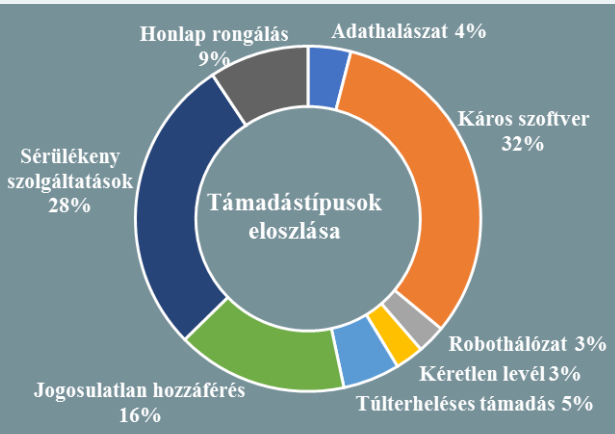
Incidens adatok:
2017.06.07. — 2017.06.13.



Angela Merkel felszólalt a digitális világ globális szabályzása mellett

(www.mobile.reuters.com)

A német kancellár szerint a pénzügyi és kereskedelmi piacokhoz hasonlóan az IT ipar átfogó szabályzására is szükség van, amelyről Mexikóvárosban tett látogatásakor beszélt. Németország, kihasználva a jelenlegi G20-as elnökségét, egy akcióterv kidolgozását tűzte ki célul, hivatkozva egy, a bankszektort célzó kibertámadások elleni harcról történt G20-as megállapodásra. A tervek szerint a jövő hónapban esedékes hamburgi találkozó során a 'szélessávú internetelérés mindenkinek' program mellett tárgyalnak majd a közös szabványok kérdéséről is. Merkel továbbá felhívást intézett az Egyesült Államok felé, úgy véli közösen kell dolgozni a problémán. **Bővebben...**

Összefogás a „blockchain” technológiák bűnözői felhasználása ellen

(www.enterpriseinnovation.net)

Egy új kezdeményezés szerint az Európai Unió finanszírozásában létrejön egy konzorcium (TITANIUM) a blockchain technológiák (amelynek alapján működik például a Bitcoin is) bűnözéssel és terrorizmussal összefüggésbe hozható használatának detektálására, megelőzésére és a bűnüldöző hatóságok munkájának technikai támogatására. A projekt további célja az európai hatóságok munkatársainak technikai képzése is. Az ötmillió eurós projektet három évre tervezik és a résztvevők között található az osztrák és a spanyol belügyminisztérium, több egyetem, valamint az Interpol is. "Olyan megoldásokat keresünk, amelyek a hatékonyság mellett a polgárok személyes adatainak védelmét is figyelembe veszik" - mondta a konzorcium vezetője, Ross King. **Bővebben...**

A „Fraud guide”-ok valós veszélyt hordoznak

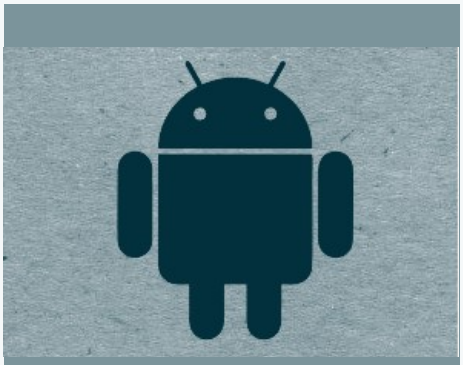
(www.helpnetsecurity.com)

Egy, a dark weben fellelhető, csalási technikákat leíró, ún. ’fraud guide’-okat vizsgáló kutatás során elemzők megállapították, hogy az ilyen dokumentumok nagyjából 20%-a alkalmas arra, hogy felhasználásukkal potenciálisan kárt okozzanak. Ezek a kézikönyvek általában arra vonatkozóan tartalmaznak információkat (esetenként igazán részletes, step-by-step leírásokat), hogy hogyan lehetséges legitim szabályokat és folyamatokat kihasználni, vagy káros kódot alkalmazni a szervezetek kompromittálására. Ezek jellemzően olyan népszerű mélywebes online piacokon keresztül érhetők el, mint az AlphaBay vagy a Hansa. Továbbá azt is kimutatták, hogy leginkább a pénzügyi és a kiskereskedelmi területeken működő (ezek együttesen 59%-ot tesznek ki) szervezeteket támadják. **Bővebben...**

Észtország külföldi „adat nagykövetséget” nyit

(www.dw.com)

Úttörő vállalkozásba kezd Észtország, miszerint leginkább kritikus és érzékeny adatai egy külföldön található (Luxemburg), negyedik szintű (Tier-4) adatközpontban kerülnek eltárolásra, annak érdekében, hogy egy átfogó kibertámadás esetén is elérhetőek maradjanak. Az érintett államok a következő hetekben írják alá a kétoldalú szerződést, a tervek szerint a központ az általános nagykövetségekkel megegyező védelmet fog élvezni (lásd az 1961-es bécsi egyezmény a diplomáciai kapcsolatokról). **Bővebben...**



ReCAPTCHA API az Androidra
(www.threatpost.com)

A Google fejlesztői mobil alkalmazásokhoz is elkészítettek egy API-t, amely alapvetően a jól bevált CAPTCHA technikát alkalmazva segít kiszűrni a botokat a valódi (emberi) felhasználók közül. Az újítás szerint az Android API azonban egy "láthatatlan" reCAPTCHA-t fog alkalmazni, amely a háttérben azonosítja a felhasználókat – ezzel elkerülve a spammer-eket és egyéb robottevékenységeket – ezáltal a felhasználók zavartalanul használhatják eszközeiket. **Bővebben...**

IT biztonsági tanács

Az informatikai biztonsági problémák esetében is fontos elv a „jobb félni, mint megijedni". Amennyiben a megszokottól eltérő működést tapasztalunk eszközeinken (pl.: lassulás, indokolatlan leállás, stb.) célszerű utána járni a lehetséges okoknak.

Minden tapasztalt gyanús esetnél tájékoztassuk az informatikai részleget, vagy az ilyen esetre kijelölt személyeket és/vagy szolgáltatónkat.

Kiberbiztonsági beruházások
(www.forbes.com)

Ugyan mára sok szervezet implementál valamilyen információbiztonsági keretrendszert (például az ISO 27001/27002), azonban ezek jellemzően nem tudják lekövetni a technológiai változásokból következő problémákat. Az esetek többségében a biztonsági termékekre való beruházás inkább esemény-orientált vagy a megfelelőség biztosítása a fő motiváló erő, de ritkán képezi a stratégiai tervezés részét. Megoldást egy teljes szemléletváltás jelenthet, miszerint a biztonsági beruházásokat hosszútávon megtérülő befektetésként kell kezelni. **Bővebben...**

Drágul a Bitcoin a ransomware támadások miatt
(www.techrepublic.com)

A New York-i Corporate Governance konferencián Kirill Tatarinov a Citrox CEO vezérigazgatója azt nyilatkozta, hogy a vállalkozások többsége – a WannaCry támadás óta – több Bitcoin-t halmoz fel a zsarolóvírus támadások által követelt váltságdíjak kifizetésére, így a támadás következtében a Bitcoin árfolyama 1,692 dollárról 2,785-ra emelkedett. A hackerek körében azzal magyarázható a Bitcoin népszerűsége, hogy a hagyományos fizetési módoknál nehezebben lekövethető. **Bővebben...**

Sérül a verseny a biztonsági szoftverek piacán?
(www.searchsecurity.techtarget.com)

A Kaspersky Lab azzal vádolja a Microsoftot, hogy felhasználva piaci dominanciáját, korlátozza a független biztonsági szoftvergyártó cégek versenyképességét a piacon. A Kaspersky Lab szerint rákényszerítik a felhasználókat a Windows Defender használatára, mely a Windows 10 összes verziójában integrált és nincs mód a letiltására vagy eltávolítására, ráadásul amennyiben a felhasználó egy másik vírusvédelmi szoftvert telepít, a rendszer "nem biztonságos" minősítést kap. **Bővebben...**

Egérmozgással a személyiséglopás ellen
(www.cnet.com)

Olasz kutatók fejlesztettek ki egy algoritmust, mely képes a felhasználók hamis válaszait szűrni az egérmozgatásuk alapján. A technológia már megjelent a Google „Nem vagyok robot" alkalmazásában, amit a robottevékenységek szűrésére alkalmaztak, elemezve a kurzor mozgásának gyorsaságát és vonalvezetését. A gépi tanulást is hasznosító új módszert lehetséges, hogy a jövőben a felhasználók azonosításában is hasznosíthatják.

Bővebben...

E-bizonyítékokhoz való hozzáférés
(www.techcrunch.com)

Az elmúlt időszakban egyre gyakoribb terrorcselekmények kapcsán európai belügyminiszterek tanácskozásokat folytattak – többek között – a titkosítással kapcsolatos kérdésekről. Emellett a múlt héten tartott brüsszeli ülésen az Európai Bizottság tagjai megvitatták a bűnüldöző szervek adatokhoz való hozzáférésének problémáit, – az ún. e-bizonyítékok – EU tagországok közötti hozzáférésének lehetőségeit. Az ülés célja az adatkérés folyamatainak felgyorsítása volt, melyre három alternatíva is felmerült. Az ülés résztvevőinek mindenesetre abban sikerült megállapodniuk, hogy jogalkotási megközelítésre van szükség. **Bővebben...**