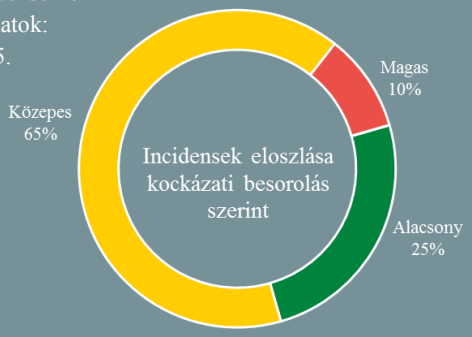
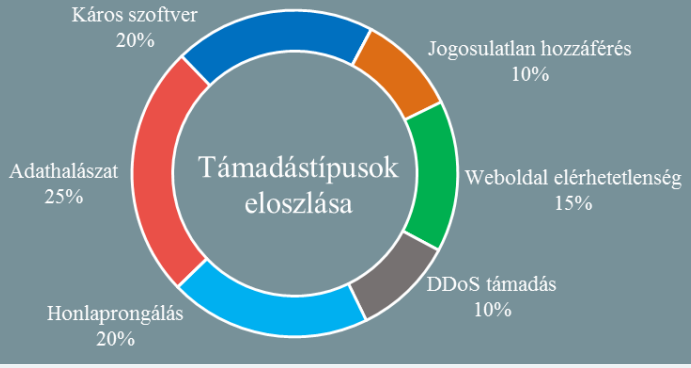
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.08.30. - 2019.09.05.





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

Az Irán elleni amerikai kibertámadásról – pro és kontra

(nytimes.com)

Az amerikai kiberparancsnokság (Cyber Command) informatikai támadást indított Irán paramilitáris szervezetének, a Forradalmi Gárdának egy kritikus fontosságú rendszere ellen, még június 20-án. A művelet kiváltó okaként az Egyesült Államok azt jelölte meg, hogy olyan hírszerzési információk birtokába jutott, amelyek szerint Irán áll az idén május és június során történt olajtankerek elleni támadások mögött. Egy amerikai vezető tisztviselő szerint Irán a megtámadott rendszerben tárolt információk alapján döntött arról, hogy pontosan mely tankerhajókat és mikor támadja meg. A támadás elrendelésekor szempont volt az Irán által lelőtt amerikai drón miatti válaszlépés, valamint az Egyesült Államok kiberképességek demonstrálása is. A csapás egyfelől sikeres volt, mivel az akció óta nem történt támadás tankerek ellen, illetve a közel-keleti ország a vártnál lassabban halad a katonai kommunikációs hálózatot is érintő károk helyreállításával, ugyanakkor egyes amerikai tisztviselők kétségbe vonják, hogy a művelet kifizetődőnek tekinthető-e. **Bővebben...**

Kína masszív kémtoborzásba kezdett a LinkedIn-en

(www.ehackingnews.com)

A kémügynökségek előszeretettel használják a közösségi oldalakat beszervezésekhez, amelyek között a LinkedIn számít az első számú célterületnek – állítják nyugati elhárító tisztek. Az Egyesült Államok, az Egyesült Királyság, Németország és Franciaország hírszerző ügynökségei már riasztást is adtak ki a nagy számban előforduló megkeresések kapcsán, amelyek mögött legnagyobb részt kínai kémek állnak. Több volt kormányzati tisztviselő kapott már „jól fizető” ajánlatot, többek között az Obama kormány egy volt külpolitikai tisztviselője, a Fehér Ház egy képviselője, illetve egy dán külügyminisztériumi tisztviselő is. **Bővebben...**

Cisco anyagok incidenskivizsgálások támogatásához

(zdnet.com)

A Cisco nemrégiben négy útmutatót tett közzé, amelyekkel segítséget szeretne nyújtani azon ügyfeleinek, akik – kompromittáció gyanúja esetén – digitális forensic vizsgálatot kívánnak végezni a gyártó termékein. A leírások a cég legjelentősebb szoftveres platformjaihoz készültek, mint a biztonsági eszközökön futó Cisco ASA (Adaptive Security Appliance), a Cisco hálózati eszközök saját operációs rendszere, a Cisco IOS (Internetwork Operating System), a Linux-alapú, szintén hálózati eszközökön alkalmazott Cisco IOS XE, valamint a hardveres tűzfalak Cisco FTD (Firepower Threat Defense) szoftvere. **Bővebben...**

A Symantec kijavította a Windows frissítések hibás kezelését

(heise.de)

A Microsoft korábban ideiglenesen felfüggesztette a Windows 7 SP1 és a Windows Server 2008 R2 SP1 frissítéseket a Symantec / Norton víruskereső szoftverrel rendelkező rendszereken. Ennek hátterében az állt, hogy a Microsoft 2019. augusztusától átállt az SHA-2 kódolásra a Windows frissítések aláírására használt tanúsítványok esetén, amelynek hatására a jelzett vírusirtó programok hamis riasztást generáltak. A Symantec augusztus 27-én közleményt adott ki, amelyben jelezte, hogy a probléma az érintett védelmi szoftverek új verzióiban megoldásra került. Ezt követően a Microsoft is feloldotta a frissítéseinek blokkolását, így a legfrissebb SEP verziót használó Windows 7 SP1 és a Windows Server 2008 R2 SP1 felhasználók ismét megkapják a windowsos biztonsági frissítéseket.

A Google adatvédelmi segítséget nyújt a fejlesztőknek

(engadget.com)

A Google bejelentette, hogy elérhetővé teszi Differential Privacy könyvtárának nyílt-forrású verzióját. A Differential Privacy, egy viszonylag új adatvédelmi megoldásnak számít, amely során az eszköz egy véletlenszerű zajjal egészíti ki a felhasználói adatokat, ellehetetlenítve ezáltal az egyes felhasználók esetleges beazonosítását. A cég más szolgáltatása során is alkalmazza a Differential Privacy módszert, például a Google Maps és a Google Fi esetén, de az Apple is használja már a böngészési előzmények, illetve a HealthKit adatok törléséhez. Az ilyen jellegű eszközök kifejlesztése a tech óriás szerint bonyolult, ezért segítségképp a megosztott könyvtárban főleg olyan funkciókra fókuszál, amelyek létrehozása különösen nehéz feladat, mint például határérték számítás a felhasználók által adott hozzájárulások tekintetében. A könyvtár elérhető a GitHub-on, ami egy ellenőrző funkciót (stochastic tester) is tartalmaz, amellyel a fejlesztők tesztelhetik alkalmazásaikat.

IT biztonsági Tanács

A marketing e-mailek sok esetben nyomon követik, hogy a címzett megnyitotta-e a levelet, és amennyiben igen, mikor tette, és hol tartózkodott ekkor.

Az NBSZ NKI weboldalán javaslatokat talál arra vonatkozóan, hogy mit tehet az ilyen rejtett adatgyűjtés ellen és megtalálja a legnépszerűbb levelező felületek ezzel kapcsolatos beállítási lehetőségeit.

Adatlopás történt a Foxitnél

(thehackernews.com)

A Foxit Software közleménye szerint ismeretlenek hozzáfértek az ügyfelek online fiókadatait tartalmazó adatbázishoz, amely e-mail címeket, jelszavakat, felhasználóneveket, telefonszámokat, cégneveket és IP címeket tartalmazott. A Foxit szoftvereit összesen több, mint 525 millióan használják világszerte, legnépszerűbb alkalmazásaik a Foxit PDF Reader, valamint a PhantomPDF. A cég közleményéből nem derül ki, hogy a jelszavak hashelve voltak-e, azonban minden érintett jelszót érvénytelenítettek, így a felhasználóknak mindenféleképpen meg kell változtatniuk azokat, amiről már kaptak is e-mailben tájékoztatást. Az incidens során bankkártya adatok nem kerültek veszélybe.

A Facebook az amerikai hatóságoknak sem engedi a hamis fiókok használatát

(washingtonpost.com)

Az Egyesült Államok bevándorlási hivatala (U.S. Citizenship and Immigration Services) korábbi álláspontján változtatva engedélyezte tisztviselőinek a hamis fiókok használatát a közösségi oldalakon egyes hivatali tevékenységek elvégzéséhez. A Facebook ugyanakkor közölte, hogy ami a cég megszemélyesítésekre vonatkozó szabályainak betartatását illeti, nem tesz kivételt az amerikai hatóságokkal, az ott dolgozóknak ─ bárki máshoz hasonlóan ─ a saját nevüket kell használniuk a közösségi oldalon. Az amerikai Belbiztonsági Hivatal múlt pénteken azzal érvelt, hogy a hamis profilok használata megkönnyíti a vízum, zöldkártya és állampolgársági igények ellenőrzését. Ennek hátterében az áll, hogy az USA Külügyminisztériuma idén június óta az amerikai vízumigényeken kötelezővé tette az igénylők számára a közösségi felhasználónevük megadását. **Bővebben...**

Titkos felhasználói adatgyűjtéssel vádolják a Google-t

(bbc.com)

A Brave böngésző azzal vádolja a Google-t, hogy a GDPR-t megkerülve rejtett weboldalakon keresztül nyomkövetést alkalmaz a felhasználóknál, a begyűjtött böngészési adatokat pedig reklámcégeknek értékesíti. A jogsértő gyakorlatot a Brave főigazgatója, Johnny Ryan leplezte le, aki annak ellenére megtalálta saját adatait a Google hirdetés értékesítési platformján, az Authorized Buyers-en (korábbi nevén doubleClick), hogy az internetes kereséseket egy olyan Chrome böngészőn végezte, amelyen nem volt bejelentkezve, és az eszközén nem kerültek tárolásra sem a böngészési előzményei, sem nyomkövető sütik (cookies). Ryan úgy véli, hogy a Google rejtett weboldalakon keresztül gyűjtötte az adatokat, amelyek egyedi azonosítókként funkcionáltak, és azt állítja, hogy egy órányi böngészés során a Google legalább kilenc ilyen weboldalt generált (további tizenegy duplikátummal). **Bővebben...**

Káros programokat rejthetnek az e-tankönyvek

(bleepingcomputer.com)

A Kaspersky Lab kutatói arra figyelmeztetnek, hogy a számítógépes bűnözők az elektronikus tananyagok és tankönyvek segítségével különböző káros kódokkal próbálhatják megfertőzni a hallgatók eszközeit. A Kaspersky saját ügyfeleinek adatai elemzése alapján azt találta, hogy az előző szemeszterben a kiberbűnözők mintegy 365 ezer alkalommal céloztak hallgatókat, ezek közül 233 000 esetben rosszindulatú kódokat tartalmazó esszék voltak a támadás eszközei. A másik jellemző kategóriát a tankönyvek jelentették, amelyek közül a legkeresettebbek a matematikai (1 213 letöltés), az irodalmi (870 letöltés) és az angol nyelvi (2 080 letöltés) elektronikus kiadványok voltak. **Bővebben...**