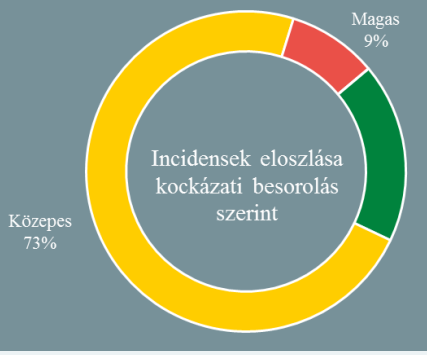
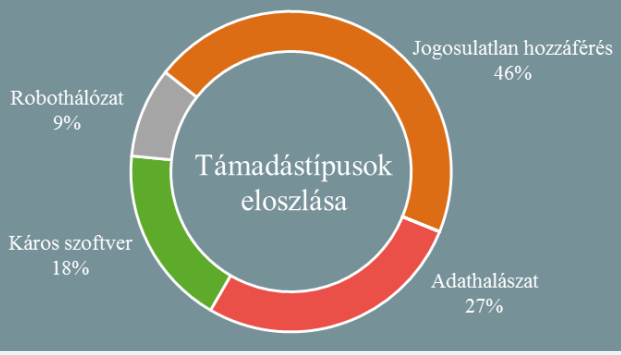
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.02.01. - 2019.02.07.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon, ahol naponta olvashatja legújabb híreinket!

Adatsértés miatt először tiltott ki terméket piacáról az EU

(www.zdnet.com)

Súlyos adatvédelmi aggályokra hivatkoztak az uniós hatóságok, amikor bejelentették az ENOX Safe-KID-One okosórák európai piacról való visszavonását. A német elektronikai gyártó weboldalán feltüntetett információk szerint az eszköz minden olyan tulajdonsággal ─ beépített GPS nyomkövetővel, mikrofonnal és hangszóróval, valamint SMS és hívó funkcióval ─ rendelkezik, amit a szülők elvárnak egy okosórától, azonban az Európai Bizottság által működtetett, nem élelmiszer jellegű veszélyes termékek európai riasztási rendszerében (RAPEX) súlyos kockázati besorolást kapott a termék. **Bővebben...**

Incidens reagálási képességek Európában

(www.enisa.europa.eu)

Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) összefoglaló jelentésében szeretne átfogó képet nyújtani az európai számítógép-biztonsági és incidenskezelő csoportok (CSIRT-ek), valamint az incidens reagálási képességek (IR) utóbbi öt év során tapasztalt fejlődéséről. Az elemzés során mintegy 81 új CSIRT-et azonosítottak, és 36 szabályozó dokumentum került átvizsgálásra. A tanulmány főbb megállapításai között szerepel, hogy a NIS irányelv implementálása pozitív hatást gyakorol az incidenskezelési képességek fejlesztésére, valamint egy uniós norma kialakítására, illetve, hogy lényeges fejlesztés tapasztalható az európai magánszektor tekintetében, ugyanakkor az EU-n kívül gyártott hardverelemek egyre nagyobb kockázati tényezőt jelentenek. **Bővebben...**

Az ENISA online eszközzel támogatja az IoT ipar biztonságát

(www.enisa.europa.eu)

Az ENISA január 31-én nyilvánosságra hozta az IoT eszközökkel kapcsolatban felmerült kockázatok azonosításában, illetve a biztonsági kérdések priorizálásában segítséget nyújtó online eszközét, amely átfogó képet szeretne nyújtani az ENISA által tavaly kiadott, okoseszközökre vonatkozó ajánlásairól, mint például a „Jó gyakorlatok az IoT biztonságának megteremtéséhez az okos gyártás kontextusában", vagy az „Alapvető biztonsági ajánlások az IoT számára". Az eszköz segítségével a szervezetek számára a védelem kialakításához meghatározhatóak a főbb fenyegetési csoportok, a lefedni kívánt biztonsági területek, vagy hogy mely standardokat és legjobb gyakorlatokat kívánják figyelembe venni.

A Trump-kormányzat kiberbiztonsági szabályainak értékelése

(www.infosecurity-magazine.com)

Az egyesült államokbeli Foundation for Defense of Democracies (FDD) kiadta a Trump-kormányzat hivatali ciklusának első felében végzett kül- és nemzetbiztonsági témájú szabályozási tevékenységének értékelését, amely külön fejezetben tárgyalja a kiber-vonatkozású intézkedéseket. Kiemeli a 2017 májusában aláírt elnöki végrehajtási utasítást ─ amely előírta az állami és magán szektor szereplőinek együttműködését a kritikus infrastruktúrák hatékonyabb védelme érdekében ─ valamint a hét hónappal később kiadott első nemzeti biztonsági stratégiát. **Bővebben...**

Az Apple regionális adattárolásra készül Oroszországban

(www.bloomberg.com)

Az Apple bejelentette, hogy összegyűjti az orosz felhasználói adatokat ─ név, szállítási- és e-mail cím, valamint az orosz szervereken tárolt telefonszámokat ─ annak érdekében, hogy megfeleljen egy 2015-ben hatályba lépett jogszabálynak, amely kimondja, hogy a szolgáltatók kizárólag az ország határain belül tárolhatják az orosz állampolgárok adatait. A bejelentés nem tesz említést az iCloud szolgáltatáson tárolt adatokra ─ üzenetekre, dokumentumokra, fényképekre és kapcsolati adatokra ─ vonatkozóan, amelyek kapcsán a tavalyi évben a kínai jogszabályi kötelezettségek miatt hasonlóan kellett eljárnia a vállalatnak, bár az iCloud felhasználói adatokon kívül, a fiókokhoz hozzáférést biztosító kulcsok is áthelyezésre kerültek Kínába. Tim Cook, az Apple vezérigazgatójának álláspontja szerint kénytelenek megfelelni az ilyen típusú nemzeti jogszabályoknak, bár már akkor igyekezett hangsúlyozni, hogy a felhasználói adatok és kulcsok biztonsága érdekében az Apple saját titkosítási technológiát alkalmaz és kizárólag a hatályos jogszabályi előírásoknak megfelelően szolgáltatnak adatokat. **Bővebben...**

IT biztonsági Tanács

A Microsoft tavaly elérhetővé tette Active Directory szolgáltatásához az Extranet Soft Lockout (Windows Server 2012 R2 használata esetén), valamint az Extranet Smart Lockout (Windows Server 2016 és 2019 esetén) biztonsági megoldásokat. Ezek célja megvédeni a jogosult felhasználókat a fiókjukból történő kizárástól, ugyanakkor védelmet nyújtani a próbálgatáson alapuló jelszótörési kísérletek ellen. A konfiguráláshoz hasznos információk érhetők el a gyártó honlapján.

Új sérülékenységeket fedeztek fel az RDP protokoll kapcsán

(bleepingcomputer.com)

A Check Point biztonsági szakemberei sérülékenységeket fedeztek fel egyes távoli asztal elérést biztosító RDP klienseket érintően. A biztonsági hibák lehetőséget adnak a kliens gépek kompromittálására ún. „reverse RDP támadás" során, amennyiben az áldozat ─ például egy rendszergazda ─ távoli asztal kapcsolattal bejelentkezik egy, a támadó irányítása alatt álló munkaállomásra vagy szerverre. A kutatók által felfedezett biztonsági problémák a nyílt forráskódú FreeRDP-t, valamint az rdesktopot érintik, de a vizsgálatok során a Microsoft saját RDP implementációjában (mstsc) is találtak egy könyvtárbejárás támadásra módot adó problémát.

Közel félmillió Ubiquiti eszköz lehet veszélyben

(securityaffairs.co)

Biztonsági kutatók szerint ─ vélhetően egy biztonsági hiba kihasználására irányuló ─ támadási kísérletek zajlanak olyan Ubiquiti hálózati eszközök ellen, amelyek a 10001-es UDP porton keresztül elérhetőek az Internet felől. Az Ubiquiti airOS firmware-ét érintő sérülékenység már tavaly június óta ismert, a gyártó pedig már dolgozik a firmware javításon, addig is megkerülő megoldásként javasolja a port internet felől történő tiltását, azzal a megjegyzéssel, hogy ez egyes szolgáltatások esetében fennakadásokat okozhat. A Rapid7 szerint jelenleg körülbelül 490 000 ─ javarészt Brazíliában, az Egyesült Államokban és Spanyolországban található ─ Ubiquiti eszköz érhető el a nevezett porton keresztül.

Kínát gyanúsítják a norvég Visma elleni kibertámadással

(zdnet.com)

A Rapid7 és a Recorded Future amerikai kiberbiztonsági cégek közös jelentése szerint a kínai államhoz köthető APT10 csoport áll az európai vállalatoknak felhő-alapú szoftveres szolgáltatásokat nyújtó, norvég Visma vállalat elleni kibertámadás mögött. A támadás 2018 augusztus 17-én történt, ennek során sikeresen kompromittálták a cég belső hálózatát, amelyhez egy Citrix fiók ellopott hitelesítő adataival fértek hozzá, majd két malware (Trochilus RAT és Uppercut backdoor) segítségével megkezdték az adatlopást. A Visma közleménye szerint a támadók csak belső céges információkhoz fértek hozzá, a kliensek adatait tartalmazó rendszereket nem érintette az incidens. A Rapid7 szerint az eset a 2017 óta zajló „Operation Cloudhopper" kiberkémkedési művelet részét képezi, amely elsősorban felhőszolgáltatókat céloz világszerte.

Egyes e-jegyrendszerek nem védik megfelelően a légiutasok adatait

(cyberscoop.com)

Legalább nyolc légitársaság (Southwest, Air France, KLM, Vueling, Jetstar, Thomas Cook, Transavia, Air Europa) használ olyan e-jegyrendszert, amely nem védi megfelelően utasainak adatait ─ derül ki a mobil biztonsággal foglalkozó Wandera tanulmányából. A biztonsági probléma abból fakad, hogy a jegyfoglalási rendszer reptéri utasfelvétellel (check-in) kapcsolatos információkat küld az utasoknak e-mailben, olyan hiperhivatkozásokkal, amelyek titkosítatlan formában tartalmazzák az ügyfelek adatait. Ez ugyan lehetővé teszi az utasok számára, hogy további hitelesítés nélkül ellenőrizzék és módosítsák a foglalásukat, azonban biztonsági kockázatot is hordoz magában.