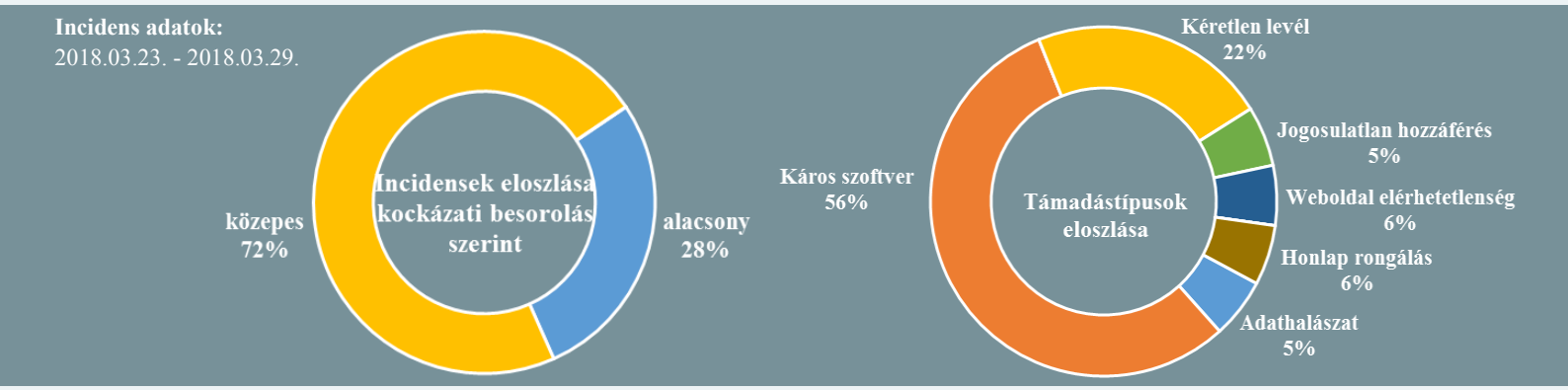

Kövessen minket online az itbiztonsag.govcert.hu oldalunkon, ahol naponta olvashatja legújabb híreinket!

A Microsoft szigorú tartalmi ellenőrzést vezet be

(www.bleepingcomputer.com)

Jonathan Corbett polgárjogi ügyvéd hívta fel a figyelmet a Microsoft 2018. május 1-től érvénybe lépő Szerződési Feltételeinek módosításaira, ami sértő szóhasználat esetén komoly retorziókat helyez kilátásba. A változásokról kiadott összefoglaló csak az Xbox termékhez kapcsolódó szolgáltatásokkal összefüggésben említi a fiók felfüggesztését, tiltását, vagy akár a fiókhoz tartozó számla zárolását, Corbett azonban a teljes Microsoft Szolgáltatási Szerződés átvizsgálásakor a Magatartási Kódexben is felfedezett egy releváns részt, amely már teljesen általánosan „Services", azaz „Szolgáltatások"-ként jelöli meg az offenzív tartalmak megjelenítését tiltó előírások vonatkozási körét. Mindezzel kapcsolatban Corbett azt kifogásolja, hogy a Microsoft nem ad pontos definíciót a káros magatartásformákról, valamint azt sem fejti ki, hogy milyen módon kívánja monitorozni a felhasználói magatartást. A büntetéssel kapcsolatban azonban már jóval részletesebb információ érhető el. Eszerint a Magatartási Kódexben foglalt előírások megszegése az adott szolgáltatásból való kitiltással, a Microsoft fiók megszüntetésével, vagy a kommunikáció esetleges blokkolásával járhat, a kivizsgálások során pedig a vállalat fenntartja a jogot a felhasználói tartalmak ellenőrzéséhez. **Bővebben...**

Vizsgálat indul a Facebook adatvédelmi gyakorlata ellen

(www.securityweek.com)

A Szövetségi Kereskedelmi Bizottság (FTC) március 26-án közzétette, hogy vizsgálatot indít a Cambridge Analytica által begyűjtött több tízmillió Facebook-os felhasználói adattal kapcsolatban, annak tisztázására, hogy a közösségi platform részéről történt-e hűtlen adatkezelés. Tom Pahl, az FTC fogyasztóvédelmi vezetője elmondta, hogy annak kiderítése is kiemelt fontossággal bír, hogy sérült-e az amerikai-európai adatvédelmi megállapodásnak (Adatvédelmi Pajzs) való megfelelés, illetve, hogy a cég végez-e olyan tevékenységet, amellyel kárt okozhat a fogyasztóinak. Ezzel párhuzamosan a Szenátusi Bírói Bizottság elnöke április 10-én meghallgatásra várja a Facebook vezérigazgatóját, hogy megvitassák a cég személyes adatok védelmével és monitorozásával kapcsolatos múlt- és jövőbeli politikáját. Emellett több iparági vezetőt is vár hasonló témájú megbeszélésre. A német igazságügyi miniszter eközben szigorúbb felügyeletet gyakorolna a Facebook felett. **Bővebben...**

Hangsúlyosabb szerephez jutnak a mobilra optimalizált weboldalak

(www.bleepingcomputer.com)

A Google közleményben tudatta, hogy áttér a „mobil-first" indexelésre, ami azt jelenti, hogy immár a weboldalak mobil verzióját részesíti előnyben az indexelés során. Az eredeti keresési algoritmusban először a 2010-es évek elején eszközölt változtatást a cég, amikor bevezették a „mobilbarát" címkéket, majd egy évvel később már lényeges módosítás jött, amikortól a Google már különböző találatokat jelenített meg a hagyományos PC-n, valamint a mobil platformon netezőknek. A cég azonban – a mostani változtatással is – kinyilvánította szándékát, hogy nem kíván két külön indexet vezetni a weboldalakról, és figyelembe véve a felhasználók internetezési szokásainak a mobil eszközökre való áttérését, indokoltnak tartja a mobil tartalmak preferálását. Hozzáteszik azonban, hogy tartalmi eltérés esetén, amennyiben az asztali változat az adott keresési paraméterek alapján relevánsabb találatot jelent vagy a mobil verziónál gyorsabban töltődik, továbbra is az kerül megjelenítésre. **Bővebben...**

Szigorítás a nem tanúsított Androidos készülékek esetében

(www.xda-developers.com)

A Google tiltja a saját fejlesztésű alkalmazásaihoz való hozzáférést azon eszközökön, amelyek általuk nem tanúsított Android verziókat futtatnak, így az érintettek többek között a Google fiókjukba sem tudnak bejelentkezni. A tech óriás tavaly vezette be az eszköztanúsítási rendszerét, melynek célja a Google alkalmazásokkal rendelkező Androidos eszközök megfelelő működésének biztosítása és a felhasználók védelme. A problémával szembesülő felhasználók számára javasolt felvenni a kapcsolatot a készülék gyártójával, ugyanakkor, ha az eszközön egy ún. egyedi (vagy más szóval „főzött") ROM – azaz egy nem hivatalos, módosított Android verzió, mint például a Lineage OS – került telepítésre, úgy a Secure Android ID megadása mellett van lehetőség feliratkozni egy fehérlistára, amivel megkerülhető a korlátozás. Ezzel kapcsolatban azonban megjegyzendő, hogy egy felhasználó összesen 100 ilyen azonosítót regisztrálhat. A témával kapcsolatban hivatalos közlemény nem érhető el. **Bővebben...**

IT biztonsági Tanács

iPhone-ok esetében az alapértelmezett jelszótípus egy 6 jegyű numerikus kód, azonban biztonságosabb egy alfanumerikus jelszó használata.

Ennek a beállításához indítsuk el a „Beállítások" alkalmazást, majd válasszuk ki a „Touch ID és jelkód" menüpontot, ezen belül pedig a „Jelkód módosítása" elemet. Az aktuális jelszó megadása után a „Jelkódbeállítások"-ra koppintva van lehetőség a jelszó típusának módosítására.

Nemzeti stratégiát alkottak a kiberbiztonsági exporttevékenység élénkítéséhez az Egyesült Királyságban

(www.computing.co.uk)

A brit kormányzat egy új stratégiát mutatott be, melynek célja, hogy megkönnyítse az ország kiberbiztonsági cégei számára termékeik és szolgáltatásaik értékesítését a tengerentúlon. Liam Fox, a nemzetközi kereskedelemért felelős miniszter tárta fel a kormány új Kiberbiztonsági Export Stratégiáját, amely célként fogalmazza meg Nagy-Britannia és a NATO tagországok kibervédelmi képességének erősítését. A most ismertetett keretrendszer – ami a Nemzeti Kiberbiztonsági Stratégia kiterjesztéseként fogható fel – a szigetország mintegy 800 kiberbiztonsági vállalata számára újabb szerződéskötéseket szeretne kiharcolni és biztosítani a jelenleg jellemző 1,5 milliárdos éves összhozam további növelését a következő évek során. Fox azonban azt is hozzátette, hogy a koncepció a kereskedelmi és biztonsági érdekek mellett figyelembe veszi az emberi jogokat is. **Bővebben...**

Megjelent a TLS 1.3

(www.bleepingcomputer.com)

Az internetes szabványokat gondozó Internet Engineering Task Force elfogadta a webes kommunikáció titkosítására használt Transport Layer Security (TLS) protokoll új, 1.3-as verzióját. Mindez egy négy éves folyamat eredményeként jött létre, melynek során a 28. tervezetet fogadták el véglegesként. Az új szabvány lényeges újításai között szerepel, hogy a régebbi titkosítási algoritmusokat (MD5, SHA-224) olyan korszerűbbekre cseréli, amelyek feltörése jóval nehezebb (például a ChaCha20, a Poly1305, az Ed25519, az x25519, és az x448), illetve, hogy a kliens és a szerver között a kapcsolat felépülésének ideje is jelentősen rövidült. A talán leginkább lényeges újítás azonban mégis az, hogy a TLS 1.3 már rendelkezik az olyan támadások elleni védelemmel, amelyek során a támadó igyekszik kikényszeríteni a szervertől, hogy az egy korábbi, sérülékeny TLS verziót használjon a kommunikáció során. A nagyobb böngészők (Chrome, Edge, Firefox, vagy a Pale Moon) a korábbi tervezeteket már támogatták, így nem várható implementációs probléma e téren, sokkal inkább a hálózati eszközök esetében, amelyeknél firmware frissítés szükséges. **Bővebben...**

Uniós szintű értékelésen estek át a távközlési protokollok

(www.enisa.europa.eu)

Az ENISA tanulmányt készített az elektronikus hírközlési rendszereket érintő kockázatokról, melynek során azt találták, hogy a régóta használt technológiák komoly veszélyt hordoznak magukban. Az EU-s szintű felmérés legfontosabb megállapításai között szerepel, hogy a 2G/3G mobilhálózatok első generációi egy évtizedekkel ezelőtt tervezett protokollra (SS7) épülnek, amely a biztonsági szempontok figyelembe vétele nélkül készült. Szerencsére egyes fejlett szolgáltatók ezt felismerve bizonyos alapszintű biztonsági intézkedéseket már bevezettek, azonban az ügynökség szerint a megfelelő védelem biztosításához ennél jóval nagyobb figyelmet kell fordítani erre a területre. A jelenlegi 4G hálózatok esetében egy már valamivel fejlettebb jelátviteli protokollt alkalmaznak (Diameter), ám ennek a sérülékenysége is bizonyított. A jövőt jelentő 5G technológia még fejlesztés alatt van, az ENISA azonban úgy véli nagy a veszélye annak, hogy a korábbi biztonsági problémák itt is megjelennek. Az összefoglaló a problémák feltárása mellett ajánlásokat is megfogalmaz az Európai Bizottság, a nemzeti hatóságok, valamint az ipari szereplők számára. **Bővebben...**