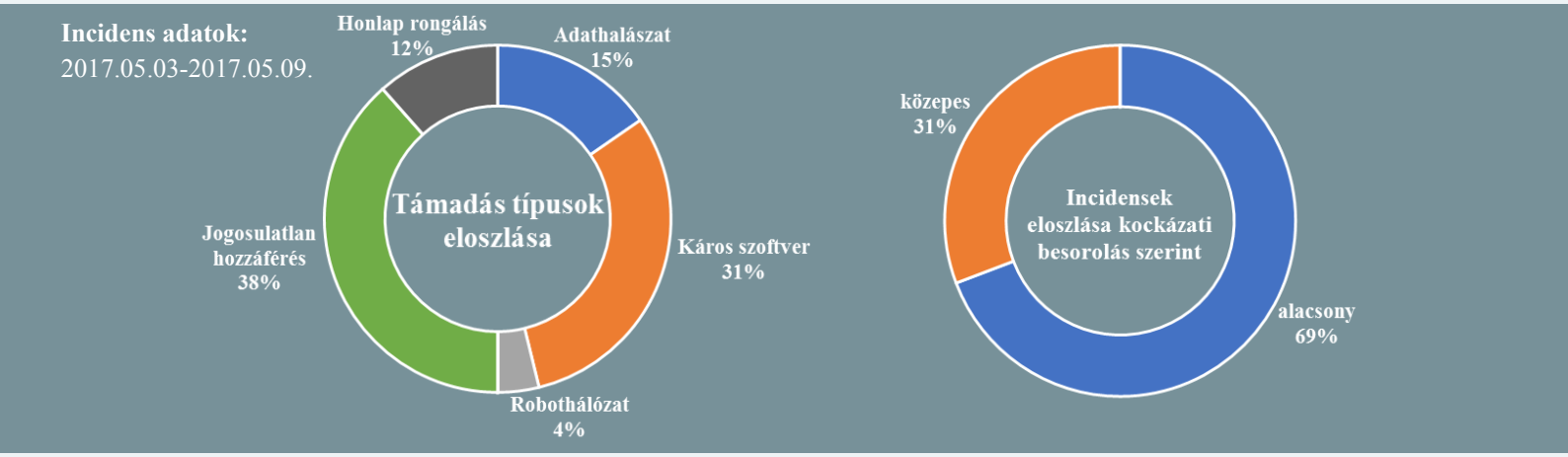
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

18. hét



Kibertámadások mindig is lesznek

(www.computerworld.com)

A vállalatokat ért kibertámadások olyan nagy számban fordulnak elő, hogy egyes nagyobb szervezetek mára elfogadták, hogy azok előbb-utóbb biztosan be fognak következni. A hangsúlyt ennek megfelelően – természetesen a hagyományos védelmi intézkedések megtartása mellett – egyre inkább arra helyezik, hogy képesek legyenek a támadásokat minél előbb felderíteni, ezzel minimalizálva az okozott kárt. Az újfajta koncepció központi eleme a fejlett elemző technikákat alkalmazó anomália detekció, ami teljesen új piacokat eredményezett az IT biztonsági termékek és megoldások palettáján. **Bővebben...**

Németország további kibertámadásokra számít

(www.in.reuters.com)

A német elhárítás (BfV) szerint nagy a valószínűsége, hogy a szeptember 24-én esedékes választásokig több támadás érjen német politikusokat és kormányzati tisztviselőket. Hans-Georg Maassen, a BfV elnöke egy potsdam-i konferencián jelezte, az ügynökség kiemelten figyel ezekre a fenyegetésekre. Erre példaként az Angela Merkel-féle CDU-t ért célzott adathalász támadások elhárítását hozta fel. **Bővebben...**

Szenzitív adatok szivárogtak ki az Aadhar rendszeréből

(www.infosecurity-magazine.com)

A világ legnagyobb biometrikus azonosító rendszere, az indiai Aadhaar mintegy 135 millió indiai állampolgár személyes azonosítójának publikus elérhetőségéért felelős. Mivel már korábban is merültek fel kétségek a rendszer biztonságát érintően, a 'The Centre for Internet and Society' mélyreható vizsgálatot végzett, ennek eredményeként került napvilágra az incidens. **Bővebben...**

A brit kormány kibővítené az internethasználat megfigyelését

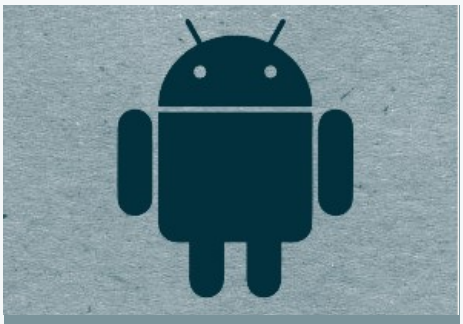
(www.digitaljournal.com)

Az Open Rights Group civil emberjogi szervezet által nyilvánosságra hozott dokumentum szerint a brit kormány (közel) valós időben monitorozná az Egyesült Királyság területén a felhasználók webes és telefonos kommunikációját. A törvénytervezet, amennyiben elfogadják, az 'Investigatory Powers Act' vonatkozó részeit módosítaná oly módon, hogy a hírszerző ügynökségek és bűnüldöző szervek számára egy munkanap átfutási idő alatt elérhetővé tenné bármely személy adatait. A javaslat emellett érinti a végponti titkosítás kérdését is, előírná a szolgáltatók számára a titkosított kommunikációhoz való hozzáférés lehetővé tételét. **Bővebben...**

A kormányzati szektor az egyik fő célpont

(www.itproportal.com)

100%-kal nőtt a kormányzati szféra elleni számítógépes támadások mértéke 2016-ban, így összesítésben vezeti a főbb célpontok listáját, adja hírül a 'Dimension Data' jelentése, amely több mint száz nemzetállamot ért kibertámadás elemzésével készült. A cég biztonsági vezetője, Matthew Gyde szerint a kormányzatok a birtokolt nagy mennyiségű szenzitív adat miatt folyamatos veszélynek vannak kitéve rivális államok, terroristák és kiberbűnözök által. "Érdekes adat, miszerint idén sok olyan incidenst tapasztaltunk, amelyek belső fenyegetéshez köthetők." **Bővebben...**



Közel 10 másodpercenként felfedeznek egy új androidos maleware-t

(www.techrepublic.com)

A G DATA biztonsági cég jelentése szerint 8,400 új Android maleware mintát fedeznek fel naponta. A felmérések alapján 2016-ban összesen 3,2 millió új Androidos malware-t találtak, a G DATA pedig arra számít, hogy ez a szám 2017-ben elérheti a 3,5 milliót is. A vizsgálat során az is kiderült, hogy a felhasználók többsége még mindig a régebbi verziókat használja, amelyek jóval sérülékenyebbek. **Bővebben...**

Adathalász támadás elleni védelem

(www.techcrunch.com)

A napokban történt Gmail felhasználókat ért adathalász támadás következtében a Google egy új biztonsági szolgáltatást fejleszt ki az Android alapú Gmail alkalmazáshoz, mely figyelmezteti a felhasználókat a gyanús linkekre. **Bővebben...**

IT biztonsági tanács

Érdemes figyelni az adathalász oldalakra, ahol a csaló weboldal egy jól ismert szervezet hivatalos oldalának láttatja magát. Ezek célja, hogy érzékeny adatokat szerezzenek a felhasználóktól.

A felhasználók és az ügyfelek folyamatos biztonságtudatosításával, valamint megfelelő szabályzók kialakításával csökkenthető a támadások sikeressége.

Hogyan látják a GDPR-t az európai szervezetek

(www.helpnetsecurity.com)

Egy felmérés szerint az európai vállalkozások alapvetően nem keresik a biztonsági ipar nyújtotta azokat a megoldási lehetőségeket – mint például a kiszervezett biztonsági szolgáltatások (MSSP) – amelyek alkalmasak az új európai uniós adatvédelmi rendelet (GDPR) által támasztott elvárások kezelésére. Valójában a digitális átállás fő mozgató rugói – ide értve a felhő-alapú technológiákat, mobil és IoT megoldásokat – keltik a legtöbb, biztonsággal kapcsolatos aggodalmat. Az uniós jogszabályt 2018. május 25-től kell alkalmazni, így a vállalatoknak egy évük maradt a megfelelés kialakítására.

A 4. ipari forradalom IT biztonsági veszélyei

(www.cnet.com)

A Trend Micro és a Politecnico di Milano mélyreható vizsgálatot folytatott vezető gyártók által használt ipari robotokon, amelynek során megállapítást nyert, hogy a vizsgált eszközök és rendszerek gyenge hálózati biztonsággal rendelkeznek. A távolról vezérelhető gépek felett a hackerek könnyedén át tudják venni az irányítást, szabotázst és termékhibákat képesek előidézni. Megoldást a Trend Micro szerint egy átfogó kiberbiztonsági szabvány jelentene. **Bővebben...**

Támadás érte Emmanuel Macron kampányát

(www.reuters.com)

Az 'En Marche!' közleményben tudatta, hogy egy támadás során ismeretlenek megszerezték, majd – néhány nappal a választások előtt – online elérhetővé is tették kampányuk levelezését. Mintegy 9 gigabyte-nyi adatot posztoltak ki 'EMLEAKS' profilnév alatt a Pastebin-re. Az incidenst követően, az akkor még érvényben lévő kampánycsend miatt hivatalos állásfoglalás nem történt. A nyomozószervek kérésére a média sem közölt információkat a nyilvánosságra került adatokról. **Bővebben...**

A SOC-ok kihívásai

(www.helpnetsecurity.com)

Egy új SANS felmérés szerint a 'security operation center'-ek (SOC) habár fejlődésen mentek keresztül – belső szolgáltatásaikat immár felhő-alapú technológiákkal is kiegészítik – kijelenthető, hogy a szervezetek továbbra sem képesek detektálni az ismeretlen fenyegetéseket. Ezen a téren nagyobb mértékű automatizálására van szükség, azontúl a hálózati műveleti központtal (NOC) történő szoros integrációra, ami – hiába kulcsfontosságú elem – a válaszadók csupán 12%-nál van jelen a kívánt mértékben.
Bővebben...

Elegendő lesz-e a Symantec akcióterve?

(www.searchsecurity.techtarget.com)

A Symantec komoly változásokat eszközölne az SSL/TLS tanúsítvány kibocsátási gyakorlatán. A nagyobb böngésző gyártók és a Symantec között régóta tartó huzavona márciusban új szintre lépett, mikor is a Google bejelentette a biztonsági cég által kiállított tanúsítványok elfogadásának korlátozását. A Symantec erre reagálva egy akciótervet hozott nyilvánosságra, amellyel – az ígéret szerint – sikerül kiküszöbölni a legkritikusabb problémákat. Egyes vélemények szerint azonban ez sem lesz feltétlenül elegendő arra, hogy helyreállítsa a tanúsítványaikba vetett bizalmat. **Bővebben...**