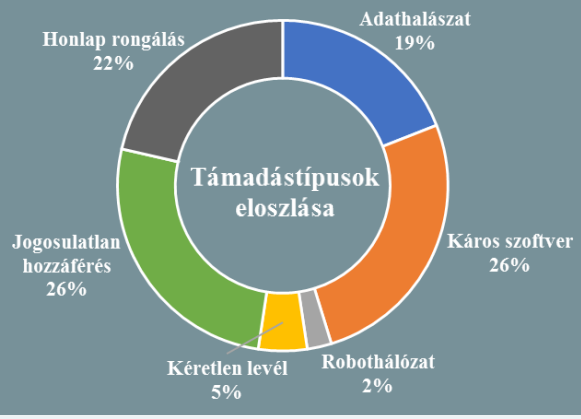
Nemzetközi IT-biztonsági sajtószemle

Incidens adatok:
2017.06.21. — 2017.06.27.



Adatmegosztási szabályok

(www.threatpost.com)

A Borderless Cyber konferencián az adatvédelmi elvekkel kapcsolatos beszélgetésen szólalt fel Clare Sullivan, a Georgetown Egyetem professzora, aki szerint az eljövendő - az amerikainál jóval szigorúbb - európai szabályzás az üzleti tevékenység során történő személyes adatok megosztását is jóval komplikáltabbá teszi, amire a vállalatoknak időben fel kell készülniük. Kiemelte, hogy egyértelmű szabályokra van szükség arra vonatkozóan, hogy a magánszektor és az amerikai valamint külföldi kormányzatok között hogyan valósuljon meg az adattranszfer, hogy az ne ütközzön az európai adatvédelmi elvekkel (GDPR). Különsen fontos ennek tisztázása a kiberfenyegetésekkel kapcsolatos információmegosztás zavartalan működtetéséhez, mivel az európai adatvédelmi modell a személyes adatok körét meglehetősen szélesen értelmezi és az olyan ártalmatlannak tűnő adatok, mint például az IP cím kapcsán is félreértelmezésre adhat módot.**Bővebben...**

Legálisan hackelhetnek a német bűnüldöző hatóságok

(www.helpnetsecurity.com)

A Bundestag elfogadott egy törvénymódosítást, amely a német rendőrség számára lehetővé teszi az ún. "szövetségi trójaik" alkalmazását acélból, hogy mindennemű digitális kommunikációhoz hozzáférjenek, még a titkosítás előtt. A módszert eddig kizárólag telekommunikációs megfigyelésre (telefonhívások, SMS-ek) és csak extrém esetben (például terrorcselekmények felderítésére) használták. Mostantól a hatóságok – többek között – a kábítószer-kereskedelem, az adócsalás és gyilkosság esetében is bevethetik a malware-t. A módosítás nem járt kritika nélkül, egyesek szerint ugyanis alkotmányellenes az, amilyen nagy betekintést ad a magánéletbe.
Bővebben...

Elkészült a Nemzetközi Kiberbiztonsági Index aktualizálása

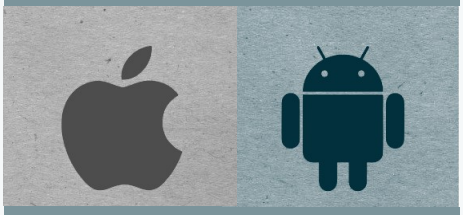
(www.scmagazineuk.com)

Az International Telecommunication Union (ITU) által gondozott 'Global Cyber-security Index' új kiadása szerint Észtország vezető a kiberbiztonság terén Európában, világviszonylatban pedig az ötödik helyen áll. Az első öt európai ország között van még Franciaország, Norvégia, az Egyesült Királyság és Hollandia. Liina Areng, az észt Information System Authority (RIA) nemzetközi közönségkapcsolatokért felelős igazgatója szerint a siker hátterében a jogi, szervezési és technikai intézkedések kombinációja és nemzetszintű megvalósítása áll. A listán szereplő államok csupán 38%-a rendelkezik nyilvános kiberbiztonsági stratégiával.
Bővebben...

A gyengített titkosítás mellett kampányol Ausztrália

(www.theregister.co.uk)

Az ausztrál kormányzat a héten megrendezésre kerülő két napos Five Eyes (FVEY) találkozón szeretné a titkosítást megkerülő 'hátsó kapuk' létesítésének kérdését a megbeszélés egyik fő témájává tenni. Ausztrália nyíltan a 'backdoor' mellett áll ki és egyértelművé tette, hogy a többi FVEY tagot is szeretné erre az álláspontra bírni és kidolgozni egy olyan stratégiát, amivel a tech vállalatokat rábírhatják az együttműködésre. Malcolm Turnbull miniszterelnök elmondta, a július 7. és 8. között megrendezésre kerülő G20-as csúcstalálkozón is fel fogja vetni a kérdést. **Bővebben...**



10 éve a piacon

(www.nypost.com)

2007. június 29-én jelent meg az első iPhone a piacon, mely új irányba terelte a mobiliparágat. A CBS Sunday Morning az évforduló alkalmával összehívta azt a négy technikai kritikust, akik 2007-ben vizsgálták az első iPhone-t. **Bővebben...**

Hamis antivírus alkalmazások

(www.itsecuritynews.com)

Az Alarming Truth Global internetes biztonsági cég megdöbbentő bejelentést tett, miszerint a WannaCry támadás óta - annak ellenére, hogy az nem érintette az Android felhasználókat - több száz Android vírusvédelmi alkalmazás jelent meg a piacon, amelyek valójában káros programokat tartalmazhatnak. **Bővebben...**

IT biztonsági Tanács

Rendkívül fontos, hogy okoseszközeinket is megfelelő védelemmel lássuk el, hiszen érzékeny adatainkat ezeken az eszközökön tároljuk.

A védelmi programokat csak megbízható gyártóktól és az adott platform által ellenőrzött hivatalos alkalmazás boltjaiból töltsünk le (Google Play, Appstore, Microsoft Store), valamint kerüljük az ingyenes, nem hiteles vírusirtók alkalmazását.

Az NSA együttműködést javasol a kibertámadások hatékony kezeléséhez

(www.threatpost.com)

A kiberbiztonság sokkal kevésbé gazdaságos, mint a kiberbűnözés, hiszen egyetlen káros szoftverbe való befektetéssel akár több ezer támadás is kivitelezhető lehet. Neal Ziring, az NSA Képességek Igazgatóságának technikai igazgatója pontosan ezen szeretne változtatni, a célja a támadások gazdaságosságának lényeges csökkentése. Erről beszélt a Borderless Cyber konferencián is, ahol kifejtette a javaslatát egy olyan keretrendszerről, amely az együttműködésen alapszik. A koncepció szerint amennyiben a hálózat egy tagját támadás éri, a közösség magasszintű tagjai (például kormányzatok) kielemeznék a támadást, ezt követően pedig megelőző intézkedéseket tudnának alkotni, percek alatt elérhetővé téve azokat a közösség minden tagja számára. **Bővebben...**

Megállapodás a gazdasági célú kibertámadásokról

(www.in.reuters.com)

Kína és Kanada egyezményt írtak alá, miszerint ettől fogva nem intéznek egymás ellen állami támogatású kibertámadást ipari titkok vagy más bizalmas üzleti információk megszerzésére. A megállapodás kizárólag a kereskedelmi-ipari kiberkémkedésre vonatkozik, a hírszerzési célú kibertámadások ellen továbbra sem biztosít védelmet. Hasonló konszenzus ez, mint ami 2015-ben született Kína és az Egyesült Államok között a vállalati kiberkémkedésről, miután az Obama adminisztráció szankciókat foganatosított kínai személyek ellen, egyes, USA elleni kibertámadások után. **Bővebben...**

Szigorúbb incidensbejelentési kötelezettség

(www.reuters.com)

Az Európai Központi Bank (ECB) az ellenőrzése alatt álló pénzintézetektől 2017 nyarától elvárja, hogy minden jelentősebb kiberbiztonsági incidensről számoljanak be, aminek fő oka, hogy az ECB nagyobb hangsúlyt kíván fektetni az IT biztonságra. "Egy sikeres tesztidőszakon vagyunk túl, amelyet 2016 során folytattunk, most pedig egy hosszútávú megoldást szeretnénk megvalósítani azon bankok számára, amelyek esetében direkt felügyeletet látunk el – mondta Sabine Lautenschlaeger, a Felügyeleti Testületének tagja. Az intézkedés segítségével pontosabban felmérhető, hogy a szektort mennyi incidens sújtja és a kiberfenyegetések hogyan fejlődnek. **Bővebben...**

Közös fellépés az EU-t célzó kibertámadások ellen

(www.dw.com)

Az Európai Unióban megállapodás született egy "kiberdiplomáciai eszköztár" használatáról. A megállapodás lényege, hogy bármely EU tagállam ellen elkövetett kibertámadás közös válaszreakciót von maga után. "A válasz arányos lesz az elszenvedett támadás mértékével, tekintetbe véve annak hatókörét, kiterjedtségét, idejét, intenzitását, komplexitását" - áll az EU-s külügyminiszterek közös közleményében. A támadások esetén foganatosítható 'megszorító intézkedések' között olyanok találhatók, mint például személyek, csoportok, vállalatok, vagy kormányok ellen hozható utazási korlátozás, vagyon befagyasztás, vagy egyéb, üzleti tevékenységet érintő korlátozás. Az intézkedés hátterében – többek között – az a félelem áll, hogy a szeptemberi német választások ellen átfogó hacker támadás várható. **Bővebben...**