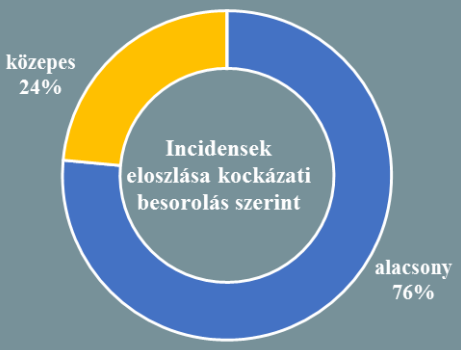
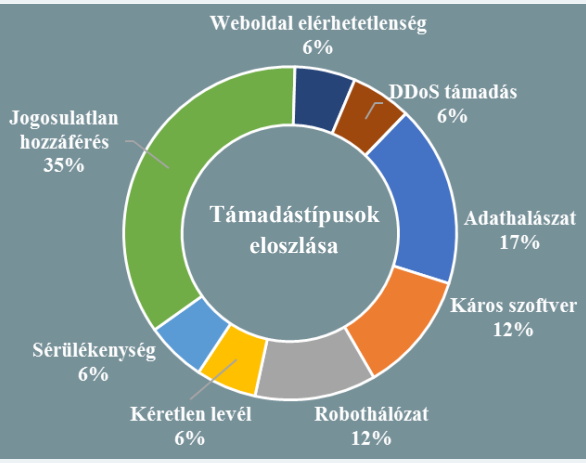
Nemzetközi IT-biztonsági sajtószemle

2017. 40. hét

Incidens adatok: 2017.10.04. — 2017.10.10.





Európai kiberverseny

(www.enisa.europa.eu)

Az Európai Kiberbiztonsági Kihívás (ECSC) idén október 31. és november 3. között, a spanyol Nemzeti Kiberbiztonsági Intézet (INCIBE) által kerül megrendezésre Malagában. Az ENISA által is támogatott európai kiberversenyen 15 országból közel 150 kiberbiztonsági szakember részvételére számítanak, olyan, a valós életből vett feladatok megoldásában, mint például webes alkalmazások sebezhetőségeinek felderítése, védett rendszerekhez való hozzáférés, vagy titkosított dokumentumok visszaállítása. A verseny mellett a szervezők egyéb programokkal is készülnek, például szakmai konferenciák és állásbörze is várható. Prof. Dr. Udo Helmbrecht, az ENISA ügyvezető igazgatója szerint a tagállamok részéről látványosan nő az érdeklődés a verseny iránt. **Bővebben...**

EU-s e-kormányzati célkitűzések

(www.computerweekly.com)

EU és EFTA tagországok képviselői a múlt hét során írták alá az 'E-kormányzati Nyilatkozatot' Tallinban. Ennek célja azon fő prioritások meghatározása, amelyek felhasználó központú kormányzati szolgáltatások kialakításához szükségesek, kiegészítve a 2009-es malmöi nyilatkozatot és a 2016-2020-as időszakra vonatkozó E-kormányzati akciótervet. A fő célkitűzések között szerepel – többek között – az elektronikus személyi azonosító (eID) és az elektronikus tranzakciókhoz nyújtott bizalmi szolgáltatásokra vonatkozó szabályokra (eIDAS) való felkészülés felgyorsítása. A Tallinn Digital Summit után Jüri Ratas észt miniszterelnök elmondta, az EU-t 2025-re vezető szereplővé szeretné tenni a kiberbiztonság terén. **Bővebben...**

Haditerveket lophatott Észak-Korea

(www.engadget.com)

Értesülések szerint a rezsim sikeresen hozzáfért dél-koreai minősített katonai dokumentumokhoz, köztük egy, az Egyesült Államokkal közösen készített haditervvel, amely az Észak-Koreai vezér megbuktatását célozta. Állítólag mintegy 235 gigabájtnyi adatot tulajdonítottak el, amelyek 80%-át még nem sikerült azonosítani, de az eddigi vizsgálatok alapján a dél-koreai különleges erők egyes készenléti tervei és kritikus infrastruktúrákat érintő érzékeny adatok is kompromittálódtak. A Yonhap hírügynökség szerint az incidensről szóló információ egy dél-koreai kormánypárti képviselőtől (Rhee Cheol-hee) származik. A BBC úgy értesült, a támadás valamikor 2016 szeptemberében történhetett. **Bővebben...**

Az energiaszektor tisztában van a kibertámadásoknak való kitettségével

(www.securityweek.com)

Az Accenture felmérést végzett azzal kapcsolatban, hogy az energiaszektorban működő vállalatok vezetői hogyan ítélik meg a kritikus infrastruktúrákat érő informatikai fenyegetéseket. A több régiót is átfogó nemzetközi vizsgálat több, mint száz energetikai cég bevonásával készült. Többek között kiderült, hogy a vezetők közel kétharmada úgy véli, a villamosenergia hálózatokat öt éven belül éri olyan – legalább mérsékelt szintű – kibertámadás, amely bizonyosan zavarokat fog okozni az ellátás biztosításában. A leginkább fenyegető tényezők között szerepelnek például a zsarolóvírusok, illetve az eszközök fizikai elpusztítását célzó támadások, de a megkérdezettek közel fele felhasználói vagy ügyfél adatok lehetséges kompromittálódásától is tart. Mindezek ellenére a vizsgálatban szereplő szerveztek 40% még mindig nem integrálta megfelelően az informatikai biztonságot a kockázatkezelési folyamataiba. **Bővebben...**

Megtévesztő az iTunes-os bejelentkező panel

(www.helpnetsecurity.com)

Az iOS-es telefonok gyakran kérik az iTunes jelszó megadását, például rendszerfrissítések installálása után vagy telepítés közben lefagyott alkalmazások esetében, emiatt a felhasználók hozzászoktak, hogy viszonylag váratlan helyzetekben is meg kell adniuk a jelszavukat. Ezek a felugró ablakok ráadásul nem csak a zárolt vagy a kezdőképernyőn jelennek meg, hanem alkalmazásokon belül is, ami a problémára figyelmet felhívó Felix Krause szerint lehetőséget ad rosszindulatú applikációkban a legitim panel leutánzására és így nagy valószínűséggel sikeres adathalász támadás végzésére. Úgy véli egy lehetséges megoldás lehet, ha sikerül elkerülni, hogy gyakran kelljen megadni az iTunes jelszót, vagy legalább azt egységesen a 'Beállítások' alatt kelljen megtenni. **Bővebben...**

IT biztonsági Tanács

Védje személyes fiókját a kéretlen levelektől és az adatokkal történő visszaélésektől az ún. eldobható vagy ideiglenes e-mail címek használatával.

Ezeket a fiókokat olyan regisztrációknál célszerű alkalmazni, amikor valamely szolgáltatást igénybe szeretnénk venni, de nem akarjuk megadni ahhoz a valós fiókunk címét. Amennyiben már nincs szükségünk a fiókra, az törölhető vagy bizonyos idő lejárta után automatikusan megszűnik.

Német hírszerző ügynökségek kodifikálnák az informatikai válaszcsapásokat

(www.in.reuters.com)

Magas rangú német hírszerző tisztek jogszabályi felhatalmazást szeretnének válaszcsapások indításához külföldről érkező kibertámadások esetén. Hans-Georg Maassen, a német elhárítás (BfV) vezetője a parlamenti felügyeleti bizottság előtt elmondta, szerinte lehetővé kellene tenni, hogy még az illetéktelen felhasználás előtt elpusztítsák a német szerverekről eltulajdonított adatokat. Azt is elképzelhetőnek tartaná, hogy olyan megfigyelésre alkalmas szoftvereket juttassanak be külföldi szerverekre, amelyekkel azután valós időben detektálhatnák a Németország elleni műveleteket. Úgy véli, ez nem sokban különbözik a kettősügynökök beszervezésétől. Christof Gramm, a katonai kémelhárítás vezetője azonban arra hívta fel a figyelmet, hogy a nemzetközi jogra is tekintettel kell lenni, mielőtt ilyen felhatalmazást adnának a titkosszolgálatoknak. **Bővebben...**

Szigorúbb lehet a Bitcoin felügyelet Oroszországban

(www.bleepingcomputer.com)

Sergei Shvetsov, az orosz központi bank elnökhelyettese blokkoltatná a kripto-fizetőeszközök vásárlására és azok valós valutára váltására szolgáló weboldalak elérését Oroszországban. A kezdeményezés nem új keletű, már 2015 óta igyekeznek tiltani egyes Bitcoin kereskedő site-okat, azonban ezeket az intézkedéseket rendszerint felülbírálták a helyi bíróságokon.

Pénzügyi tisztviselők gyakorta fejezik ki aggodalmukat azzal kapcsolatban, hogy a digitális fizetőeszközök szabályozásának hiánya a bűnszövetkezetek számára egy újfajta lehetőséget nyújt a pénzmosásra és az adózási törvények kijátszására. Amennyiben életbe lép a szigorítás, a jövőben kriptopénzekre maximum bányászat útján lehet majd szert tenni Oroszországban. **Bővebben...**

Kiberbiztonsági tárgyalások vezető nagyhatalmak között

(www.bna.com)

Megtörtént az első bűnüldözői és kiberbiztonsági témájú egyeztetés az Egyesült Államok és Kína között (U.S.-China Law Enforcement and Cybersecurity Dialogue - LECD), amely kapcsán máris jelentős pozitív fejlemény bontakozott ki, hiszen a két ország több kiberbiztonsági kérdésben is konszenzusra jutott. Ennek értelmében a felek – többek között – arról egyeztek meg, hogy nem indítanak ipari kémkedési céllal kibertámadást egymás ellen és nem támogatnak ilyen célú csoportokat, emellett hangsúlyosabbá teszik az együttműködést a kiberbűnözői tevékenységek felderítéséhez. Iparági szakértők és korábbi amerikai kormányzati tisztviselők üdvözölték a megállapodást és a nemzetközi kiberbiztonsági együttműködés fontos lépéseként értékelték azt. **Bővebben...**

Kompromittálódott telefon a Fehér Házban

(www.politico.com)

A Fehér Ház technikai támogató csapata derítette fel, hogy John Kelly magántelefonja feltételezhetően még decemberben kompromittálódott, amikor John Kelly a belbiztonság titkára volt. Az incidensre annak kapcsán derült fény, hogy Kelly több hónapnyi problémás működés után szervízbe adta a készüléket. Még nem tisztázott, hogy a telefont milyen módszerrel fertőzték meg, sem pedig az, hogy milyen adatokat szerezhettek meg róla. **Bővebben...**