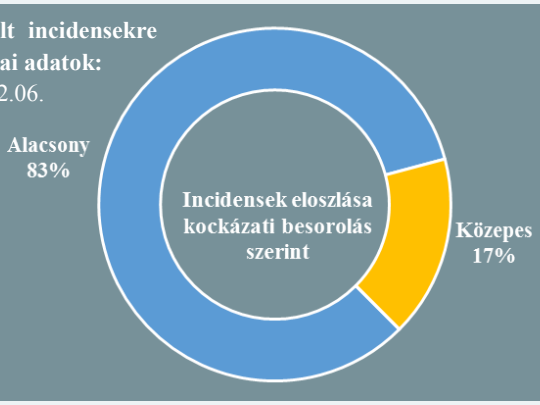
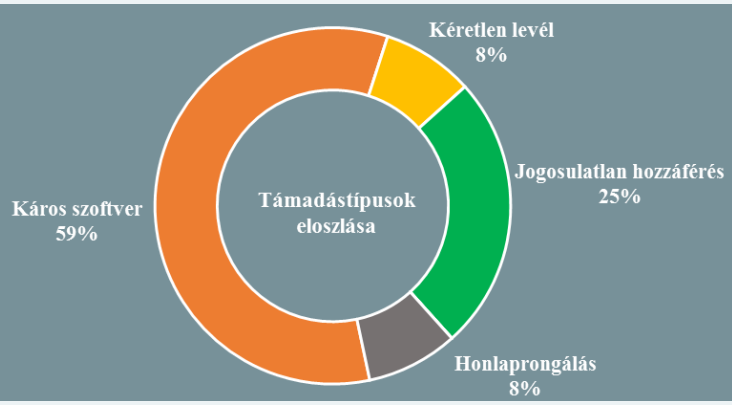
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2018. 49. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.11.30. - 2018.12.06.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!

Nem számít az inkognitó mód, a Google akkor is személyre szabottan jeleníti meg a keresési találatokat – állítja a DuckDuckGo

(thenextweb.com)

A Google bevallott módon bizonyos mértékben személyre szabottan jeleníti meg a keresési találatokat, például a keresés ideje, valamint a földrajzi helyzet függvényében. Egy szakmai körökben viták kereszttüzében álló nézet szerint azonban ezen túlmenően a felhasználók profilozásával, a böngészési szokásokat – például további kereséseket – is figyelembe veszi az eredménylisták összeállításához, ez az ún. „buborék hatás" (filter bubble). A DuckDuckGo internetes kereső friss tanulmányában pedig azt állítja, a böngészők privát böngészési (inkognitó) módja sem véd meg ettől. A profilozást nyíltan elutasító DuckDuckGo 87 ember bevonásával készült vizsgálata során a szimultán indított keresések a várakozásokkal ellentétben minden egyes, a vizsgálatban részt vevő személy esetében egyedi keresési eredményeket produkáltak, amelyekre ráadásul semmilyen befolyást nem gyakorolt, hogy a kereséseket privát böngészés során végezték-e. A Google reagált a tanulmányra, amelynek következtetéseit hibásnak tartják, kezdve a feltételezéssel, hogy az eredmények demográfiai profilozáson alapulnak, amelyet határozottan visszautasítanak.

Elharapódzó kiberkonfliktusok Oroszország és Ukrajna között

(securityweek.com)

Az ukrán biztonsági szolgálat (SBU) közleménye szerint sikeresen elhárítottak egy, az ország bírósági információs rendszerét ért kibertámadást, amelyért Oroszországot teszik felelőssé; az alkalmazott módszerről ugyanakkor mindössze annyit hoztak nyilvánosságra, hogy a támadás káros kódokat tartalmazó hamis elektronikus számlalevelekkel indult. A két ország közötti politikai konfliktus már több ízben nyilvánult meg a hadviselés ötödik dimenziójának tekintett kibertérben, óvatos feltételezések szerint pedig ebbe a sorba illeszkedhet a napokban nyilvánosságra hozott, orosz egészségügyi intézmények elleni kibertámadás is. Az esetet vizsgáló szakértők összefüggést valószínűsítenek a november 25-ei kercsi incidenssel, amelynek során az orosz határőrség tüzet nyitott három ukrán hajóra a tengerszorosnál, majd a fogságba ejtett legénység néhány sérült tagját moszkvai kórházakba szállították. A vizsgálatok során megállapították, hogy a támadásban részt vevő fájlok egy részét ukrán IP címekről töltötték fel a VirusTotal-ra.

A legtöbb TLS implementáció sérülékeny egy új támadási módszerrel szemben

(scmagazineuk.com)

Biztonsági kutatók egy új támadási metódusról közöltek információkat, amellyel a legújabb TLS implementációk régebbi, sérülékeny verzióra kényszeríthetők. A kutatók 9 különböző RSA-alapú biztonsági protokoll legfrissebb verzióját vizsgáltak át (OpenSSL, Amazon s2n, MbedTLS, Apple CoreTLS, Mozilla NSS, WolfSSL, GnuTLS, BearSSL és a BoringSSL), ezek közül csupán az utolsó kettő volt ellenálló a szóban forgó módszerrel („FLUSH+RELOAD") szemben. Az eredményeket összefoglaló, „The 9 Lives of Bleichenbacher's CAT: New Cache ATtacks on TLS Implementations" című tanulmány ajánlásokat is tartalmaz, például javasolja az RSA kulcs csere helyett a Diffie-Hellman eljárásra történő áttérést. Martin Thorpe, a Venafi munkatársa az eset kapcsán arra hívja fel a figyelmet, hogy bizonyos biztonsági intézkedések megnehezíthetik egy-egy támadás végrehajtását. **Bővebben**

Pillanatok alatt terhelték a gyanútlan felhasználók számláit iOS-es csaló appok

(arstechnica.com)

Reddit felhasználók jelentették, hogy az Apple App Store-on két olyan, magas értékelésű alkalmazás található, amelyek egy megtévesztés révén 100 dollár körüli összeget emelnek le az áldozat számlájáról; ezeket az Apple idő közben már el is távolította. A szóban forgó alkalmazások (Fitness Balance, valamint a Calories Tracker) azt állították magukról, hogy egészségügyi szolgáltatást nyújtanak (kalóriaszámlálás, testtömegindex mérés, stb.) azonban ehelyett megterhelték azon felhasználók számláit, akik megadták bankkártyaadataikat az Apple fiókjukban. A konkrét összegek 99.99 dollár, 119 dollár, vagy 139 euró között változtak ─ országtól függően. A megtévesztés úgy működött, hogy az alkalmazások megnyitás után megjelenítettek egy üzenetet, amelyben arra kérték a felhasználót, hogy olvastassa le ujjlenyomatát egy kalóriafigyelő funkció miatt. **Bővebben...**

IT biztonsági Tanács

Az NCC Group kutatói egy biztonsági audit során felfedezték, hogy az „Account is sensitive and cannot be delegated” flag bekapcsolása jelentősen **korlátozta volna** a NotPetya ransomware fertőzés terjedését a vállalati hálózatokon. Ez a Windows Active Directory beállítás megakadályozza, hogy egy account hitelesítő adatait szolgáltatások és alkalmazások is felhasználhassák.
Ennek használatát a Microsoft is **javasolja** a magas jogosultságokkal rendelkező fiókokon.

Orosz hackerek 2016-2017 között hozzáfértek a cseh külügy levelezéséhez

(zdnet.com)

A cseh Biztonsági Információs Szolgálat (BIS) 2017-es évet összefoglaló jelentése szerint 2016 és 2017 során kibertámadásokat hajtottak végre a cseh külügyminisztérium (MFA), a védelmi minisztérium, valamint a hadsereg ellen. A támadásokért a Turla és az APT28/Sofacy csoportokat teszik felelőssé, amelyek hátterében a széles körben elfogadott nézet szerint az orosz biztonsági szolgálat (FSZB), valamint a katonai hírszerzés (GRU) áll. Az egyik felfedezett kampány során a támadók 2016 elejétől kezdődően képesek voltak hozzáférni az MFA elektronikus levelezési rendszerén több, mint 150 e-mail fiókhoz. A jelentés kiemeli, hogy ennek során olyan információkhoz juthattak, amelyeket felhasználhatnak későbbi támadások előkészítéséhez, valamint további potenciális célpontok kiválasztásához. **Bővebben...**

Komoly biztonsági hibákat tártak fel egyes kommunikációs protokollokban

(thenextweb.com)

Tervezési hiányosságokból és hibás implementációkból fakadó súlyos biztonsági problémákat találtak kettő, gépek közötti kommunikációra (M2M) használt protokollban ─ közli a japán Trend Micro új tanulmányában. Mind a Message Queueing Telemetry Transport (MQTT), mind a Constrained Application Protocol (CoAP) széles körben használt IoT rendszerek esetében, nem ritkán ipari környezetekben. A kutatók csupán egyszerű kulcsszavas keresésekkel képesek voltak sérülékeny szervereket találni, és hozzáférni közel 200 millió MQTT, valamint 19 millió CoAP üzenethez, amelyek akár ipari kémkedés, DoS, vagy egyéb célzott támadások alapjául is szolgálhatnának. **Bővebben...**

Harc a terrorpropaganda ellen: német kritika az EU által tervezett feltöltés-szűrő kapcsán

(heise.de)

Az Európai Bizottság azon rendelettervezete, amelynek alapján határozottabban lehetne fellépni a terrorizmussal összefüggő online tartalmakkal szemben, ellenreakciókat vált ki Németország részéről. A tervezet szerint a terrorgyanús tartalmakat a szolgáltatóknak egy órán belül el kellene távolítaniuk, ezen kívül pedig jelentési kötelezettségük is lenne az ilyen vonatkozással bíró tartalmak esetében. Ezen ügyek kezelése mindenképpen költségtöbbletet eredményezne mind az állam (pl.: megfelelő hatósági szervezetrendszer felállítása), mind pedig a gazdasági társaságok (pl.: kapacitás-növelési kényszer) oldalán. **Bővebben...**

Nemzetközi anti-botnet útmutató a biztonságos internetért

(cyberscoop.com)

A számos technológiai szervezetet magába tömörítő Council to Secure the Digital Economy (CSDE) útmutatót adott ki „Anti-Botnet Guide” címmel, a digitális rendszerek robothálózatokkal szembeni globális biztosításához. Az anyag ─ amelyet iparági képviselők máris mérföldkőnek neveznek a technológiai szektor önszabályozásának folyamatában ─ olyan alapvető jó gyakorlatokat tartalmaz, amelyeket a szektor különféle szereplői is hasznosíthatnak. A kezdeményezés mögött az az elképzelés húzódik meg, hogy amennyiben ezek a szereplők azonos felfogásban, összehangoltan képesek a termékeik, rendszereik és ügyfeleik biztonságáért tenni, az internet védettebb lesz a botnetek okozta fenyegetéstől. **Bővebben...**