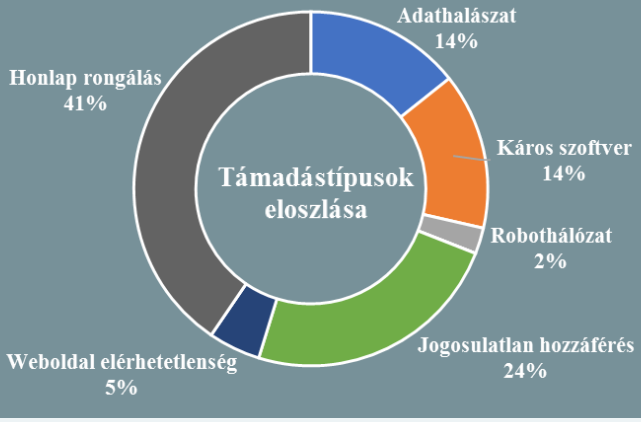
Incidens adatok:
2017.09.06. — 2017.09.12.



EU-s kibervédelmi gyakorlat

(www.thestar.com)

Múlt hét csütörtökön került megrendezésre az Európai Unió védelmi miniszterei számára tartott első kiberháborús játék, amelynek során egy informaikai támadásra való reagálást teszteltek. A szimuláció során hackerek egy haditengerészeti küldetést szabotáltak, ezzel párhuzamosan pedig közösségi platformokon egy, az EU-s intézkedésekre irányuló lejárató kampányba kezdtek. A korábbi hasonló eseményekkel szemben újdonság volt, hogy egy olyan esetet írt le, amiben a katonai műveleti parancsnokság átmenetileg elérhetetlenné válik. Ezzel kapcsolatban a minisztereknek több döntést is meg kellett hozniuk, például, hogy nyilvánosságra hozzák-e az eseményeket. **Bővebben...**

Oroszországban is szabályoznák a kriptovaluták piacát

(www.thestar.com)

Az orosz kormányzat szabályozni kívánja az országon belüli kriptovaluta forgalmat, mondta Anton Siluanov orosz pénzügyminiszter. Kezdetben az orosz pénzügyi hatóságok élesen léptek fel a nem állami ellenőrzés alatt működő intézmények által kibocsátott fizetőeszközökkel szemben, azonban mára elfogadják a kriptovaluták globálisan növekvő piacát. "A tiltás értelmetlen lenne, szabályzásra van szükség." - nyilatkozta Siluanov. Ennek értelmében a pénzügyminisztérium szándéka szerint az év végéig kidolgozza a törvényjavaslatot, amely meghatározza a virtuális valuták vásárlásának rendjét, amelybe beletartozik a vásárló személyének regisztrálása is. Siluanov szerint a virtuális pénzeket a háztartásokra vonatkozó értékpapír vásárláshoz hasonlóan kellene szabályozni.
Bővebben...

Adatvédelmi szabályokat sértett a Facebook

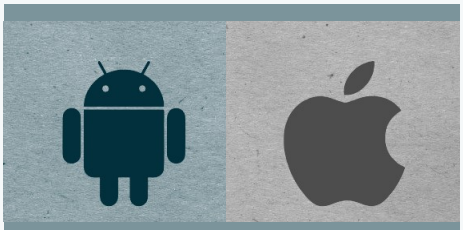
(www.securityaffairs.co)

A spanyol adatvédelmi ügynökség (AEPD) 1,2 millió eurós bírságot szabott ki a Facebookra az adatvédelmi szabályok megsértésének vádjával. Az AEPD állítása szerint a tech óriás anélkül gyűjti a felhasználók adatait, hogy egyértelmű tájékoztatást adna, miként használja fel azokat kereskedelmi célra. Továbbá szerintük az adatgyűjtés kiterjed az olyan különösen érzékeny személyes adatokra is, mint a szexuális beállítottság, a vallási nézetek, vagy a böngészési szokások. Szintén súlyos jogsértés, hogy az összegyűjtött felhasználói adatokat a felhasználás után sem törlik maradéktalanul. A Facebook nem ért egyet a vádakkal és azzal védekezik, hogy a felhasználók maguk választják meg a nyilvánossággal megosztott adatok körét, melyeket nem használnak fel célzott hirdetésekhez. **Bővebben...**

Kanadában engedélyezték a Bitcoin Befektetési Alapot

(www.motherboard.com)

Júliusban létrejött az első kanadai, 'Bitcoin Trust' nevű kriptovaluta befektetési alap, amelyet a Vancouver székhelyű First Block Capital (FBC) hozott létre, a régióban felelős British Columbia Securities Commission szabályozási ügynökség jóváhagyásával. Ez a pénzügyi megoldás lehetővé teszi, hogy pusztán a Bitcoin növekvő árfolyama termeljen profitot, így a befektetőknek valójában egyetlen Bitcoin-t sem kell vásárolniuk. Közleménye szerint a BCSC nyitott további kriptovaluta alapok engedélyezésére is, amennyiben azok teljesítik a megfelelőségi előírásokat. Az Egyesült Államokban egy hasonló kezdeményezés bukott el ez év márciusában. **Bővebben...**



Androidos eszközöket célzó fenyegetések

(www.itproportal.com)

Az Avast biztonsági cég a Mobile World Congress-en mutatta be legújabb tanulmányát, miszerint az Androidos eszközöket célzó támadások 40%-al nőttek 2016-hoz képest. A top három fenyegetés közé tartozik a kémkedés, a rosszindulatú, valamint az illegális, hamis alkalmazások. **Bővebben...**

Ultrahangos támadás

(www.nakedsecurity.com)

Múlt héten a kínai kutatók tanulmánya szerint több hangalapú alkalmazás (mint a Siri, a Google Now, stb.) Az emberi hangtartományon kívül eső hangutasításokra is reagálnak. A támadók az ultrahangos hangparancsokat kiadva a felhasználó tudta nélkül káros tevékenységet folytathatnak az eszközökön, ezt a támadás típust "delfin támadásnak" (Dolphin Attack) nevezték el. **Bővebben...**

IT biztonsági Tanács

A Google-féle G Suite használatakor az alábbi javaslatok segíthetnek növelni a biztonságot:

- 2-faktoros autentikáció, „Password Alert” Chrome kiegészítő, DMARC policy és „Work profile”-ok használata.
- Külső domain-es leveleknél a felugró figyelmeztető üzenetek figyelése.
- Az alkalmazás beállítások csoportokban való kezelése.

Új európai kiberbiztonsági törvényjavaslat

(www.enisa.europa.eu)

Jean-Claude Juncker hivatalosan bejelentette az Európai Bizottság javaslattételét az ENISA jövőjére vonatkozó szabályzásról, amely a 'Kiberbiztonsági Törvény' nevet kapta. A tervezet megerősíti az ENISA szerepét és lehetővé teszi az Ügynökség számára, hogy jobban támogassa a tagállamok, a NIS irányelveknek való megfelelőségének kialakítását. Alapvetően két új feladatcsoport jelenik meg, amelyekben fontos szerep hárul az ENISA számára, a Kiberbiztonsági Krízis Menedzsment, és az ICT termékek és szolgáltatások kiberbiztonsági tanúsítvány rendszere és szabványosítása. **Bővebben...**

Az Európai Unió növelné a kibervédelmi kiadásokat

(www.firstpost.com)

Az Európai Bizottság a magasabb kibervédelmi szint érdekében több intézkedést is tervez, például átmenetileg növelni kívánja a technológiai beruházásokat, a felhasználók védelme érdekében szigorúbb biztosítékokat vezetne be és nagyobb hangsúlyt fektetne a támadások diplomáciai úton történő megelőzésére. A konkrét javaslatokat e hónap során kívánják nyilvánosságra hozni, amelyek között – egy kiszivárgott dokumentum szerint – olyanok szerepelnek, mint titkosítási képességek fejlesztése biztonságos digitális azonosító rendszerek létrehozásához újgenerációs kvantum technológia felhasználásával, a szellemi tulajdon fokozott védelme és a biztonságos e-kereskedelem. Új elemként jelenik meg az "ellátási kötelezettség" elve a szoftverfejlesztés terén. **Bővebben...**

Meghosszabbításra vár az amerikai megfigyelési törvény

(www.nytimes.com)

A Trump adminisztráció sürgeti az amerikai Kongresszust, hogy minél előbb újítsák meg az év végén lejáró külföldi hírszerzési-megfigyelési törvényt, mely lehetővé teszi a kormányzat számára az információgyűjtést azon személyekről, akik gyanús tevékenységet, például fegyverkereskedelmet, terror - és/vagy kiberbűnözői tevékenységet folytatnak az Egyesült Államokon kívül. Jeff Session főállamügyész és Dan Coats a Nemzeti Hírszerzőügynökség Igazgatója arra kérik a Kongresszust, hogy ne csak meghosszabbítsák, hanem állandó törvényként rögzítsék azt. A legtöbb republikánus és demokrata támogatja a tevékenység folytatását, azonban egyesek szerint szükséges a határozott idejű meghosszabbítás a törvény időszakos felülvizsgálata miatt. **Bővebben...**

Átfogó intézkedések az amerikai kritikus infrastruktúrák védelmében

(www.infosecurity-magazine.com)

Az Egyesült Államok Energiaügyi Minisztériuma (DOE) 20 IT biztonsági projektet indít az olaj, a villamos energia és a földgáz infrastruktúrák, akár a szélsőséges időjárási viszonyokkal, akár a kibertámadásokkal szembeni ellenálló képességének növelése érdekében. A DOE célja az állami- és a magánszektorral szoros együttműködésben olyan energetikai szállító rendszerek létrehozása, amelyek az esetleges támadások és incidensek során is képesek a kritikus szolgáltatások nyújtására. Ennek biztosításához a koncepciónak a tervezés, a telepítés és üzemeltetés szintjén is meg kell valósulnia. Rick Peery Energiaügyi Miniszter szerint a kritikus infrastruktúrák rendelkezésre állásának kérdését kiemelten kezelik, hiszen az elengedhetetlen az állampolgárok biztonságához és a gazdaság működéséhez. **Bővebben...**