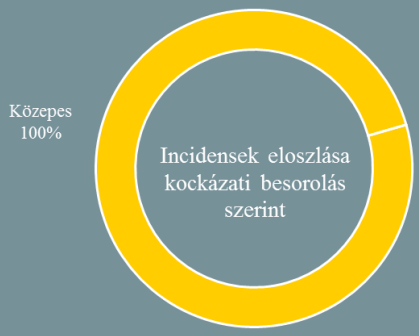
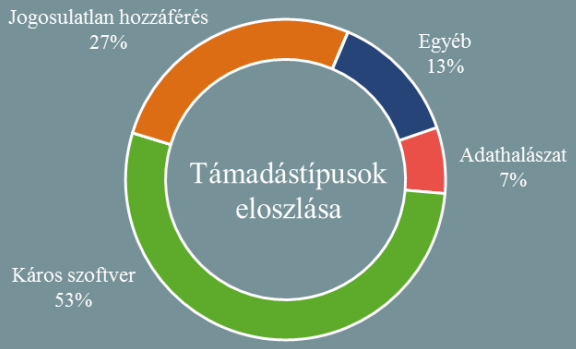
Nemzetközi IT-biztonsági sajtószemle

2019. 19. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.05.03. - 2019.05.09.





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

Mostantól vége az üzenetküldő alkalmazások anonim használatának Oroszországban

(ehackingnews.com)

Egy május 5-én érvénybe lépett orosz kormányrendelet értelmében az üzenetküldő szolgáltatásoknak ellenőrizniük kell a regisztrációkor megadott adatok hitelességét a telefonszám alapján, amihez a mobil szolgáltatótól kell információt kérniük. A szolgáltatónak ─ amennyiben megtalálja a telefonszámot a saját adatbázisában ─ vissza kell igazolnia az ügyfél adatait, valamint rögzítenie kell, hogy az adott felhasználó melyik üzenetküldő szolgáltatást használja, végül a korábbiaknak megfelelően egy azonosítási kódot kell küldenie az ügyfélnek. Minderre összesen 20 perc áll rendelkezésre, amennyiben ez időn belül nem érkezik visszaigazolás a mobil szolgáltatótól, a regisztráció nem tekinthető véglegesnek. Alexander Zharov, az orosz médiafelügyelet vezetője szerint az azonosítási eljárással kikerülhető, hogy valaki más telefonszámát regisztrálja, ami elősegíti a bűnüldöző hatóságok munkáját. Azon szolgáltatók, akik nem tesznek eleget a szabályozásnak, bírságra számíthatnak, valamint a szolgáltatásuk Oroszországból történő kitiltására.

Bankkártya adatokat szivárogtatott egy kanadai mobil szolgáltató

(techcrunch.com)

Rendszerhibák naplózására használta a Freedom Mobile azt az Elasticsearch szervert, amely egy hibás konfiguráció következtében ügyféladatokat is rögzített. Ha mindez nem lett volna elég probléma, a mintegy ötmillió bejegyzést tartalmazó adatbázist még jelszóval sem védték, így az bárki számára szabadon hozzáférhető volt. A kompromittálódott adatok között található az ügyfelek neve, e-mail és postai címe, születési dátumuk, emellett egyes esetekben bankkártya információk, beleértve a lejárati dátumot és a biztonsági kódot (CVV) is. **Bővebben...**

Fontos biztonsági funkciót kap a WordPress

(securityweek.com)

A WordPress tartalomkezelő (CMS) legújabb ─ már elérhető ─ 5.2-es verziójával több fontos biztonsági újdonságot is bevezet. Ezek között szerepel például a Site Health hibakeresési funkciókkal történő kiegészítése, vagy a PHP Error Protection, amely kritikus PHP hibák biztonságos kezelését teszi lehetővé. A legfontosabb fejlesztés azonban valószínűleg az, hogy a WordPress frissítések ezt követően digitálisan aláírásra kerülnek, amelyeket a WordPress oldalak ellenőrizni tudnak. **Bővebben...**

Exchange szerverekre specializálódott backdoorral támad a Turla

(securityaffairs.co)

Az orosz kötődésű Turla APT csoport (vagy más néven Waterbug, Venomous Bear vagy KRYPTON) egy szofisztikált backdoort alkalmaz Exchange szerverek ellen ─ adta hírül az ESET. Elemzésükből kiderül, hogy a LightNeuron néven hivatkozott káros kóddal legalább 2014 óta folytatnak kiberkémkedési célú támadásokat. A biztonsági cég eddig legalább három szervezet esetében állapított meg érintettséget; az áldozatok között szerepel egy nem megnevezett kelet-európai külügyminisztérium, egy közel-keleti diplomáciai szervezet, és egy brazil cég. Az ESET szerint ez az első alkalom, hogy olyan malware-t azonosítottak, ami kifejezetten Exchange szerverekre specializálódott, oly módon, hogy működését egy kompromittált Exchange Transport Agenttel biztosítja. **Bővebben...**

Adathalász támadást tesz lehetővé a UC Browser sérülékenysége

(securityaffairs.co)

Egy Google keresést javító új funkció bevezetése idézhette elő a kínai fejlesztésű UC Browser és az UC Browser Mini Androidra szánt verzióinak sérülékenységét, amely kizárólag az alkalmazások legújabb — UC Browser 12.11.2.1184-es és a UC Browser Mini 12.10.1.1192-es — verzióit érinti. A biztonsági rés kihasználásával a támadók képesek lehetnek meghamisítani a mobilböngésző címsorában megjelenő URL-t, így a felhasználókat könnyen átirányíthatják az általuk üzemeltetett adathalász weboldalakra, bár az SSL tanúsítványok nem hamisíthatók a módszerrel. A sérülékenységet egy Arif Khan nevű biztonsági kutató fedezte fel, aki a kihasználásról blogján videót is közölt. **Bővebben...**

IT biztonsági Tanács

Az incidenskezelési platformok nagymértékben segíthetik a SOC-ok, CSIRT-ek és CERT-ek munkáját az információbiztonsági események kivizsgálása során.

A konkrét szoftver kiválasztásakor fontos szempont lehet, hogy az mekkora anyagi terhet jelent a szervezet számára, azonban szerencsére elérhetőek ingyenes szolgáltatások is.

Erre jó példa a TheHive project, amely egy nyíltforrású, ingyenes, 4 az 1-ben incidens kivizsgálási platform, amely ráadásul a MISP-pel, egy hasznos fenyegetési információkat tartalmazó közösségi felülettel is szinkronizálható.

Továbbra is aktívan kihasználják az Oracle WebLogic sérülékenységét

(threatpost.com)

A Palo Alto Networks fenyegetés felderítő csapata, a Unit 42 szerint, habár április 26-óta elérhető a hivatalos javítás, egyre nő az Oracle WebLogic nemrég nyilvánosságra hozott sérülékenységét (CVE-2019-2725) kihasználó támadások száma. A biztonsági hiba nyilvánosságra kerülése után először a Sodinokibi zsarolóvírussal, valamint a Muhstik botnettel fertőzték a sérülékeny szervereket, azonban utóbb egy Monero kriptovaluta bányász program (XMRig), valamint a GandCrab zsarolóvírus is egyre gyakrabban tűnik fel. A kutatók ennek kapcsán felhívják a figyelmet arra, hogy a biztonsági frissítések telepítése azokon a rendszereken is létfontosságú, amelyek az internet irányából közvetlenül nem elérhetőek, mivel a támadók a belső hálózatok kompromittálásával is képesek lehetnek hozzáférni a megcélzott rendszerhez. **Bővebben...**

Koncepcióváltást jelezhet a Chrome új funkciója?

(www.engadget.com)

A Google várhatóan ezen a héten új funkciót vezet be a Chrome böngészőhöz, amely nem csupán részletesebb információt ad a nyomkövető sütikről (tracking cookies), hanem lehetőséget is biztosít azok korlátozására. Az elképzelés nem új keletű — a Mozilla Firefox kiterjesztett nyomkövetés-védelme például már tavaly óta elérhető — azonban a Google eddigi üzletpolitikáját tekintve mégis jelentős lépésként értékelhető. A Facebook Cambridge Analytica botrányát követően a Google szemmel láthatóan nagyobb figyelmet fordít a felhasználók adatainak védelmére, a lehetséges paradigmaváltás mögött pedig vélhetően az az elképzelés áll, hogy a reklámbevételek csökkenését ellentételezni fogja a felhasználói bizalom és az ebből fakadó márkahűség. *(Szerk.: A Chrome ugyanakkor a Google tracking szolgáltatását nem fogja blokkolni, ezzel jócskán megkérdőjelezve az adatvédelmi elveket.)*

Új védelmi megoldásokat kínál a Microsoft a választások kibervédelmi ellenállóképességek növeléséhez

(www.securityweek.com)

A Microsoft a választási folyamatok biztonságosabbá tételét tűzte ki célul a már korábban elindított Defending Democracy Programjával, amely most két új megoldással jelentkezik. Az egyik a Galois-val közösen fejlesztett ElectionGuard, amely egy ingyenes, nyílt forráskódú szoftverfejlesztő készlet (SDK), a másik pedig a Microsoft 365 for Campaigns nevű szolgáltatás, ami a politikai kampányokat igyekszik megvédeni a célzott adathalász támadásoktól. Előbbi célja lehetővé tenni olyan szavazó rendszerek fejlesztését, amelyek az eredményeket a szavazók és harmadik felek számára is ellenőrizhetővé teszik, fejlett titkosítást használva biztonságosak, valamint auditálhatóak. **Bővebben...**

Németországban csak minden harmadik iskolában van mindenki által használható internet-hozzáférés

(www.heise.de)

Németország számos általános iskolájában a tanulók részére nem biztosított az internet-hozzáférés a tantermekben. Gyakran – minden ötödik iskolában – a diákoknak saját készülékeiket kell használniuk, ha a tanítás kapcsán digitális feladatok merülnek fel. A gimnáziumokban sem sokkal jobb a helyzet, a hozzáférési arány ezekben az intézményekben is csupán 45 százalék. Csupán a tanárok 47 százaléka rendelkezik saját hivatali e-mail címmel, és még ennél is kisebb azok száma, akik külön munkahelyi PC-vel rendelkeznek. **Bővebben...**