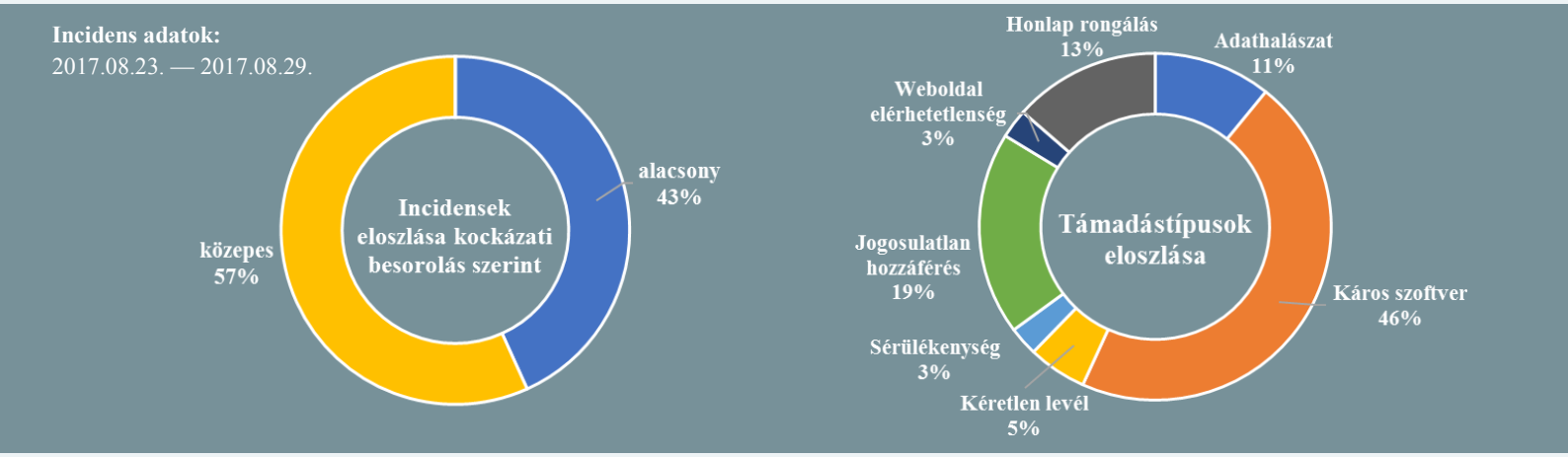


Digitális valutákra vonatkozó szabályok

(www.thestar.com)

Új előírások állnak kidolgozás alatt Kínában a kriptodevizák bevezetésére vonatkozóan, amelyeket átmenetileg be is szüntethetnek a szabályzatok elkészültéig - adta hírül a Caixin kínai pénzügyi lap. A digitális fizetőeszközök jogi szempontból továbbra is „szürke zónában" vannak, annak ellenére, hogy a vállalatok egyre gyakrabban használják őket tőkebevonásra nyilvános felhívások, ún. ICO-k (Initial Coin Offering) vagy ITO-k (Initial Token Offering) során. Az ilyen kezdeményezések segítségével a kibocsátók – lényegi szabályozási felügyelet nélkül – jelentős összegeket képesek felhalmozni. A Xinhua kormányzati hírügynökség erre vonatkozó júliusi jelentése szerint idén az ICO és ITO tevékenységek jelentősen megnövekedtek Kínában: mintegy 65 ICO kapcsán 2,62 milliárd yuan gyűlt össze, 105 000 szponzortól. **Bővebben...**

Új európai adót mérnek az amerikai tech óriásokra

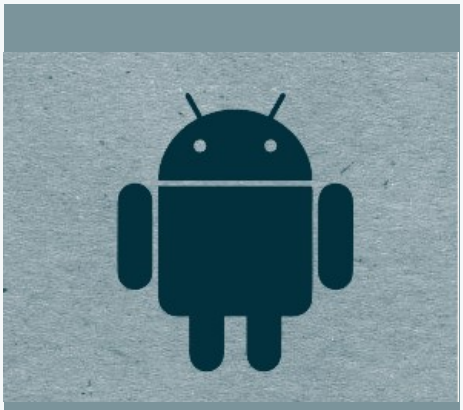
(www.thestar.com)

Bruno Le Maire francia pénzügyminiszter egy Facebook Live chatben tett nyilatkozata szerint Németország és Franciaország új indítványt tervez a tech vállalatok adóztatására vonatkozóan. Ennek nem titkolt célja, hogy az érintett cégek bevételeikkel arányosan járuljanak hozzá a közterviseléshez azon országok esetében, ahol a jövedelmet szerzik. A részleteket a pénzügyminiszterek következő találkozóján szeretnék bemutatni a nagy tech vállalatoknak – mint a Google, az Apple, a Facebook és az Amazon – amely szeptember közepén, Tallinban kerül majd megrendezésre. Az elképzelések szoros összhangban állnak Emmanuel Macron francia elnök választási kampányában hangoztatott ígéretével, miszerint kemény fellépést tervez az amerikai tech cégekkel szemben, a jelenlegi alacsony adókulcsot "tisztességtelennek" nevezve. **Bővebben...**

Történelmi jelentőségű kibertámadásra számíthat az Egyesült Államok

(www.nextgov.com)

Az USA kritikus infrastruktúrái kiberbiztonsági szempontból aggasztó állapotban vannak, állítja az amerikai belbiztonsági hivatal tanácsadó testülete, a NIAC (National Infrastructure Advisory Council). Ezt az álláspontot több száz korábbi tanulmány és mintegy 38, főképp a pénzügyi és az energetikai szektor terén dolgozó IT biztonsági szakemberrel folytatott interjú során alakították ki. A jelenlegi helyzetet egy – a 2001. szeptember 11-ei terrortámadáshoz hasonlóan – vízválasztó esemény előtti állapotként jellemzik, ami a kormányzat és a kritikus fontosságú iparágak szereplőitől azonnali intézkedéseket és hatékony összefogást kíván. A tanulmány tizenegy fő javaslatot fogalmaz meg, amelyek lényegesen hozzájárulhatnak a biztonsági szint növeléséhez. Például kiemelik a fenyegetettség felderítés (threat intelligence) fontosságát és kritikát fogalmaznak meg a hírszerző ügynökségekkel szemben, miszerint gyakrabban és szélesebb körben kellene a felderített fenyegetésekre vonatkozó információkat elérhetővé tenniük. **Bővebben...**



Egységes biztonsági tanúsítási programot kezd a Google

(www.techradar.com)

A nyílt rendszerekre jellemzően az Androidot futtató eszközök is magukban hordozzák annak a fokozott esélyét, hogy káros kóddal fertőzött alkalmazás települjön rájuk, illetve gyakorta szenvednek hibás kódolásból fakadó problémáktól. A Google ezt felismerve gyártókkal, eladókkal és fejlesztőkkel közreműködésre lépve egy jóváhagyási rendszer segítségével szeretné informálni a felhasználókat az ajánlott termékekről, amelyek csomagolására a 'Google Play Protect' logója kerül majd. Azok a telefonok, tabletek, valamint egyéb eszközök kaphatják meg a jóváhagyást, amelyek teljesítik a biztonságra vonatkozó szigorú előírásokat. **Bővebben...**

IT biztonsági Tanács

Egyre több vállalat ismeri fel a biztonsági eseménykezelő rendszerek (SIEM) fontosságát. A hatékony működéshez azonban elengedhetetlen a releváns 'use case'-ek és korrelációs szabályok felállítása és folyamatos karbantartása.

Ennek alapja az átfogó kockázatelemzés és auditálás, a fenyegetés management és a belső folyamatok megfelelő szervezése.

Ezúttal India és Pakisztán volt a célkeresztben

(www.securityaffairs.co)

A Symantec IT biztonsági cég egy újabb Indiával és Pakisztánnal szembeni kémkedési kampányról közölt információkat. Elemzések alapján ugyan feltételezhetően több hacker csoport is közreműködött a kampányban, azonban "az alkalmazott technikák és módszerek" arra engednek következtetni, hogy azt azonos cél, vélhetően egy idegen állam érdekében tették, ám ezzel kapcsolatban több részletet nem árultak el.

A támadás során az "Ehdoor" hátsó ajtó segítségével kompromittálták a célzott eszközöket, mely támadási módszert a Symantec először 2016 szeptemberében észlelte a Közel-Keleti régióban, amikor kormányzati és katonai szervezeteket támadtak. **Bővebben...**

Adatvédelem a Brexit után

(www.independent.co.uk)

A brit adatvédelmi törvények továbbra is összhangban maradnak az EU adatvédelmi irányelveivel, miután az Egyesült Királyság kilép az Európai Unióból - hangsúlyozta a brit kormány. A múlt hét során kiadott munkadokumentumban a brit kormányzat Európai Uniós kilépésért felelős részlege (DExEU) felvázolta a személyes adatok az Európai Unió és az Egyesült Királyság közötti biztonságos és szabályozott módon történő megosztására vonatkozó javaslatait. A brit vállalatvezetői szövetség (Institute of Directors) EU-s és kereskedelmi szabályzatokért felelős vezetője üdvözölte a hírt, azonban kifejtette, hogy a kormánynak rövid távon elsősorban a megfelelőségértékelést kellene előnyben részesítenie, semmint, hogy egy véglegesnek szánt egyedi modellt dolgozzon ki, ami sokkal inkább egy hosszabb távú feladat. **Bővebben...**

Ismét kibertámadás érte a brit egészségügyet

(www.ibtimes.co.uk)

A 2017 májusában pusztító 'WannaCry' zsarolóvírus kampány után ismét kibertámadás érte az Egyesült Királyság egészségügyi hatóságának infrastruktúráját. Az eddigi információk szerint ezúttal a skót Lanarkshire-beli NHS központ és a körzet kórházai, valamint egyéb egészségügyi ellátó pontjai álltak a célkeresztben. A támadás miatt a betegeket arra kérték, hogy csak vészhelyzet esetén keressék fel a kórházakat, mivel az egészségügyi dolgozók nem tudtak hozzáférni a páciensek egészségügyi adataihoz, valamint a levelező rendszerhez sem. Az incidens augusztus 25-én történt, amellyel kapcsolatban részletes információkat mindeddig nem közöltek, mivel a kivizsgálás még tart. Mindössze annyit hoztak nyilvánosságra hogy a káros kód nem azonos azzal, ami májusban terjedt. **Bővebben...**

Újabb internetes megszorításokat vezetnek be Kínában

(www.ibtimes.co.uk)

2017 október 1-től lép életbe a kínai kormányzat internetes szabályzásért felelős intézményének (CAC) új szabályzata, amelynek értelmében a felhasználók immár csak valós adatokkal regisztrálhatnak internetes fórumokon és más platformokon, ennek ellenőrzéséért pedig az internetes cégek és szolgáltatók lesznek felelősek, csakúgy, mint a szabálysértések azonnali jelentéséért a hatóságok számára. Az anonimitás kizárása mellett az online médián közölt információra vonatkozóan létrehoztak egy részletes tiltólistát. **Bővebben...**