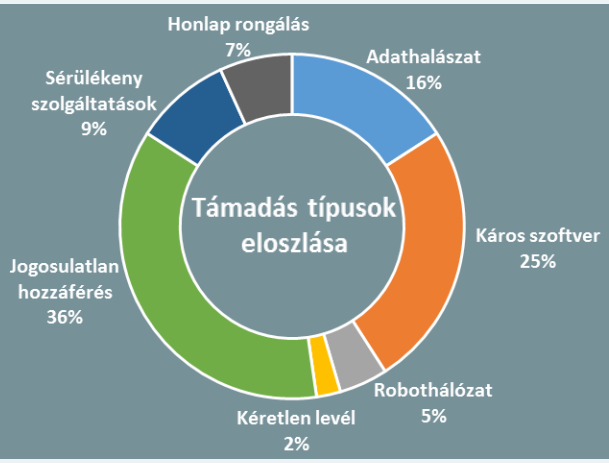
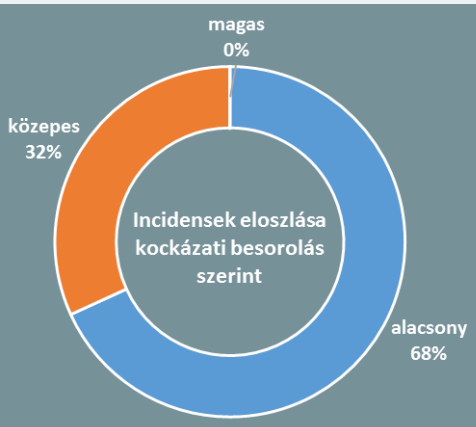
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

IT-biztonsági sajtószemle

16. hét





Késik a Trump-féle kiberbiztonsági tervezet

(www.cnet.com)

Donald Trump januárban azt az ígéretet tette, hogy a hivatalba lépését követő 90 napon belül kinevez egy kiberbiztonsági csapatot, amelynek feladata egy átfogó kiberbiztonsági tervezet megalkotása az Egyesült Államok számára. A Fehér Ház szóvivője szerint ugyan már felállt egy részben kormányzati, részben magánszférából érkező szakemberekből álló csoport, azonban konkrét intézkedésekről, eredményekről továbbra sincs hír. **Bővebben...**

Még mindig az emberi tényező számít a legnagyobb problémának

(www.infosecurity-magazine.com)

Az Institute of Information Security Professionals (IISP) IT biztonsági felmérése alapján a vezető kockázati tényező továbbra is a humán erőforrás (81%), míg a technológiai és a folyamatokból adódó kockázatok jóval kevésbé mérvadóak. A jelentés szerint a legnagyobb probléma, hogy a nyugdíjba vonuló, tapasztalt szakemberek utánpótlása nem megoldott, valamint kitér az alkalmazottak kiberbiztonsági kézségeivel kapcsolatos kihívásokra és a változó munkaerőpiac dinamikájára is. **Bővebben...**

Kétfaktoros hitelesítés a környezeti zaj felhasználásával

(www.heise.de)

A kétlépcsős hitelesítés lassan szabványnak számít az online szolgáltatásoknál. A svájci ETH kutatói kifejlesztettek egy új eljárást, amely nem igényel emberi interakciót. A 'Sound Proof' egy intelligens algoritmus segítségével összehasonlítja két eszköz (például egy laptop, amelyen keresztül a szolgáltatást elérni kívánjuk és egy okostelefon) környezetéből származó zajokat, annak megállapítására, hogy ugyanabban a helyiségben tartózkodnak-e. Amennyiben igen, automatikusan autentikálja a felhasználót. **Bővebben...**

A francia választások váltak az APT28 célpontjává

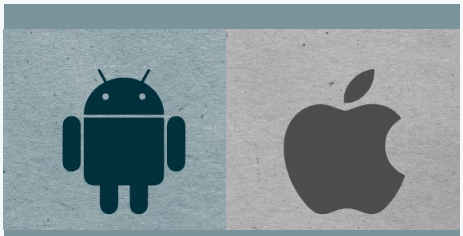
(www.motherboard.vice.com)

A Trend Micro bizonyítékot talált arra, hogy az APT28 legalább négy, Emmanuel Macron politikai pártjának nevéhez (En Marche) hasonló domain-t, valamint hozzájuk tartozó e-mail címeket hozott létre. A hacker csoport célja valószínűleg adathalászati kampányok indítása, hogy befolyásolhassák a választásokat. **Bővebben...**

Biztonsági készségek a kritikus kockázatok kezelésére

(www.helpnetsecurity.com)

Egyre többen ismerik fel, hogy az informatikai biztonság elengedhetetlen egy szervezet életében, azonban ez a legtöbb esetben kimerül a szoftveres támadások kivédésére tett intézkedésekben. Seth Robinson a CompTIA vezérigazgatója szerint ez nem elegendő, egy új, átfogó megközelítés szükséges, amely a technikai megoldásokon kívül kiterjed az eljárásokra, oktatásokra, valamint külső auditokkal, sérülékenység vizsgálattal egészül ki. **Bővebben...**



Zseblámpás trójai

(www.scmagazine.com)

Egy zseblámpa alkalmazásnak álcázva szivárgott be egy rosszindulatú trójai program a Google Play áruházba. Az alkalmazás adminisztrátori jogosultságokat kér, amelyek birtokában regisztrálja a fertőzött eszközt a támadó szerverére és megkezdi káros tevékenységeit (SMS lehallgatás, hamis értesítések küldése, stb.) **Bővebben...**

Kína szigorúbb ellenőrzést kér az Apple-től

(www.reuters.com)

Kínai internetes szabályzók felszólították az Apple-t, hogy szigorítsa az Apple Store-ban elérhető szoftveralkalmazások ellenőrzését, mivel az amerikai cég egyre több alkalmazást és szolgáltatást értékesít Kínában. A hírek szerint már meg is kezdték a tárgyalásokat néhány élő közvetítést lehetővé tevő applikáció vizsgálatáról. Az Apple korábban megerősítette, hogy a kínai hatóságok kérésére eltávolítja a New York Times angol és kínai nyelvű hírolvasó appjait az iTunes Store-ból. **Bővebben...**

IT biztonsági tanács

Használjunk összetett és hosszú jelszavakat, sőt inkább jelmondatokat, amelyek könnyen megjegyezhetők és lehetőleg valamilyen módosítást követően – például számok használatával magánhangzók helyett – szótárakban nem szereplő jelszósorozatot kapjunk.

Ne adjuk ki senkinek a jelszavunkat és azt, hogy milyen logika szerint választunk jelszavakat!

Amerika megsérti a „magánélethez való jogot"

(www.infosecurity-magazine.com)

Több emberjogi szervezet intézett felhívást a Belbiztonági Minisztériumhoz (DHS), azt követelve, hogy ne írják elő az Államokba érkező külföldiek számára a kényszerű adatszolgáltatást, amely szerintük súlyosan sértené az emberi jogokat. A Trump adminisztráció néhány héttel korábban nyilvánosságra hozott tervezete szerint ugyanis a határátlépőknek kötelezően fel kellene fedniük közösségi oldalaikon használt jelszavaikat, mobil kapcsolataikat is egyéb privát adataikat. **Bővebben...**

Elfogták a Kelihos botnet működtetőjét

(www.reuters.com)

Spanyol nyaralása közben letartóztatták a 2010 óta működő Kelihos botnet orosz működtetőjét, Peter Yuryevich Levashovot. A Kelihos-t évekig levélszemét küldésére használták, valamint jelszólopások, rosszindulatú kódok és zsarolóprogramok terjesztésére. A botnet viszonylag kiterjedtnek számított, időnként meghaladta a 100,000 egyidejűleg fertőzött eszközt is. Levashov – pontosabban online aliasa 'Peter Severa' – a Spamhaus ismert spammerek Top10-es listáján évekig szerepelt. **Bővebben...**

A kiberbűnözés felé vezető út

(www.nationalcrimeagency.gov.uk)

A fiatal hacker-ek legfőbb motivációja nem a pénz, hanem a hírnév, állapította meg az NCA (Nacional Crime Agency) egyik jelentésében. Jamie Graves, a ZoneFox vezérigazgatójának elmondása alapján, ki kell alakítani egy olyan megoldást, mely a fiatal hackereket nem elnyomja és üldözi, hanem felkutatja, és tudásukat a kiberbiztonság javára fordítja a magán- és a közszférában egyaránt. **Bővebben...**

Dánia szerint Oroszországhoz köthető egyes kormányzati e-mail fiókok kompromittálódása

(www.nytimes.com)

A dán kormány kibervédelmi központjának új jelentése szerint 2015-ben és 2016-ban hackerek kompromittálták a Védelmi Minisztérium és a Külügyminisztérium e-mail fiókjait. Bár a jelentésben szó szerint nem nevezték meg Oroszországot, Claus Hjort Frederiksen védelmi miniszter megosztotta észrevételeit Moszkvában, valamint a jelentésben APT 28-ként hivatkoztak a hacker ügynökre. Oroszország tagadja érintettségét. **Bővebben...**

Az "árnyék IT" kezelése négy lépésben

(blogs.microsoft.com)

Árnyék IT alatt értjük a vállalati infrastruktúrákon, az IT részleg tudta és jóváhagyása nélkül használt szoftverek és hardverek összességét. A Microsoft négy fő lépést fogalmazott meg, amelyek jelentősen hozzájárulhatnak a biztonsági szint növeléséhez. Ezek között olyan tanácsok találhatók, mint például a felhő-alapú szolgáltatások használatának részletes felmérése, vagy a valós felhasználói aktivitásra szabott, specifikus házirendek alkalmazása. **Bővebben...**