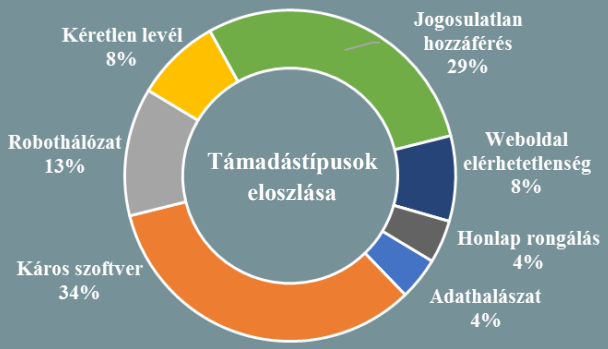
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2017. 44. hét

Incidens adatok: 2017.11.01. — 2017.11.07.



Folytatódik a bankok elleni kiberrablás-sorozat

(www.thedailystar.net)

A kiberbűnözői csoport – amely a SWIFT globális pénzügyi üzenetközvetítő hálózat ellen indít támadásokat – legutóbb egy nepáli bankot állított célkeresztbe. Információk szerint a múlt hónapban történt az incidens, melynek során a katmandui központú NIC ASIA Bank-tól indítottak hamis átutalásokat, mintegy 4,4 millió dollár értékben. A támadást egy nemzeti ünnep idejére időzítették, amikor a bank zárva volt. A nepáli központi bank (NRB) közleményben tudatta, hogy nemzetközi összefogással az összeg jelentős részét sikerült visszaszerezni, azonban így is több, mint fél millió dollárnyi kár keletkezett. Az eset kivizsgálása még tart, ennek végeztével az NRB javaslatokat szeretne közreadni a hasonló támadások megelőzésének érdekében. A SWIFT, habár a konkrét esettel kapcsolatban nem formált hivatalos véleményt, jelezte, hogy bármilyen gyanús tevékenység kapcsán javasolják a pénzintézetek számára, hogy vegyék fel velük a kapcsolatot. **Bővebben...**

Mit lép az EU az IoT eszközök kockázatának csökkentése érdekében?

(www.enisa.europa.eu)

Prof. Dr. Udo Helmbrecht, az ENISA ügyvezető igazgatója november 7-én az Európai Parlamentben tartott beszédet a "dolgok internetéhez" (IoT) kapcsolódó biztonsági kihívásokról és legjobb gyakorlatokról. Úgy véli – hivatkozva az új technológiai vívmányok okozta fenyegetésre – amennyiben Európa lényegesen nem javít a kiberbiztonságra vonatkozó megközelítésén, az hatalmas kockázatot jelent és egyre nagyobb mértékben lesz hatással az állampolgárok életére. A probléma kezeléséhez az ENISA megerősítésének fontosságát, valamint a jövőre életbe lépő hálózati és információs rendszerek biztonságáról szóló irányelvet (NIS Directive) emelte ki. Emellett a digitális termékek piacán egy egységes EU-s kiberbiztonsági tanúsítási keretrendszert szeretnének létrehozni, amely a tervek szerint megfelelő szintű védelmet fog garantálni. Ez annál is inkább égető probléma, mert becslések szerint a használatban lévő IoT eszközök száma 2020 előtt eléri a 20 milliárdot. **Bővebben...**

IT biztonsági kérdések a kvantumszámítás tükrében

(www.forbes.com)

Az elektronikus kommunikáció biztonságossá tételére széles körben használt Publikus Kulcsú Infrastruktúra (PKI) által nyújtott erős védelem annak köszönhető, hogy az üzenetek kibontására szolgáló privát kulcs, a kulcspár nyilvános részéből a jelenlegi számítási kapacitások mellett reális idő alatt nem visszafejthető. A kvantumszámítás megjelenésével azonban ez az idő radikálisan csökkenhet, az ilyen műveletek akár órák vagy napok alatt is elvégezhetők lehetnek majd – idézik Bikash Koley-t, a Juniper Network vezérigazgatóját. A kvantumszámítógépek hétköznapi felhasználására sokak szerint még néhány évtizedet várni kell, ugyanakkor az amerikai szabványügyi hivatal (NIST) úgy véli, idejekorán meg kell kezdeni az előkészületeket, hogy a kvantumszámítógépek által okozott információbiztonsági kérdésekre megfelelő megoldások születhessenek. **Bővebben...**

A népszerű iPhone alkalmazások nem védik megfelelően a bejelentkezési adatokat

(www.heise.de)

Biztonsági kutatók elemzései szerint a leggyakrabban letöltött iPhone és iPad alkalmazások több mint fele olyan biztonsági réseket tartalmaz, amelyek lehetővé teszik a hitelesítő adatokhoz való hozzáférést. A hamburgi biztonsági szakértő, Thomas Jansen kutatása szerint a 200 legnépszerűbb ingyenes iOS alkalmazás közül 111 esetében mutatható ki biztonsági probléma. Az érzékeny adatok – mint a felhasználó nevek és jelszavak – nem, vagy nem elégséges titkosítással kerülnek továbbításra. **Bővebben...**

IT biztonsági Tanács

Egyre jellemzőbb, hogy a Chrome Web Store-ban olyan böngésző bővítmények jelennek meg, amelyek gyanús tevékenységet végeznek (ilyen például az Image Downloader).

Csak olyan bővítményt töltsünk le, amire igazán szükségünk van és mindig ellenőrizzük, hogy az milyen jogosultságokat kér. Az ártalmas kiegészítők általában megpróbálnak teljes hozzáférést szerezni a webes forgalom módosításához.

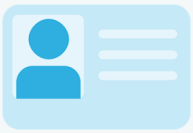
Automatizált népszámlálási törekvések

(www.engadget.com)

Az angol statisztikai hivatal (ONS) a kormányzat egy új, népszámlálással kapcsolatos kezdeményezésének részeként tanulmányozni kezdte a 18. életévüket betöltött brit Vodafone ügyfelek anonimizált mobil telefonos adatait. Az adatvédelmi törvényeknek való megfelelés érdekében csak a mobil szolgáltató hálózatára való csatlakozás helye és ideje került feldolgozásra. Az előző év márciusa és áprilisa közötti időszakból gyűjtött ingázási információk egyezést mutatnak a legutóbbi népszámlálás során kapott adatokkal. A tervek szerint 2023-ra teljesen ki is váltanák a hagyományos, papír-alapú adatgyűjtést. **Bővebben...**

Komoly sebezhetőség érinti az észt e-személyit

(www.bleepingcomputer.com)



2017. október 16-án egy biztonsági hibát (ROCA) fedeztek fel az Infineon Technologies cég által gyártott TPM lapkakészletekben, amelyet széles körben használnak laptopoktól kezdve IoT eszközökön át, például az észt elektronikus személyi azonosítókban is. Utóbbi kapcsán az észt hatóságok vizsgálatot folytattak, melynek során megállapították, hogy minden 2014. október 16. és 2017. október 26. között kibocsátott e-személyi érintett (az összes okmány kb. 58%-a), azaz gyenge RSA kulcsot használ. A biztonsági rés kihasználásával az azonosítók lemásolhatók és megszemélyesítésre adhatnak módot. A hiba kiküszöböléséhez az érintett – mintegy 760 000 állampolgár – kártyáján lévő tanúsítványt frissíteni kell, mivel azok november 3-óta elektronikus ügyintézésre nem használhatók. **Bővebben...**

Az Internet egyharmadát érte már DDoS támadás

(www.securityaffairs.co)

Szakértők kiterjedt vizsgálatot végeztek az utóbbi időszakban egyre gyakrabban tapasztalt szolgáltatásmegtagadást okozó támadásokkal kapcsolatban. Egyfelől úgy vélik, a nagy fordulatot a 2016-os év hozta meg, az olyan kiterjedt IoT botnetek felbukkanásával, amelyek az internet nagyobb szegmenseinek az időleges elérhetetlenségét is okozhatják. Ilyen volt a Mirai, azonban újabb, folyamatosan növekvő hálózatokat fedeztek fel (Reaper). További aggasztó felfedezés, hogy azok a támadások, amelyek nem feltétlenül járnak ennyire szembetűnő eredménnyel, sokkalta gyakoribbak, mint azt a hasonló elemzések alapján sejteni lehetett: világszerte körülbelül 30 000 ilyen incidens történik naponta. A támadások mintegy 25%-a az Egyesült Államokat éri és a Google, a Godaddy, és a Wix által hosztolt weboldalak a leggyakoribb célpontok. **Bővebben...**

Megjelentek a Bitcoin csalások

(www.blog.malwarebytes.com)

A kriptovaluták népszerűségének növekedésével az erre specializálódó megtévesztő tevékenységek is megjelentek – adja hírül a Malwarebytes Labs. Ismertté váltak például olyan weboldalak, amelyek – ígéretük szerint – a részükre befizetett Bitcoin összeg többszörösét juttatják vissza a felhasználónak, ingyenesen. Az ilyen hirdetésekben általában csupán nagy vonalakban utalnak a motivációra és a működés alapjaira, így az elemzés alapjául szolgáló site esetében is. Jerome Segura, a Malwarebytes elemzője szerint annak ellenére, hogy a csaló oldalak csak rövid ideig élnek és jellemzően csak első ránézésre tűnnek valós szolgáltatásnak, mégis sokan esnek áldozatul a megtévesztéseknek. A cég azt tanácsolja, hogy az irreális ígéreteknek a felhasználók semmiképp ne adjanak hitelt, különösen, ha az kriptovalutával kapcsolatos. **Bővebben...**