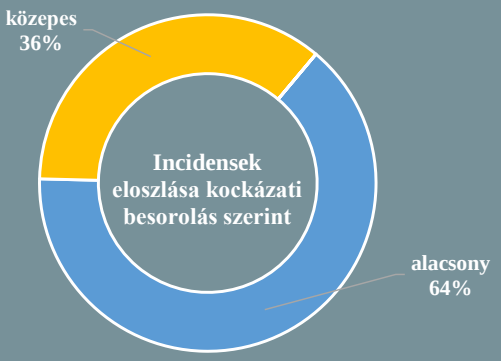
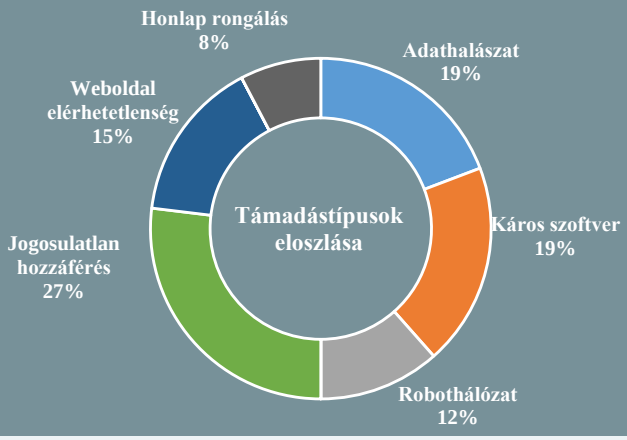
Incidens adatok:
2017.07.12. — 2017.07.18.





Szingapúr: szigorítás a kritikus információs infrastruktúrák védelmében

(www.databreachtoday.com)

Nyilvános konzultációt hirdetett a szingapúri Kommunikációs és Információs Minisztérium és a Kiberbiztonsági Ügynökség (CSA) Szingapúr új kiberbizonsági jogszabálytervezete kapcsán. A tervezet szigorú előírásokat fogalmaz meg a kritikus információs infrastuktúrákat üzemeltetők számára, például előírja, hogy az adatszivárgások bejelentésének néhány óra alatt meg kell történnie, emellett a kiberbiztonsági termékeket és szolgáltatásokat nyújtó cégek számára a kiemelten érzékeny szolgáltatásokat engedélyhez köti. A cél egy olyan átfogó keretrendszer megalkotása, amely minden létfontosságú szolgáltatásra vonatkozik, mivel a jelenleg hatályos jogszabály elsősorban a kiberbűnözésre fókuszál. Mindez magába foglalja a CSA szerepének és lehetőségeinek a bővítését is. Egyes kutatók szerint a szigorítás ugyan pozitív hatással lesz a biztonságra, azonban az érintett szervezetek számára hatalmas terhet jelent majd a megfelelés biztosítása. **Bővebben...**

India nagyszabású kiberbiztonsági programba fog

(cio.economictimes.indiatimes.com)

A tervek szerint az indiai National Cyber Coordination Center (NCCC) az országos hálózati forgalom monitorozásával és támadás gyanú esetén valós idejű elemzéssel és beavatkozással szeretné megakadályozni India kiberterében történő nagyobb támadásokat. A központ az internetszolgáltatók eszközein és egyes adatközpontokon keresztül kíván hozzáférni a hálózati forgalomhoz. Kezdetben néhány adatközpontot és két internet szolgáltatót vonnának be, utóbbi kapcsán az állami tulajdonú BSNL-t nevezték meg. A program július végén vagy augusztus elején indul és az első időszakban szervezetileg a CERT-In részeként. **Bővebben...**

Betörtek egy amerikai védelmi szoftvereket gyártó cég rendszerébe

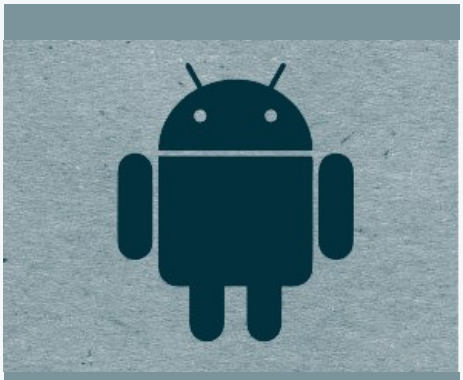
(www.theregister.co.uk)

Az amerikai Igazságügyi Minisztérium szerint két iráni személy kompromittálta a védelmi technológiát fejlesztő egyesült államokbeli Arrow-Tech rendszerét. A vádak szerint öt évig készítették elő a támadást, amelynek során beszivárogtak a vállalat hálózatába. Céljuk a 'PRODAS' nevű integrált fegyvertervezési szoftver megszerzése volt, amelyet azután Iránnak és más államoknak értékesítettek volna. A PRODAS USA-n kívüli exportja korlátozott és valószínűtlen, hogy valaha is engedélyt kapott volna a technológia Iránnak való értékesítése. A szoftver eladási ára 40 és 800 ezer dollár között mozog. **Bővebben...**

Az ír energia szektort is támadás érte

(www.independent.co.uk)

A mind Észak-Írország, mind az Ír Köztársaság számára villamos energiát nyújtó Electricity Supply Board vezető mérnökei személyre szabott, káros kóddal fertőzött e-maileket kaptak. Elemzők véleménye szerint a támadók célja a vezérlőrendszerekbe való beszivárgás lehetett, amellyel a villamosenergia-hálózat tömeges leállását idézhették volna elő, hasonlóan ahhoz, ami Ukrajnában történt. Írország kibervédelmi központja vizsgálja az esetet, amely az eddigi információk szerint nem okozott zavart a hálózatban, de nem zárható ki, hogy a támadóknak sikerült érzékeny adatokat megszerezniük, például jelszavakat. **Bővebben...**



Biztonságosabb lesz a Google Play Áruház

(threatpost.com)

Múlt hét szerdán a Google megosztott néhány részletet a 'Peer Group Analysis' nevű új védelmi funkcióról, ami a gépi tanulás módszertanát is alkalmazva igyekszik kiszűrni a gyanús alkalmazásokat. Ehhez a Google először funkció alapján típuscsoportokba sorolja az internetes áruházába feltöltött alkalmazásokat, majd biztonsági szempontból elemzi azok működését. Többek között vizsgálja a jogosultság igényeket és a megfigyelt tevékenységeket, illetve egyéb meta adatokat. Az összegyűjtött jellemzők alapján történik meg a típuscsoporttal való összehasonlítás, ami ha eltérést mutat, káros minősítést kaphat az applikáció. **Bővebben...**

IT biztonsági Tanács (nyaralásra)

Utazásaink és nyaralásunk alkalmával is tartsuk naprakészen szoftvereinket, valamint kapcsoljuk ki a szükségtelen szolgáltatásokat és funkciókat (tartózkodási helyzet megosztás, WiFi, Bluetooth).

WiFi hotspotok használatakor tekintsük azokat nem megbízható internetelérésnek és fontoljuk meg VPN szolgáltatás igénybevételét.

Minden eddiginél nagyobb kockázat éri a kritikus infrastruktúrák rendszereit

(www.information-age.com)

Az amerikai SANS intézet több száz szakember – részint ipari vezérlőrendszereket (ICS) üzemeltetők, részint energia szektorbeli kiberbiztonsági felelősök – bevonásával felmérést végzett az ICS rendszerek biztonsági helyzetének felméréséhez. Eszerint tízből négy ICS hálózati szempontból átláthatatlan, az érintett rendszerek védelmi felelőseinek 40%-a anélkül kénytelen ellátni a feladatát, hogy időben detektálni tudná a támadásokat és meg tudná állapítani azok forrását. A legnagyobb kockázatot azon eszközök jelentik, amelyek nem rendelkeznek önálló hálózati védelemmel, ezek után a nem szándékosan okozott belső incidensek, a hacktivisták és állami támogatású hackerek okozta fenyegetések, illetve a lista élbolyába frissen felkerült zsarolóvírusok következnek. Egy másik fontos megállapítás szerint a válaszadók mindössze 46%-a telepíti rendszeresen a biztonsági frissítéseket. **Bővebben...**

Új Apple adatközpont Kínában

(www.securityweek.com)

Az Apple bejelentette, hogy létrehozza első kínai adatközpontját, annak érdekében, hogy javítsa szolgáltatásait a régióban, illetve, hogy képes legyen megfelelni az új kínai kiberbiztonsági előírásoknak. Ennek értelmében a kínai felhasználóik iCloud-os adatait egy helyi, állami tulajdonú cég, a Guizhou-Cloud Big Data kezeli majd. A közleményében azonban kiemelték, hogy a vállalatra jellemző szigorú adatvédelmi és biztonsági irányelveken továbbra sem módosítanak, valamint nem építenek hátsó kaput a rendszerbe a kínai kormány számára. **Bővebben...**

Sérülékenyek a katonai légi járművek

(in.reuters.com)

A német hadsereg repülésbiztonsági vezetője új kezdeményezést indított a számítógépes fenyegetések ellen. Ansgar Rieks vezérőrnagy, a Német Katonai Légiközlekedési Hatóság vezetője az Aerospace Center (DLR) azon bemutatójára hivatkozva beszélt erről, ahol demonstrálták, hogy hackerek képesek lehetnek átvenni az irányítást katonai légi járművek felett, mindezt egy relatíve olcsó (nagyjából 5 000 eurós) eszköz segítségével. Az intézkedés kidolgozásában a Bundeswehr új kiberparancsnoksága (CIR) is részt vesz. **Bővebben...**

Átszervezik az amerikai kiberparancsnokságot

(www.foxnews.com)

Több hónapos halogatás után véglegesítési szakaszba ért az USA katonai kiberparancsnokságának átszervezésére vonatkozó tervezet. Mindeddig annyi bizonyos, hogy leválasztanák a Nemzetbiztonsági Ügynökségről (NSA), ennél pontosabb részleteket azonban még nem hoztak nyilvánosságra. A szervezet vezetőjének minden valószínűség szerint William Mayville tábornokot kérik fel. Az átszervezés hátterében az a cél áll, hogy nagyobb szabadságot biztosítsanak a szervezetnek, mivel eddig sok olyan törvényi megkötés vonatkozott a kiberműveletekre, amelyek a katonai operatív célokkal ütköztek. Egyes szakértők szerint ugyan a változtatás elkerülhetetlen, azonban nehéz és valószínűleg hosszú folyamat lesz elérni az NSA kompetencia szintjét. **Bővebben...**