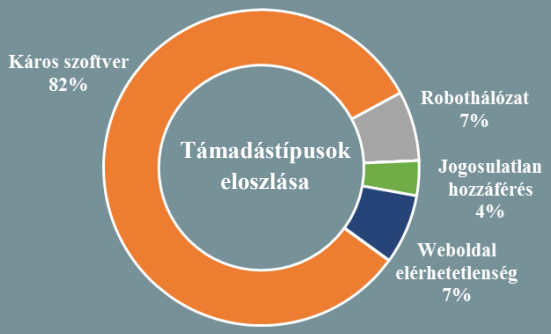
Nemzetközi IT-biztonsági sajtószemle

2017. 49. hét

Incidens adatok: 2017.12.06. — 2017.12.12.



USB eszközök a vállalati szférában

(www.helpnetsecurity.com)

A vállalati USB eszközökre vonatkozó biztonsági szabályok sok esetben elavultak és egyáltalán nem felelnek meg a kritikus vállalati adatok védelmi követelményeinek – állapítja meg az Apricorn. A felmérés szerint hiába támaszkodik 10-ből 9 dolgozó napi munkája során valamilyen USB eszközre, azok mindössze 20%-án alkalmaznak titkosítást, illetve a hatékony monitorozás jellemző hiánya lényeges információbiztonsági kockázatot jelent, ami hozzájárulhat az adatszivárgások bekövetkezéséhez. A megkérdezettek 70%-a úgy véli, az USB eszközök használata javítja szervezetük IT működésének hatékonyságát, valamint hozzájárul a termelékenység növeléséhez is. **Bővebben...**

Kiberbiztonsági találkozó

(www.nato.int)

Az Európai Unió és a NATO felelős tisztviselői múlt hét pénteken gyűltek össze, hogy számbavegyék az információcserére, gyakorlatokra és képzésekre vonatkozó jelenlegi intézkedéseket, illetve megvitassák további fontos területek, mint például a krízismenedzsmenttel kapcsolatos bevált gyakorlatok egymás közötti megosztását. A tisztviselők kiemelten foglalkoztak a NATO Cyber Defense Pledge-hez kapcsolódó legutóbbi fejlesztésekkel is, valamint a kiberműveletek önálló területként történő elismerését célzó törekvésekkel, az EU-s kiberbiztonsági csomag mellett. 2017 szeptemberében az informatikai rendszerek biztonsága új lendületet kapott az "Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése" című közös Európai Uniós közlemény kapcsán. **Bővebben...**

Frissített CSIRT nyilvántartás

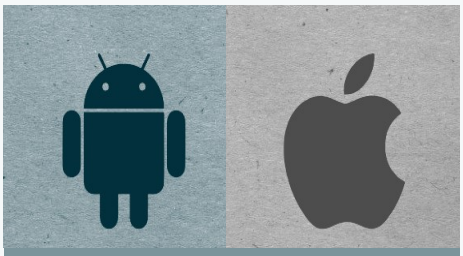
(www.enisa.europa.eu)

A hálózati és információs rendszerek biztonságáról szóló EU-s irányelv (NISD) megvalósításának folyamata során az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) a számítógép-biztonsági és incidenskezelő csoportok (CSIRT) online nyilvántartásán jelentős átalakítást hajtott végre. A nagyobb hatékonyság érdekében új funkciókat vezettek be, melyek főleg a grafikai elemeket és a statisztikai kimutatásokat érintették, ezzel szemléltetve a CSIRT-ek különböző közösségekben (pl.: Trusted Introducer, FIRST) való részvételét, a tagsági állapotukat és az elérhetőségüket. A CSIRT-ek interaktív térképe szerint jelenleg mintegy 45 országban összesen 342 CSIRT létezik, amely jelentős növekedést mutat a korábbi évekhez képest. Ezek közül jelenleg 35 csoport működik NISD-nek megfelelően. **Bővebben...**

Újabb felszólítás a tech óriásoknak

(www.theguardian.com)

Az Európai Bizottság arra szólítja fel az olyan tech óriásokat, mint a Facebook, a Google, a Youtube, vagy a Twitter, hogy tegyenek nagyobb erőfeszítéseket a szélsőséges tartalmak terjedésének megakadályozásához. Bár az elmúlt két évben bíztató előrelépések történtek az EU-s jogszabályoknak való megfelelés érdekében, Julian King – az EU biztonsági biztosa szerint ideje felgyorsítani a folyamatokat. Amennyiben az EU nem lesz elégedett az érintett vállalatok illegális tartalmak blokkolására, illetve azok gyors eltávolítására vonatkozó intézkedéseivel, kényszerítő jogszabályokat hozhat. A ''Global Internet Forum''-on résztvevő vállalatok szerint ugyanakkor már így is komoly előrehaladás történt az Europol részvételével, ugyanis a közösen létrehozott, ismert terrorista személyekről információt tartalmazó adatbázis már több, mint 40 000 mintát tartalmaz, amelynek segítségével akár 2 óra alatt detektálható és eltávolítható a káros tartalom. **Bővebben...**



Mobil eszközök biztonsága
(www.itproportal.com)

A mobil eszközökön folytatott munkavégzés napjainkban életmóddá vált, így a vállalatok kezdik kialakítani a saját BYOD (Bring-your-own-device) politikájukat, ennek részeként pedig igyekeznek lehetővé tenni munkavállalóik számára, hogy a vállalati infrastruktúrához és adatokhoz távolról is hozzáférjenek. Az ennek érdekében bevezetett biztonsági intézkedések ellenére a mobil eszközök növekvő száma nagyobb kockázatot is jelent, amelyet a közelmúlt adatszivárgási incidensei (Uber, Equifax, Yahoo, Deloitte) is alátámasztanak. A Check Point tanulmányának elkészítése során megkérdezett vállalatok 20%-a nyilatkozott úgy, hogy szenvedtek már el támadást, míg 94%-uk számít a jövőben az ilyen jellegű támadások számának megnövekedésére. **Bővebben...**

IT biztonsági Tanács

Hálózatunk és az átmenő adatforgalom biztonsága érdekében javasolt minden esetben lecserélni routerünk adminisztrátori felületének, valamint a WiFi hozzáférésének gyári jelszavát.

Amennyiben készülékünk lehetővé teszi, saját WiFi hálózatunk mellett alakítsunk ki vendéghálózatot is.

Biztonsági javaslatok az amerikai választási rendszer védelméhez
(www.infosecurity-magazine.com)

Egy chicago-i választási képviselő biztonsági tervet tett közzé, melynek célja az amerikai választások folyamatainak biztonságossá tétele. A DEFCON és a Chicagói Egyetem szervezésében megtartott eseményen bemutatott program számos stratégiát ismertet az érdekelt felek számára a szavazási infrastruktúra (szavazórendszerek, hálózatok és adatbázisok) védelmére vonatkozóan, valamint a fenyegetések felderítésére és az incidensekből való felépülés támogatására. A javaslatok között szerepel például egy, a szavazás biztonsági vonatkozásaiért felelős személy (EIISO) kinevezése, tudatosító képzések indítása, auditok szervezése. Emellett olyan könnyen megvalósítható, mégis átfogó tevékenységeket is tartalmaz a szövetségi vezetők számára, amelyekkel hatékonyan támogathatják az ország több, mint 9 000 szavazati joghatóságát. **Bővebben...**

Készül a NIST kiberbiztonsági keretrendszerének új verziója
(securityaffairs.co)

Az amerikai Nemzeti Szabványügyi és Technológiai Intézet (NIST) december 5-én adta ki a kritikus infrastruktúrák kiberbiztonsági védelmének növelését célzó keretrendszer második tervezetét, amely egy nyilvános véleményezési időszak, valamint egy workshop során gyűjtött tapasztalatok alapján került most frissítésre. Az új verzió többek között deklarálja a keretrendszer alkalmazhatósági körtét és nagyobb segítséget nyújt az ellátási láncok kockázatmenedzsmentjéhez való felhasználáshoz. A jelenlegi kiadást a tervek szerint 2018 során cserélik. **Bővebben...**

A Szövetségi Kommunikációs Bizottság eltörölte a netsemlegességet
(www.bleepingcomputer.com)

Az FCC 3-2 arányban megszavazta az Obama kormány által hozott netsemlegességet biztosító szabályok hatályon kívül helyezését. Ajit Pai, az FCC vezetője szerint az intézkedés a fogyasztók javát szolgálja majd azáltal, hogy élénkíti a versenyt. A demokrata párti biztosok szerint azonban ezek a szabályok fogták vissza az internetszolgáltatókat attól, hogy a tartalmakhoz való hozzáférés differenciálásával befolyásolják a felhasználókat. A szolgáltatók eddig általánosságban úgy nyilatkoztak, hogy nem kívánnak változtatni az eddigi ügymeneten. **Bővebben...**

Kitiltották a Kaspersky termékeket az amerikai kormányzati rendszerekről
(www.cnet.com)

Donald Trump kedden hitelesítette a 2018-as nemzeti védelempolitikát meghatározó törvényt (National Defense Authorization Act), mely többek között rendelkezik a Kaspersky Lab biztonsági cég termékeinek a kormányzati hálózatokból való kitiltásáról. Ennek értelmében a szövetségi hivataloknak 30 napjuk van az összes Kaspersky-s szoftver azonosítására, ezt követően 60 nap áll rendelkezésre, hogy megkezdjék azok eltávolítását. A 2016-os amerikai elnökválasztás befolyásolására irányuló orosz tevékenység kapcsán több kormányzati intézkedést is hoztak korábban. Az Egyesült Államok elnöke májusban elnöki rendeletben szólította fel az amerikai kormányzati szerveket, hogy korszerűsítsék számítógépes rendszereiket és erősítsék meg azok védelmét. Szeptemberben pedig a Belbiztonsági Minisztérium (DHS) adott ki kötelező érvényű irányelvet, melyben már korlátozták a Kaspersky Lab termékek használatát. **Bővebben...**