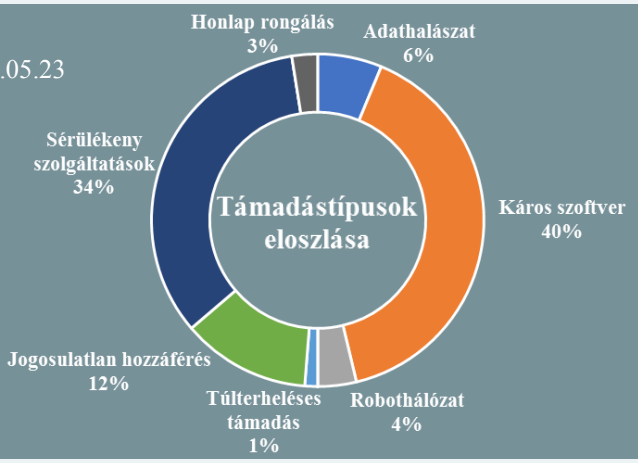
Incidens adatok:
2017.05.17 — 2017.05.23



A Signal üzenetküldő alkalmazás bevezetése az amerikai szenátusban

(threatpost.com)

A 2016-os amerikai elnökválasztás óta Amerika egyre növekvő figyelmet fordít a kiberbiztonságra. Ennek szellemében az Államok szenátusa múlt hét kedden jóvá hagyta a 'Signal' titkosított üzenetküldő alkalmazás használatát a kongresszusi tagok részére. Ron Wyden szenátor külön levélben üdvözölte, hogy a kormányzat nem csupán egy szabályzási kérdésként tekint a titkosításra, hanem elfogadni látszik azt a kiberbiztonság fontos részeként. **Bővebben...**

Fordulat az amerikai 'nyílt internet' szabályzás terén

(www.techrepublic.com)

Az Egyesült Államok Szövetségi Kommunikációs Bizottsága (Federal Communications Commission - FCC) 2:1 arányban elfogadta a 'Restoring Internet Freedom' (RIF) javaslatot, amely a 2015-ös, még az Obama kormányzat által alkotott 'Nyílt Internet Rendeletet' módosítaná nagy mértékben. A változtatás megszüntetné az ún. 'Title II' kategóriát, ezáltal az internet hozzáférés biztosítását telekommunikációs helyett információs szolgáltatássá (Title I) minősítené vissza, lényegesen csökkentve az internet szolgáltatókra vonatkozó jogi megkötéseket és korlátozásokat. **Bővebben...**

Nő a HTTPS-t használó adathalász weboldalak száma

(news.netcraft.com)

Mióta 2017 januárjában a Mozilla Firefox és a Google Chrome a felhasználók figyelmeztetésére elkezdte megbízhatatlannak nyilvánítani a nem HTTPS protokollon keresztül elérhető online bejelentkezési felületeket, egy nem várt következményként az SSL-t használó adathalász weboldalak száma jelentősen megnőtt. Erre magyarázat lehet, hogy a támadók az adathalász tartalmakat sokszor eleve SSL tanúsítvánnyal rendelkező site-okon helyezik el. Paul Mutton, a Netcraft munkatársa szerint az adathalász webhelyek többsége azért továbbra is a standard HTTP protokollt használja. **Bővebben...**

Kiberbiztonsági kihívások és javaslatok

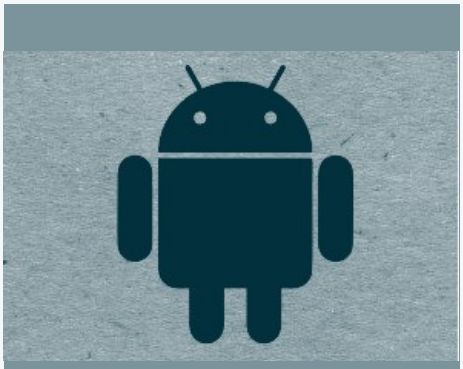
(www.helpnetsecurity.com)

Az Európai Hálózati- és Információbiztonsági Ügynökség (ENISA) a gazdasági szereplőkkel közös álláspontra jutott a kiberbiztonság terén, amely reflektál a vállalatok aggályaira és javaslatokat fogalmaz meg a döntéshozók számára. A létrehozott dokumentum négy fő területre összpontosít, amelyet aktívan vitatnak meg uniós szinten: a szabványosítás és tanúsítás, a biztonsági folyamatok és szolgáltatások, a biztonsági követelmények és végrehajtásuk, valamint a gazdasági dimenziók. **Bővebben...**

Németországban is hódít a kiberbűnözés

(www.deepdotweb.com)

Állami és iparági vezetők szerint a kiberbűnözés Németországban is növekvő probléma. Markus Koths, a BKA vezetője szerint ehhez a legnagyobb löketet a 'kiberbűnözés mint szolgáltatás' (CaaS) megjelenése adta. 2016-hoz képest duplázódott, így mintegy 82,000-re nőtt a biztonsági események száma, közel 51 millió eurós kárt okozva. Ez csupán a bejelentett esetekre vonatkozik, ami egyes becslések szerint mindössze 10%-a a valós mennyiségnek, mivel a vállalatok – elsősorban a presztízsveszteségtől való félelmükben – jellemzően nem jelentik be azokat. **Bővebben...**



Új biztonsági rendszert kap az Android
(www.searchsecurity.com)

A Google éves fejlesztői konferenciáján bemutatásra kerültek a plusz védelmi vonalnak szánt 'Google Play Protect' új funkciói, amelyek közül a legfontosabb a korábban letöltött applikációk folyamatos, automatikus ellenőrzése annak érdekében, hogy azok telepítés után se tölthessenek le káros összetevőket. Az alkalmazás ráadásul felhasználói közreműködés nélkül képes intézkedést hozni, amennyiben gyanús aktivitást észlel. A tervek szerint a következő hetekben várható a megjelenése minden olyan eszközön, amelyen telepítve van a 'Google Play'. **Bővebben...**

IT biztonsági tanács

Fontos adatainkról rendszeresen készítsünk biztonsági mentést egy külső adattárolóra, hogy megelőzhessünk egy esetleges adatvesztést, valamint csökkenthessünk egy esetleges vírustámadás következtében fellépő adatvesztés mértékén.

A gyakori adatmentés csökkenti az adatvesztés mértékét.

Érzékeny adatainkat lehetőleg titkosított külső adattárolóra mentsük.

Hogyan védjük a felhőt a zsarolóvírusoktól?
(www.helpnetsecurity.com)

A felhőbiztonsággal foglalkozó Evident.io jó gyakorlatokat közölt, amelyekkel növelhetjük a felhő-alapú szolgáltatások biztonságát. Az ilyen technológiákat használó vállalatok számára a zsarolóvírusok elleni védelem első lépése megérteni, hogy pontosan milyen logikai rétegekből épülnek fel a rendszert alkotó komponensek. Ezen rétegek sajátos biztonsági igényeinek figyelembevételével azután hatásos védelmi intézkedéseket lehet hozni, erre találunk néhány fontos példát. **Bővebben...**

Minden sarkon fenyegetés leselkedik a mobilozókra
(www.helpnetsecurity.com)

Az iPass új jelentése szerint a szervezetek 40 %-a úgy véli a munkahelyen kívül dolgozó C-szintű vezetők a leginkább kitettek egy hacker-támadásnak. Ők számítanak a legvonzóbb célpontnak, mivel jellemzően nem szokványos munkarendben, sok esetben irodán kívül is dolgoznak és olyan érzékeny vállalati adatokhoz is hozzáférnek, amikhez egy átlagos dolgozó nem. Az ingyenes WiFi-t nyújtó internetes kávézók csábító helynek számítanak az irodán kívüli munkavégzéshez, ahol azonban könnyen támadás áldozatává válhatnak. A felmérésben válaszadók mintegy 42%-a is ezt jelölte első számú kockázati helyszínnek emellett sokan (30%) a repülőtereket, illetve a szállodákat (16%) is problémásnak ítélik. **Bővebben...**

NIST keretrendszer
(www.techrepublic.com)

Donlad Trump, az Egyesült Államok elnöke megújította a 2013-ban, még Obama kormányzat által megalkotott kiberbiztonsági végrehajtó rendeletet, melynek célja egy egységes keretrendszer megvalósítása volt. Trump új kiberbiztonsági végrehajtó rendelete nem csak a kormányhoz, hanem bármilyen méretű vállalkozáshoz is igazítható.
Bővebben...

Google vs. USA
(www.forbes.com)

A Google hat különböző szövetségi ügyben folytat tárgyalásokat az Amerikai Egyesült Államok kormánya ellen, melyben az FBI kéri a tengerentúlon tárolt Gmail adatok átadását a cégtől. A Google szerint azonban nincs jogalapja erre, mivel a 'Stored Communications Act' jogszerű alkalmazása egyértelműen csak a belföldi területekre vonatkozik. A törvénnyel kapcsolatban már több hasonló elhúzódó bírósági ügy is volt. **Bővebben...**

A WannaCry támadásnál egy még veszélyesebb jöhet
(www.bgr.in)

A világ még nem heverte ki a WannaCry tömeges terjedését, máris új fenyegetés veszélyezteti a számítógépes világot. Egy új, 'EternalRocks' nevű malware-t fedeztek fel, ami úgy tűnik sokkal veszélyesebb mint a WannaCry, ami így is több mint 300,000 készüléket fertőzött meg összesen, mintegy 150 országban. Az 'EternalRocks' lényegében az NSA-től kiszivárgott 7 különböző kihasználó kódot felhasználva, két fázisban támad. A másodikként letöltődött komponens ráadásul csak 24 óra elteltével aktiválódik, ami nagyban megnehezíti az észlelését. **Bővebben...**