Az áldozat a Modlishka szerverhez csatlakozik, ami a háttérben a felhasználót megszemélyesítve intéz kérést a valódi oldal felé. **Bővebben...**

DNS eltérítéses támadásokkal gyanúsítják Iránt

(fireeye.com)

A FireEye egy legkésőbb 2017 januárja óta zajló kiterjedt kibertámadási kampányra hívja fel a figyelmet, amely kormányzati, telekommunikációs és egyéb internetes infrastruktúrák ellen zajlik világszerte, de legfőképp a közel-keleti, észak-afrikai, európai és észak-amerikai régiókban. **Bővebben...**

Egy hiteles forrás a GDPR-megfelelőség kialakításához

(protonmail.com)

Az Európai Unió Általános Adatvédelmi Rendelete (GDPR) fontosságához képest nem bővelkedik a megfelelőség kialakítását segítő hatékony útmutatókban, ezen kíván változtatni a GDPR.eu weboldal ─ adja hírül a Protonmail blog bejegyzésében. Eszerint a ProtonMail csapata tavaly 101 üzleti vezető megkérdezésével igyekezett felmérni a szervezetek felkészültségi szintjét, és azt találták, hogy fél évvel a rendelet hatálybalépését követően sem mondható el, hogy a vállalkozások többsége megfelelne a szigorú elvárásoknak. Úgy találták, hogy az egyik fő akadály, hogy a kis- és középvállalkozások számára már a jogszabály helyes értelmezése is komoly kihívást jelent, amelynek áthidalásához kevés az autentikus forrás. **Bővebben...**