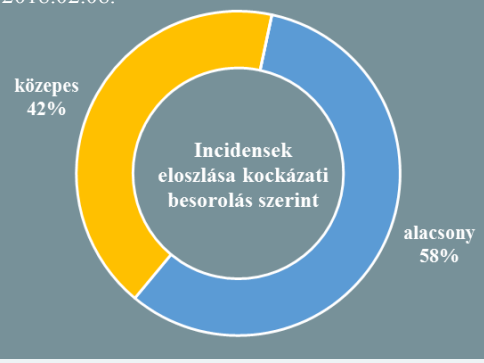
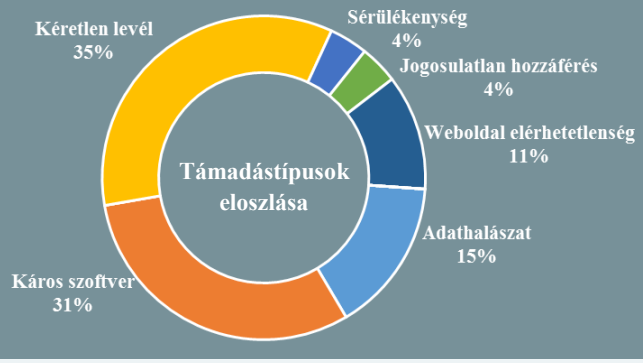
Incidens adatok: 2018.02.02. — 2018.02.08.





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

Biztonságos Internet Nap 2018

(www.ec.europa.eu)

Idén 2018. február 6-án kerül megrendezésre a Biztonságos Internet Nap (Safer Internet Day - SID), melynek idei jelmondata: „Alkoss, csatlakozz, tiszteld a másikat: a jobb internet veled kezdődik!”. A SID célja – összhangban az Európai Biztottság jobb internetet célzó stratégiájával – a biztonságosabb és felelősségteljesebb online technológia-használat hirdetése a fiatalkorúak számára. Az események során nem csupán az aktuális veszélyekre – például az online zaklatásra – hívják fel a figyelmet, hanem konkrét ajánlásokat is tesznek a biztonságosabb online jelenlét megvalósítása érdekében. A program 2004-ben indult az Európai Unió SafeBorders projekt részeként, mely az évek során túlnőtt az eredeti elképzelésen és mára világszerte mintegy 100 ország részvételével biztosítanak különböző programokat az érdeklődőknek. A program hivatalos, angol nyelvű weboldalán eljuthatunk a résztvevő országok listájához, amelyen az államok saját nyelvű weboldalához is találunk elérhetőséget. Itt tájékozódhatunk a programokról, kiadványokról. **Bővebben...**

A digitális devizapiac szabályozására készül az Egyesült Államok

(www.reuters.com)

Az amerikai pénzügyi szabályozó testületek egy 2018. február 06-án megrendezésre kerülő kongresszusi meghallgatáson tervezik felhívni a törvényhozók figyelmét a kriptovalutákkal való kereskedést szabályozó új szövetségi keretrendszer megalkotásának fontosságára. Egyes kongresszusi források szerint az ülés nagy valószínűséggel az Amerikai Határidős Árutőzsde Felügyelet (CFTC) és az Amerikai Értékpapírpiaci és Tőzsdefelügyelet (SEC) hatásköreire fókuszáló tényfeltáró gyakorlat lesz, arra összpontosítva, hogy azok mennyiben képesek megvédeni a befektetőket az árfolyam-ingadozásoktól, a különféle megtévesztő tevékenységektől, valamint a kiberbűnözőktől. Jelenleg ugyanis nincs olyan szervezet, melynek ez dedikált feladata lenne és az sem tisztázott, hogy melyik testület tölthetné be ezt a szerepet. A jogi szempontból szürke zóna felszámolása azonban egyre sürgetőbb, amelyre jó példa a japán valutaváltó Coincheck-et ért incidens, amelynek során a támadók 530 millió dollár értékben tulajdonítottak el kriptovalutákat. **Bővebben...**

A számítógépes bűnözés felé hajlanak a brit tinédzserek

(www.bleepingcomputer.com)

A 2017-es év végén nyilvánosságra hozott University College London (UCL) kutatói által készített tanulmány szerint az egyesült királyságbeli 11 és 14 év közötti fiatalok többsége jobban érdeklődik a számítógépes bűncselekmények, mint más deviáns magatartásformák (például a dohányzás, a drogfogyasztás, lopás) iránt. Kiderült, hogy a válaszadók 4,8%-a kísérelt már meg illetéktelenül hozzáférni más felhasználó közösségi oldalához, e-mail fiókjához vagy számítógépéhez, 0,9%-uk pedig rosszindulatú programokat is terjesztett az Interneten keresztül. Ezzel szemben a „hagyományos” bűncselekmények számosságukat tekintve csökkenő tendenciát mutatnak, ám a testi sértés okozása még így is vezető bűncselekmény. Egy másik vizsgálat, amelyet a National Crime Agency végzett, pedig arra jutott, hogy a brit hackerek átlagos életkora 17 év, és a fő motiváló erő társaik elismerésének a kivívása. **Bővebben...**.

Az iBoot-nál jóval több belső információ szivárogtatott ki az Apple-től

(www.motherboard.vice.com)

Az incidens egy meg nem nevezett iPhone kutató szerint az Apple történetének eddigi legsúlyosabb adatszivárgása és módot adhat hibák és sérülékenységek felderítéséhez, annak ellenére, hogy az még az iOS 9-es verziója esetében volt használatban. Az online magazin úgy tudja, egy alacsony beosztású dolgozó lopta el a kódot és osztotta meg a jailbreak közösségbeli barátaival. Maga a szivárogtató – az Apple-lel kötött titoktartási szerződésre hivatkozva – nem szólalt meg a témában, a Motherboard szerint az értesülések két olyan személytől származnak, akik első körben kapták meg tőle a kódot. Ők úgy tudják, hogy jóval több belső információ szivárgott ki a cégtől, mint ami a GitHub-on hozzáférhetővé vált. Elmondásuk szerint ezeket a bizalmas információkat eredetileg nem szándékozták megosztani a széles nyilvánossággal, kizárólag saját kutatásaikhoz akarták felhasználni. Az eredeti körből – jelenleg tisztázatlan körülmények között – kikerült kód 2017 őszén egy Discord csoport tagjai között kezdett terjedni, majd először egy Reddit poszt során, ezt követően pedig a GitHubon vált publikussá. **Bővebben...**

IT biztonsági Tanács

Az interneten számos veszély (pornográfia, adatszivárgás, zaklatás stb.) leselkedik a kiskorúakra, amikkel szemben célszerű az ún. gyermekvédelmi szűrőszoftverek alkalmazása. Ezek az alkalmazások szülői felügyeletet biztosítanak a gyermekek számítógépes tevékenységeinek ellenőrzéséhez és az online tartalmakhoz való hozzáférés korlátozásához.

Az ilyen jellegű szoftvereket az internet-hozzáférést nyújtó szolgáltatók kötelesek elérhetővé és használhatóvá tenni ügyfeleik számára.

Házkutatást tartottak a Coincheck-nél

(www.securityweek.com)

A japán hatóságok egy héttel azt követően vonták vizsgálat alá a tokiói központú virtuális pénzváltó céget, hogy mintegy 530 millió dollárnyi értékű 'NEM' kriptovalutát tulajdonítottak el tőlük. A kutatást a japán pénzügyi szabályozó szerv FSA (Financial Services Agency) munkatársai végezték a Coincheck székházában, Taro Aso pénzügyminiszter szerint a helyszíni vizsgálatra az ügyfelek vagyonának biztosítása miatt volt szükség. A hiatal szerint a Coincheck mulasztott a biztonsági előírások terén, és emiatt sérülékennyé vált a január 26-án történt adatlopással szemben. Az FSA február 13-ig adott határidőt a cégnek, hogy kivizsgálják az eseményt és meghozzák a megfelelő védekező intézkedéseket. A vállalat válaszában arról biztosította a hatóságot, hogy mind a 260 000 érintett ügyfelét kártalanítja, hivatalos valutában (jen), összesen 422 millió dollár értékben. **Bővebben...**

Alacsony színvonalú a kis- és középvállalkozások védelme Ausztráliában

(www.itwire.com)

A kis-és középvállalkozások (SMB) közel fele nem áll készen arra Ausztráliában, hogy megbirkózzon a 2018. február 22-én hatályba lépő adatszivárgásról szóló törvény támasztotta követelményekkel – állítja egy új tanulmány. Eszerint az SMB-k csupán 18%-a rendelkezik megfelelőségi politikával, habár 33%-uknál legalább folyamatban van annak kidolgozása. A 10 és 99 fő közötti létszámú vállalkozások tekintetében végzett felmérés olyan főbb kockázati tényezőket is azonosított, mint például, hogy az SMB-k 57%-a az elmúlt 12 hónapban nem végzett kockázatértékelést, vagy hogy 63% esetében megengedett a távoli munkavégzés és az adatokhoz való hozzáférés is. A saját készülékek használatával kapcsolatban kiderült, a válaszadó cégek csupán 44%-ánál volt érvényben erre vonatkozó biztonsági szabályzat és csak 37%-nál korlátozták az ily módon hozzáférhető adatok körét. Paul Gracey, a felmérést végző HP South Pacific Printing System igazgatója kiemelte, hogy a szervezetek általában kizárólag harmadik féltől vásárolt szoftverekre bízzák a védelmüket, azonban a kívánt biztonsági szint eléréséhez integráltabb megoldások alkalmazására van szükség. **Bővebben...**

Adatszivárgás Svájc legnagyobb telekommunikációs szolgáltatójánál

(www.securityaffairs.co)

A Swisscom bejelentette, hogy egy rutin ellenőrzés során tudomásukra jutott, hogy adatok szivárogtak ki a cégtől, közel 800 000 felhasználót érintően, ami összehasonlításképp a teljes svájci népesség közel 10 %-át jelenti. A cég a felfedezést követően maga jelentette az incidenst az illetékes svájci hatóságnak (FDPIC), valamint közleményben tájékoztatta a nyilvánosságot. Eszerint a kivizsgálás során megállapításra került, hogy a támadók 2017 őszén egy üzleti partner azonosítói segítségével szereztek jogosulatlan hozzáférést a vállalat adataihoz. A legtöbb kompromittálódott adat mobil szolgáltatás előfizetésekhez kapcsolódik, köztük olyanok, mint az ügyfelek neve, címe, telefonszámai és születési ideje. A cég azzal védekezik, hogy a hatályos adatvédelmi jogszabályok értelmében ezek nem számítanak érzékeny információnak, illetve, hogy más forrásból (például üzletszerzési listák) is hozzáférhetőek. Védekező intézkedésként szigorították a partner szervezetek hozzáféréseit, még idén bevezetik számukra a kétfaktoros hitelesítést, illetve letiltották azokat a lekérdezéseket, amelyek a teljes ügyfélkörre irányulnak. **Bővebben...**