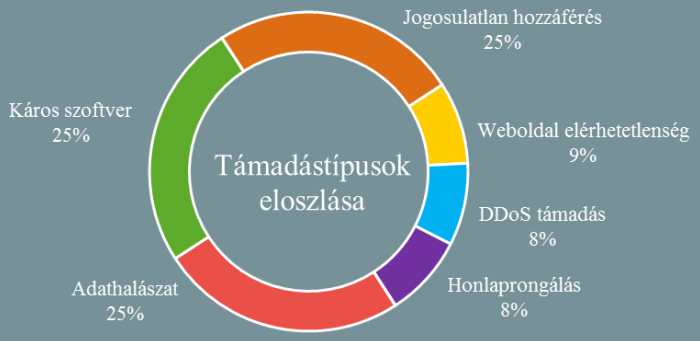
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 23. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.05.31. - 2019.06.06.



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

Kibertámadás érte az Ausztrál Nemzeti Egyetemet

(securityaffairs.co)

Ausztrália legnagyobb egyeteme ─ az Ausztrál Nemzeti Egyetem ─ kibertámadás áldozatává vált, amelynek során a hackerek az egyetem dolgozóinak és hallgatóinak szenzitív adataihoz ─ például banki információkhoz, útlevélszámokhoz, iskolai eredményekhez ─ fértek hozzá, az elmúlt 19 évre vonatkozóan. A tavaly év végén történt biztonsági incidensnek összesen több, mint 200 000 érintettje van. A hatóságok mindeddig nem kötötték konkrét csoporthoz a támadást, de a nyomok egy magasan képzett kollektívára utalnak. Ausztrál intézmények az utóbbi évek során számos alkalommal álltak kibertámadások kereszttüzében, legutóbb februárban, amikor az ausztrál parlament hálózata vált célponttá.

Újabb bizonyíték a BlueKeep által hordozott veszélyre

(bleepingcomputer.com)

A Zəɹosum0x0 álnevet használó kutató készített egy MetaSploit modult a BlueKeep sérülékenység kihasználásához, amelyet azonban a sérülékeny rendszerek nagy száma miatt nem tesz nyilvánosan elérhetővé. A szakember ellenben közzétett egy videót, amelyben egy Windows 2008-as gépen demonstrálja a kihasználást, ami elmondása szerint Windows 7 és Server 2008 R2 esetében is működik, azonban például a szintén sérülékeny Windows Server 2003 esetében nem. Zəɹosum0x0 szerint néhány hete még voltak kétségek a sebezhetőség súlyosságával kapcsolatban, azonban mára egyértelművé vált, hogy a hiba kihasználása lehetséges. **Bővebben..**

Újabb Windows távoli asztal sebezhetőségre derült fény

(securityaffairs.co)

A Carnegie Mellon Egyetem egy kutatója fedezte fel a Microsoft Windows távoli asztal kapcsolatot (Remote Desktop Protocol ─ RDP) érintő sebezhetőségét (CVE-2019-9510), amely kliensoldali támadások során kihasználható a képernyőzár megkerülésére. A biztonsági probléma a Network Level Authentication (NLA) funkció hibájából ered, ami azt eredményezi, hogy amennyiben az RDP session hálózati hiba miatt megszakad, az automatikus helyreállítás nem zárolt állapotot állít vissza. A sérülékenység a Windows 10 1803-as verzióját, valamint a Windows Server 2019-et érinti. **Bővebben...**

A ProtonMail tagadja, hogy kormányzati igényre felhasználói után kémkedne

(securityaffairs.co)

Nemrégiben az a vád érte a ProtonMail-t, hogy bírói végzés nélkül, önkéntes alapon valós idejű megfigyelést tesz lehetővé a bűnüldöző hatóságok számára. Mindez Stephan Walder, a Cybercrime Competence Center vezetőjének előadása közben hangzott el, amelyet Martin Steiger svájci ügyvéd még az előadás alatt Twitter üzenetben közzé is tett, majd saját blogján hosszabb formában is tárgyalt. Ebben részletesen foglalkozik a ProtonMail-t érintő jogszabályi kötelezettségekkel és úgy találja, hogy a kapcsolódó hatályos jogszabályok (Swiss Federal Act on the Surveillance of Post and Telecommunications – SPTA, valamint az Ordinance on the Surveillance of Post and Telecommunications – SPTO) nem kötelezik a ProtonMail-t valós idejű megfigyelés biztosítására, azaz bármely ilyen jellegű együttműködés önkéntes alapon történik. Steiger erre a ProtonMail saját átláthatósági jelentéséből hoz valós példát, miszerint 2019 áprilisában hatósági megkeresésre az e-mail szolgáltató IP logolást vezett be egy felhasználónál, ami szerinte kimeríti a kérdéses kategóriát. **Bővebben...**

Agresszív reklámok okoznak bosszúságot több százmillió android felhasználónak

(www.zdnet.com)

Az elmúlt évben több, mint 440 millió Android felhasználó töltött le olyan alkalmazást a Google Play Store-on keresztül, amelyek tartalmazták az alkalmazáson kívüli hirdetéseket megjelenítő BeiTaPlugin nevű programkönyvtárat. A 2018-as megjelenésű, fejlesztői körökben nagy népszerűségnek örvendő SDK kezdetben pontosan azt nyújtotta, amit ígért, azaz lehetővé tette az egyszerű és automatizált hirdetések alkalmazásokon belül történő megjelenítését. Ez év februárjában és márciusában azonban a BeiTaPlugint tartalmazó appok felhasználói egyre gyakrabban szembesültek olyan hirdetésekkel, amelyek blokkolták a telefonkészülékek képernyőjéhez vagy egyes szolgáltatásokhoz való hozzáférést, ellehetetlenítve a beérkező hívások fogadását, vagy más alkalmazások megnyitását. A fejlesztők feltételezhették, hogy a program „új funkciója" nem feltétlenül nyeri majd el a felhasználók tetszését, ugyanis azt több praktikával kívánták leplezni. **Bővebben...**

IT biztonsági Tanács

A VPN egy rendkívül hasznos szolgáltatás, azonban mielőtt bizalmat szavaznánk egy szolgáltatónak érdemes néhány szempontot figyelembe venni és nem csupán a költségek alapján döntést hozni.

Javasolt felhasználói vélemények után kutatni ─ több platformon is ─ és alaposan utánajárni a VPN szolgáltatóknak, lehetőségeknek, ajánlásoknak.
A legfontosabb kritériumokat weboldalunkon **itt** találja.

Leáll a GandCrab zsarolóvírus

(securityaffairs.co)

Az először 2018 elején feltűnt GandCrab zsarolóvírus készítői népszerű hacking fórumokon jelentették be, hogy felhagynak a ransomware fejlesztésével és „üzletfeleiket" is arra kérik, hogy 20 napon belül állítsák le a káros kóddal történő támadásokat. A zsarolóvírust főként orosz sötét webes fórumokon reklámozták, ún. RaaS (Ransomware-as-a-service), azaz bérelhető szolgáltatásként. A káros kód több, mint egy éves pályafutása során számos módosításon esett át, tavaly októberben már az 5.0-ás verziónál tartott. A bejelentés szerint a GandCrab RaaS hálózat összbevétele elérte a 2 milliárd dollárt, amelyből maguk a fejlesztők nettó 150 millióra tettek szert. **Bővebben...**

A Microsoft arra kér, tanuljunk a WannaCry támadás tanulságaiból

(securityweek.com)

Mint a múlt hét során kiderült, közel egymillió eszközre továbbra sem telepítették a BlueKeep sérülékenységet befoltozó, több hete kiadott hibajavítást, így a Microsoft újabb figyelmeztetést adott ki. A tech óriás május havi frissítési csomagjában javította a régebbi Windows rendszereket érintő sérülékenységet (CVE-2019-0708), ami komoly biztonsági kockázatot jelent, ugyanis kihasználásával átvehető az irányítás az érintett rendszerek felett. Súlyosbító tényező, hogy a 2017-es WannaCry-hoz hasonlóan itt is fennáll az esély, hogy a kihasználó káros kód féregszerűen tovább terjedjen a hálózaton, azaz elég egyetlen interneten keresztül elérhető sérülékeny munkaállomás, és potenciálisan a teljes szervezet fertőzötté válhat. **Bővebben...**

Elkészült a sérülékenységek kihasználását vizsgáló eddigi legátfogóbb tanulmány

(www.zdnet.com)

Egy új, hiánypótló kutatás azt vette górcső alá, hogy az utóbbi 10 évben felfedezett sérülékenységeket milyen arányban használták fel kibertámadásokhoz. A felmérés ─ amely a legkiterjedtebb ilyen jellegű kutatásnak számít ─ úgy találta, hogy a 2009 és 2018 között beazonosított, mintegy 76 000 sérülékenység csupán 5,5%-a (4 183 biztonsági hiba) vált támadás eszközévé. Érdekességképp a kutatók nem találtak összefüggést a támadások valószínűsége és a között, hogy az adott sérülékenységhez jelent-e meg proof-of-concept (PoC). Úgy tűnik azonban, hogy minél magasabb egy sérülékenység kockázati besorolását meghatározó CVSSv2 pontszáma, annál valószínűbb, hogy ki is fogják használni azt. **Bővebben...**

Szakértők szerint Németországban a kisebb cégeknél felhígulhat az adatvédelem

(www.heise.de)

A német szövetségi adatvédelmi biztos élesen bírálja az adatvédelmi előírások bizonyos lazításának gondolatát a kis- és középvállalkozások vonatkozásában, amelyet egyes németországi politikai erők kezdeményeztek. Véleménye szerint ez nem a kapcsolódó – legalább tíz munkavállalót foglalkoztató cégeket érintő – jogi szabályozás ésszerűbbé tételét jelentené, hanem aláásná a vonatkozó védelmi előírásokat. Az adatvédelmi biztos azt is hangsúlyozta, hogy az európai általános adatvédelmi rendelet (GDPR) egy éve van hatályban, és az azzal kapcsolatos, az ellenzők által készített mérlegvonást még korainak tartja, különös tekintettel arra, hogy számos szervezet a rendelet végrehajtására két éves átmeneti időszakot kapott. **Bővebben...**