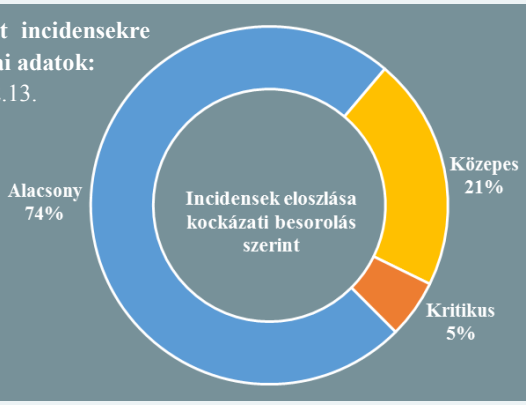
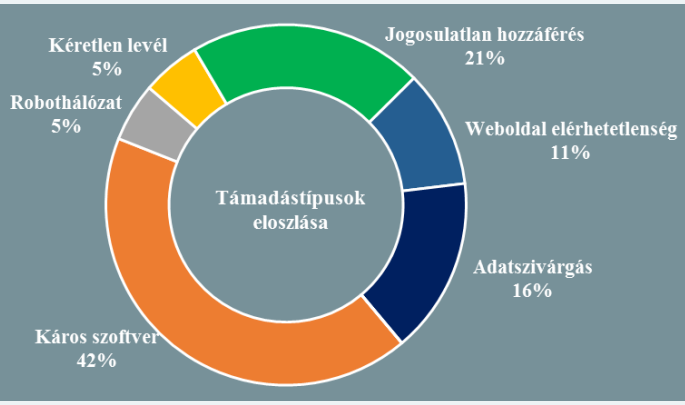
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2018. 50. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.12.07. - 2018.12.13.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!

Svájc: a kantonok úttörője megszünteti az elektronikus szavazási platformot

(www.heise.de)

Svájc Genf kantonja 2020 februárjáig kivezeti a használatból az elektronikus szavazási rendszert, az erre vonatkozó döntésnek nagyrészt financiális okai vannak. A rendszer 2003-as bevezetése óta több mint százötvenszer került használatra; 2017-ben a genfi szavazók közel hatvan százaléka ezzel a módszerrel adta le szavazatát. Időközben azonban állami szinten olyan fejlesztési követelmények kerültek meghatározásra az elektronikus szavazási rendszerrel összefüggésben, amelynek pénzügyi vonzatait – médiahírek szerint – a kanton már nem kívánja biztosítani. A fejlesztés egyrészt 2,3 millió euró plusz kiadást jelentene, emellett meg kell említeni a hivatalosan ugyan nem közreadott, de mégis fennálló, manipulálásra alkalmas biztonsági problémákat is, amelyeket egy civil informatikai klub munkatársa fedezett fel a rendszerben. Az elektronikus szavazási rendszer jövője egyelőre nyitott Svájcban: a központi kormányzat szándéka szerint ezen lehetőséget 2019-ig biztosítani kellene a kantonok többségében, azonban csatlakozásra nem kötelezhetőek.

Új néven és kibővült hatáskörrel működik tovább az ENISA

(www.enisa.europa.eu)

2018. december 10-én megállapodás született az Európai Unió kiberbiztonsági rendeletéről, amelynek értelmében a jelenlegi Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) EU Kiberbiztonsági Ügynökség (EU Agency for Cybersecurity) néven működik tovább, kiterjesztett szerepkörben. A kiberbiztonsági rendelet kulcsfontosságú pontjai között szerepel, hogy az ENISA nagyobb humán és pénzügyi erőforrást biztosító megbízást kap a jövőben, ennélfogva ─ a várakozások szerint ─ nagyobb támogatást lesz képes biztosítani az uniós tagállamoknak a kiberbiztonsági fenyegetésekkel és támadásokkal szemben, valamint a tervek szerint hatékonyabb segítséget nyújt majd az intézmények számára az általános kiberbiztonsági eljárásrendek kidolgozásában, végrehajtásában és felülvizsgálatában. Mindezek mellett szerepet kell vállalnia az uniós kiberbiztonsági tanúsítási keretrendszer bevezetésében is, a nemzeti tanúsítási hatóságokkal, valamint iparági szakértőkkel történő szoros együttműködésben.

A kiberbűnözés ma virágzóbb üzletág, mint valaha

(www.welivesecurity.com)

Az ESET blogján egy hosszabb posztban foglalkozik az illegális kereskedelem online jelenlétének helyzetével. Ennek során arra a következtetésre jut, hogy aggasztó módon a feketekereskedelem túlnőtt a „sötét weben” és egyre nagyobb arányban jelenik meg a hagyományos böngészés során fellelhető online tereken. Komoly változás állt be például a lopott bankkártya adatok értékesítésének mikéntjében, az ugyanis már nem csupán eldugott fórumokon történik, hanem indexelt oldalakon, nem ritkán agresszív reklámhadjárat kíséretében (lásd Carding Mafia). A másik fő ok, amiért a poszt szerzője, Stephen Cobb „újgenerációsként” tekint a kiberbűnözői tevékenységre, az a legális kereskedelemre jellemző komplex szolgáltatási csomag megjelenése, amelynek része többek között a termékek, szolgáltatások, eladók értékelése, a vásárlói elégedettség-felmérés, vagy a „terméktámogatás”. Mindemellett a háttér infrastruktúra is jóval szervezettebbé és összetettebbé vált az elmúlt évek során (lásd a RAND 2014-es tanulmányát).

Bővebben...

Az áldozatok PayPal fiókját veszi célba egy androidos kártevő

(www.zdnet.com)

Az ESET szakértői felfedeztek egy akkumulátor optimalizáló applikációba (Optimization Battery) rejtett trójai kártevőt, amely az áldozat PayPal fiókjához igyekszik hozzáférést szerezni, majd a háttérben utalást indítani, anélkül, hogy a felhasználónak esélye legyen ennek megakadályozására. Mindezt úgy éri el, hogy telepítéskor engedélyt kér az Android Accessibility használatához, amely többek között lehetővé teszi a képernyő és az operációs rendszer közötti interakciók automatizálását, ezzel szimulálva a felhasználói utasításokat (koppintásokat). A jogosultság megszerzése után az app addig várakozik, amíg a felhasználó meg nem nyitja a PayPal applikációt, és sikeresen be nem jelentkezik a fiókjába. **Bővebben...**

IT biztonsági Tanács

Online vásárlás előtt mindig olvassuk el az általános szerződési feltételeket (ÁSZF), valamint érdemes megismerni az általunk választott webáruházzal kapcsolatos vásárlói véleményeket és felhasználói tapasztalatokat.

Az Infokommunikációért és Fogyasztóvédelemért Felelős Államtitkárság weboldalán található adatbázisban előzetesen ellenőrizhetjük, hogy a felkeresett webáruház szerepel-e a szabálytalanul működő, súlyos jogsértéseket elkövető internetes boltok listján.

Amennyiben a lehetőségek engedik fizetési mód kiválasztásánál válaszszuk az utánvétet.

Megszületett az első jogszabály a titkosítás megkerüléséről

(www.cyberscoop.com)

Az ausztrál parlament elfogadta a törvényt, amely a technológiai vállalatok számára kötelezővé teszi, hogy hatósági kérelemre hozzáférést biztosítsanak a hálózatukon áthaladó titkosított kommunikációkhoz. Azon cégek, amelyek nem felelnek meg az elvárásoknak, bírságra számíthatnak. Az intézkedést komoly kritika éri a tech cégek részéről, mondván a hátsó ajtók a hackerek számára is lehetőséget adnak az információszerzésre, valamint maguk a kormányok is visszaélhetnek a lehetőséggel. Lizzie O'Shea, emberi jogi jogász úgy véli, ez csupán az első lépés, és előbb-utóbb a többi „Öt Szem" nemzet is hasonló szabályozást fog hozni.

Kelet-európai bankok elleni támadásokra hívja fel a figyelmet a Kaspersky

(www.cyberscoop.com)

Az orosz kiberbiztonsági cég szerint informatikai támadások történtek kelet-európai pénzintézetek ellen, amelyek során a támadók közvetlenül a bankok hálózatára kapcsolódó fizikai eszközöket is alkalmaztak: laptop, Raspberry Pi, illetve egy USB-szerű, támadó eszköz, a Bash Bunny is a repertoár részét képezte. A jelentés szerint könnyű álcázhatóságuk miatt ezek lokalizálása annak ellenére nagy kihívást jelentett, hogy jelenlétükre egyértelműen fény derült az engedélyezett és a hálózatra valójában csatlakoztatott készülékek számának eltérése miatt. A támadást több fázisban hajtották végre, az eszközöket pedig telepítés után a beépített GPRS/3G/LTE modem segítségével távolról irányították login adatok, valamint fizetési információk után kutatva. A rejtőzködésre nagy gondot fordítottak, többek közt PowerShell szkriptekkel próbálták elkerülni a védelmi szoftverek általi detektálást. A kutatók szerint, az általuk „DarkVishnya" néven azonosított kampány több tízmillió dolláros kárt okozott legalább nyolc bank számára. Az elkövetők kilétével kapcsolatban a riport nem foglal állást.

A Super Micro semmilyen jelét nem találta a Bloomberg-féle kémchipnek

(www.reuters.com)

A kínai kémchipekkel idén októberben hírbehozott Super Micro vállalat tájékoztatása szerint egy külső cég által végeztetett biztonsági audit nem talált bizonyítékot arra vonatkozóan, hogy a Bloomberg állításai valósak lennének. A Reuters információi szerint a vizsgálatot a Nardello & Co. végezte jelenleg gyártás alatt lévő, valamint az Apple és az Amazon részére korábban értékesített alaplap verziókon. Az ellenőrzések során sem engedély nélküli komponenst, sem adatszivárgást nem azonosítattak.

Kibertámadás ért egy olasz gáz- és olajtársaságot

(www.securityaffairs.co)

Informatikai támadás történt hétfőn az olasz Saipem olaj- és gázszolgáltató egyes szerverei ellen. Információk szerint az offenzívát az indiai Chennaiból indították, ami a közel-keleti régióban (Szaúd-Arábia, Egyesült Arab Emírségek és Kuvait) található szervereket célozta, az olasz, francia és brit központokat azonban nem érintette. A Saipem kevés információt hozott nyilvánosságra a támadásról, mivel annak kivizsgálása, valamint az infrastruktúrára gyakorolt hatások felmérése jelenleg is zajlik. Mindazonáltal a cég közleményében említi, hogy a rendszeres biztonsági mentéseknek köszönhetően nem számítanak adatvesztésre, amelyből a Security Affairs arra következtet, hogy zsarolóvírus támadás történhetett.