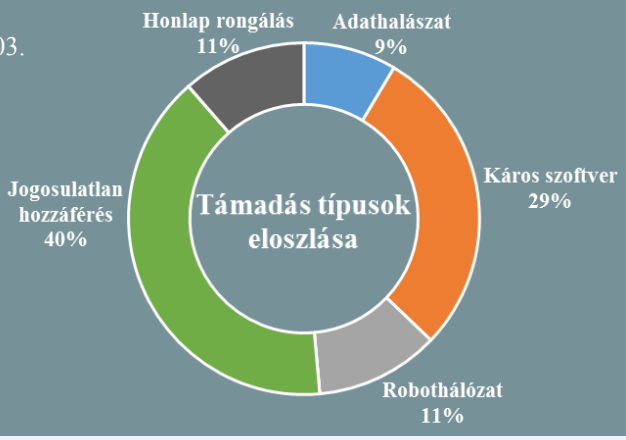
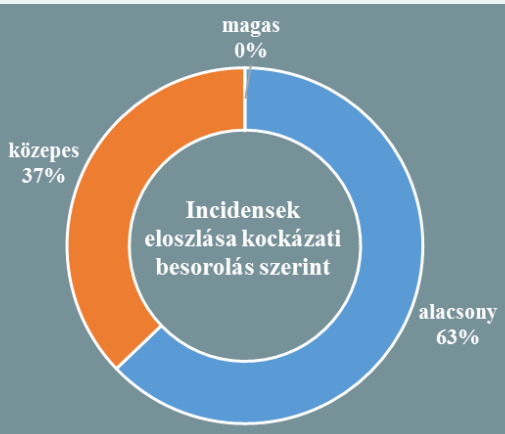
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

IT-biztonsági sajtószemle

17. hét

Incidens adatok:
2017.04.26-2017.05.03.





Kibertámadás az izraeli kormány ellen

(www.securityaffairs.co)

Az izraeli miniszterelnöki hivatal közleményben ismertette, hogy egy jelentős mértékű kibertámadást sikerült elhárítaniuk. A tájékoztató mindössze két nappal azt követően érkezett, hogy a Shin Bet és a Mossad vezetői, valamint más magas rangú védelmi tisztségviselők közös levélben figyelmeztették Benjamin Netanyahu miniszterelnököt, hogy új javaslata – amely kiterjesztett jogkörrel látná el a két éve felállított izraeli Kibervédelmi Hatóságot – jelentősen akadályozná a többi szervezet kibervédelmi tevékenységét. **Bővebben...**

Webes kiberbiztonsági enciklopédia

(www.researchcenter.paloaltonetworks.com)

A Paloalto Networks biztonsági cég weboldalán ingyenesen elérhetővé tett egy IT biztonsági témájú gyűjteményt, amely a kiberbiztonság terén leggyakrabban használt fogalmak tisztázását tűzte ki célul. Emellett a weboldalon a témához kapcsolódó hasznos cikkek is elérhetők, jó gyakorlatokkal és hasznos tanácsokkal, például a végpontvédelem kialakításához, vagy éppen a felhő-alapú szolgáltatások kiválasztásához. **Bővebben...**

Sikeres Europol akció

(www.europol.europa.eu)

Az Europol koordinálásában, brit és spanyol bűnüldöző szervek összefogásával valósult meg egy nemzetközi kiberbűnözői csoport felszámolása. A csoport 2013 közepe óta működött és káros szoftverek széles palettáját – többek között trójai programokat, keyloggereket – terjesztették világszerte, így sokezer host fertőzéséért tehetők felelőssé. Az Europol 2015 vége óta folytatott nyomozást, aminek eredményeként két akció során összesen öt személyt tartóztattak le, valamint több eszközt is lefoglaltak. **Bővebben...**

Törvényjavaslat az információbiztonsági paradigmaváltáshoz

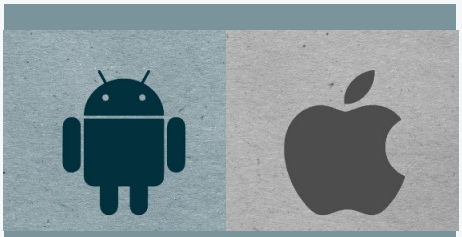
(securityweek.com)

Edward J. Markey, az USA-beli Massachusetts állam szenátora az Institute for Critical Infrastructure Technology-vel (ICIT) együttműködve törvényjavaslatot tett a kritikus infrastruktúrák védelme érdekében. A tervezet egy új szemlélet mentén került kialakításra, a biztonsági termékek fogyasztóit szeretné ellátni minél pontosabb információkkal, amelyekre azután beszerzési döntéseiket alapozhatják. Az elképzelés szerint ez arra sarkallná a gyártókat, hogy az üzleti stratégia részévé tegyék az IT biztonságot. **Bővebben...**

Kibertámadás katonai művelet helyett

(www.washingtontimes.com)

Nagyobb a valószínűsége annak, hogy Észak-Korea kibertámadást indít az Amerikai Egyesült Államok ellen, mint hogy katonai erőket vessen be, nyilatkozta John Kelly, az USA belbiztonsági minisztere. Habár az utóbbi napok során az USA mellett Észak-Korea is kilátásba helyezett katonai csapást, mégis sokkal elképzelhetőbb egy kibertámadás, amelyre Észak-Korea az USA szerint is képes lehet. Erre példa a 2014-es, a Sony Pictures-t ért incidens, amely széles körben elfogadott módon a diktatúrához köthető. **Bővebben...**



Mennyire biztonságosak a bankok mobilapplikációi?

(www.helpnetsecurity.com)

Az Accenture és a NowSecure, észak-amerikai banki szervezetek applikációin végzett tesztjei kimutatták, hogy a vizsgált alkalmazások – platformtól függetlenül – legalább egy biztonsági problémával rendelkeznek. Kiemelt problémának minősül többek között, hogy más alkalmazások is képesek a fájlok írására a banki alkalmazásokon belül, valamint nem megfelelő szintű a kommunikáció biztonsága. **Bővebben...**

Biztonságosabb Android eszközök

(www.techrepublic.com)

A biztonság növelésére számos alkalmazás és szolgáltatás érhető el (ADM - Android Device Manager, DuckDuckGo, Képernyő zár, AppLock), melyek segítségével növelhető a biztonság, de ugyan ennyire fontos az Android rendszer folyamatos frissítése, valamint a használni kívánt alkalmazások kizárólagosan GooglePlay Áruházból történő beszerzése. **Bővebben...**

IT biztonsági tanács

Használjunk naprakész, automatikusan frissülő víruskereső- és vírusirtó biztonsági szoftvert, valamint alkalmazzuk a beépített tűzfalat, ügyelve annak megfelelő beállításaira.

Csak megbízható forrásból szerezzünk be programokat, különösen a biztonsági szoftverek minőségére és megbízhatóságára ügyeljünk!

Nagyszabású nemzetközi kiberbiztonsági gyakorlat

(www.ccdcoe.org)

A múlt hét során került megrendezésre a legnagyobb nemzetközi kiberbiztonsági gyakrolat, a 'Locked Shields', a NATO szervezésében. A gyakorlat során a csapatok a valós életből vett komplex feladatokat kaptak. Ezúttal – többek között – az elektromos hálózatot kezelő ipari vezérlőrendszer (SCADA) valamint katonai rendszerek védelmét kellett ellátniuk. Az eseményen, amelyet 2010 óta minden évben megrendeznek, idén közel 900 IT security szakértő vett részt, akik közül az első helyen összesítésben a cseh csapat végzett. **Bővebben...**

Kibertámadások 10 éve és most

(www.gcn.com)

2017. április 27-e a tízéves évfordulója az Észtországot ért kibertámadásnak, amely az első, egy nemzet teljes internetes infrastruktúrája ellen elkövetett átfogó támadásként, egy új korszak kezdetét jelezte a kiberhadviselés terén. Az eset után a NATO kibervédelmi központját Észtországban helyezte el, valamint megszületett a 'Tallin manual', ami a nemzetközi jog kibertámadásokra való alkalmazását tárgyalta. A 2017 februárjában megjelent 'Tallin 2.0', pedig elsősorban arra keresi a választ, hogy az elmúlt 10 év során hogyan is változtak a kiberfenyegetések. **Bővebben...**

Az információs hadviselés és a Facebook

(www.zdnet.com)

A Facebook közleményben tudatta, hogy a hagyományos rosszindulatú tevékenységek mellett – fiókok feltörése, káros tartalom terjesztése, spammelés, stb. – immáron figyelmet szentelnek egyéb manipulatív tevékenységek elleni fellépésnek is. Ide tartozik a felhasználók véleményének ideológiai vagy politikai okokból történő befolyásolására irányuló aktivitás, amelyekre összefoglaló néven 'információs művelet'-ként hivatkoznak. Az ilyen tevékenységek felderítésére és megakadályozására több eljárást is alkalmaznak, például a gépi tanulás módszertanát. **Bővebben...**

Belgium jóváhagyta a nemzeti kibervédelmi tervet

(www.7sur7.be)

2015 decembere óta készült a tervezet, amely a kritikus infrastruktúrákra vonatkozóan meghatározza a szükséges lépéseket, amikkel meg lehet akadályozni vagy korlátozni a támadásokat, valamint lehetővé teszi a NATO speciális csoportjának bevetését egy informatikai támadás esetén. Az utóbbi években a Belgiumot ért IT biztonsági incidensek száma jelentősen megnőtt, a CERT.be havi szinten átlagosan 1300+ bejelentést rögzít. **Bővebben...**

Az NSA visszakozik

(www.nytimes.com)

Az NSA felhagy azzal a gyakorlattal, hogy begyűjtse azon amerikai állampolgárok üzeneteit, akik a külföldi partnerükkel folytatott kommunikáció során olyan személyről tesznek említést, akit a szervezet megfigyelés alatt tart. A tevékenységet korábban már számos kritika érte, utóbb pedig törvénytelennek is minősítették. Az új eljárás szerint csupán a célszemély direkt forgalmát foghatják el. **Bővebben...**