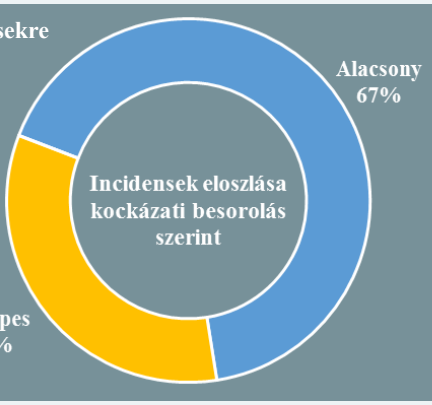
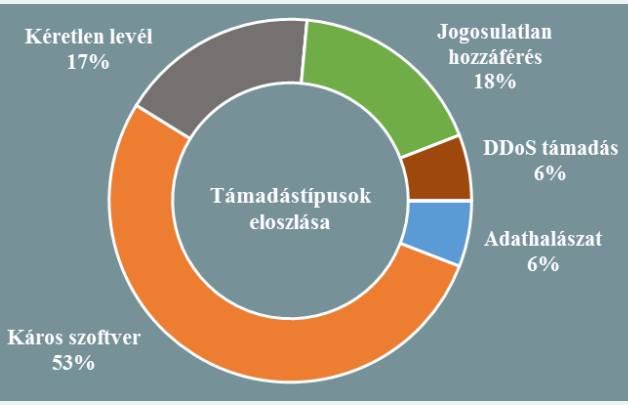
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.08.24. - 2018.08.30.





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

Jelszó-feketelisták alkalmazását javasolta a NIST, már több megoldás is elérhető a piacon

(www.helpnetsecurity.com)

Bár a biztonsági szakemberek reményei szerint az újfajta, erősebb azonosítási módszerek lassanként kiszorítják a jelszavak használatát, jelenleg mégis ez az uralkodó módszer, ami azonban több problémával is küzd. Nyílt titok, hogy a felhasználók ─ egy új felmérés szerint például az amerikai dolgozók negyede ─ többnyire könnyen kitalálható karaktersorozatokat választanak, és előszeretettel használják ugyanazt a jelszót munkahelyi és magán fiókokhoz egyaránt. Az amerikai szabványügyi hivatal (NIST) a digitális azonosításra vonatkozó irányelveinek frissítésével most egy új jó gyakorlatot igyekszik meghonosítani, miszerint javasolja, hogy minden autentikációt megvalósító alkalmazás végezzen biztonsági ellenőrzést egy gyakran használt, könnyen kitalálható, és már kompromittálódott jelszavakat tartalmazó lista felhasználásával, azonban ilyen feketelista létrehozását nem vállalta. **Bővebben...**

Tömeges adatszivárgás az Air Canadánál

(nakedsecurity.sophos.com)

Kanada legnagyobb légitársasága a mobil applikációját használó összes ─ mintegy 1,7 millió ─ ügyfelénél platformtól függetlenül jelszócserét kényszerít ki, miután a cég a héten közölte, augusztus 22. és 24. között több fiók esetében „szokatlan bejelentkezési tevékenységet” detektáltak. A közlemény szerint nagyjából 20 000 felhasználót érintett közvetlenül az incidens, esetükben feltehetőleg több személyes adat, köztük útlevél információk is kompromittálódhattak. A légitársaság szerint kicsi az esély a kanadai útlevelekkel való visszaélésre, amennyiben az okmány tulajdonosa birtokolja az eredeti példányt, és egyéb személyazonosításra alkalmas igazolványokat. **Bővebben...**

Kutatók okostelefonokról nyertek ki RSA kulcsokat

(www.bleepingcomputer.com)

A Usenix biztonsági konferencián egyetemi kutatók egy olyan új eljárást mutattak be, amelynek segítségével fizikai hozzáférés nélkül képesek voltak okostelefonokról titkosító kulcsokat kinyerni. A módszer alapjául az elektromágneses kisugárzás érzékelése szolgál, amely nem új technika, hiszen a 90-es évek óta jól dokumentált, ám a témával foglalkozó szakemberek az utóbbi évek tesztjei során csak komoly időigénnyel, és csak közvetlenül az adott eszköz chipjén mérve voltak képesek megszerezni az információt. A Georgia State University kutatói ezzel szemben 20 cm távolságból, mindössze néhány másodperc alatt 95.7, valamint 99%-os pontossággal meg tudták határozni a titkosító kulcsokat, amihez elég volt egy gyors mintát venniük a kikulcsolási műveletről. **Bővebben...**

Az EU szerint még mindig sok az illegális tartalom a közösségi oldalakon, jön a törvényi szigor

(http://www.euronews.com)

Julian King, a biztonsági unióért felelős EU-biztos a Financial Timesnak elárulta, az Európai Bizottság szerint az illegális tartalmak eltávolítására 2016-ban bevezetett „önszabályozó” program nem volt működőképes, ezért a Bizottság úgy döntött, beváltja fenyegetését, és jogszabályban rögzíti az elvárást. Érzékenyen érintheti ez a közösségi platformokat, mivel az eddigi 24 órás türelmi időt az előzetes hírek szerint 1 órára fogják csökkenteni. A törvényjavaslat véglegesítése azonban még zajlik, a részleteket pedig csak szeptemberben hozzák nyilvánosságra. **Bővebben...**

Wi-Fi adatokat szivárogtat az Android

(www.bleepingcomputer.com)

A Nightwatch Cybersecurity kutatói komoly biztonsági rést fedeztek fel az Android jogosultsági rendszerén, miszerint a telepített appok a felhasználó tudta nélkül szenzitív hálózati adatokhoz férhetnek hozzá. Az adatszivárgás speciális belső rendszerüzeneteknek (Intentek) köszönhető, amelyeket minden androidos alkalmazás és rendszer folyamat képes olvasni. Ezek két típusa – mint kiderült – olyan információkat tesz elérhetővé, mint a Wi-Fi hálózat neve, a BSSID, az eszköz lokális IP címe, DNS szerver információk, illetve – Android 6.0-nál korábbi verzió esetében – az eszköz MAC címe. Egy, a valós életben is alkalmazható támadási szcenárió szerint a támadó, miután rábírta a célszemélyt egy megfelelően konfigurált applikáció telepítésére, a kiolvasott BSSID birtokában az áldozat helyzetére vonatkozó információkhoz juthat hozzá, olyan publikus adatbázisok segítségével, mint például a Skyhook, vagy a WiGLE. **Bővebben...**

IT biztonsági Tanács

Fiatalkorú gyermek szülőjeként tájékozódjunk az őket célzó főbb internetes veszélyforrásokról és jogsértő tevékenységekről – mint például a drogfogyasztásra való csábítás, zaklatás, rasszista és erőszakos cselekedetre uszítás – majd teremtsünk alkalmat arra, hogy mindezt átbeszéljük a gyermekkel.

További információk és a káros tartalmakról bejelentési lehetőség a Nemzeti Média– és Hírközlési Hatóság nemrég frissített **Internet hotline oldalán** érhető el.

Új biztonsági funkciókat vezet be az Instagram

(instagram-press.com)

A legfontosabb újítás, hogy a képmegosztó platform immár támogatja a harmadik féltől származó autentikátor applikációk használatát a kétfaktoros azonosításhoz, mivel eddig csupán SMS-en keresztül volt erre lehetőség. Emellett azonban két további fontos funkció is bevezetésre került a célból, hogy a felhasználók nagyobb rálátást kapjanak a követett Instagram fiókokra. Az egyik a fiókok verifikálása, ami azok valódiságát, és az irányelvekkel összhangban történő használatát hivatott igazolni, valamint az „Account Info”, amely felfedi, hogy egy adott profil mikor készült, melyik országból használják, az utóbbi egy évben történt esetleges felhasználónév váltásokat, a megosztott reklámokat, illetve a legtöbb közös követővel rendelkező hasonló fiókokat. A bejelentés két héttel azt követően történt, hogy Instagram fiókok tömeges feltöréséről érkeztek hírek. **Bővebben...**

NATO tanulmány a dezinformációs kampányok működéséről

(www.stratcomcoe.org)

Egy, a NATO által dezinformációs kampányokról készített tanulmány a káros narratívák kiinduló pontjaként a blogokat jelöli meg, és azt vizsgálja, hogy az itt megjelenő álhírek milyen módon kerülnek felhasználásra a közösségi platformokon – elsősorban a Twitteren és a Facebookon – keresztül. A szerzők több százezer, 1993 és 2017 között született blogbejegyzés elemzésével képesek voltak azonosítani a dezinformációs blogok tipikus jellegzetességeit, és ezek alapján javaslatokat fogalmaztak meg a detektálásukhoz. Bemutatták, hogy a tartalmak hogyan követhetőek nyomon mémeken, hashtageken és URL-eken keresztül, a vizsgálatok során ráadásul egy Balti államokat célzó konkrét kampányt is felfedeztek. A tapasztalatok hozzájárulhatnak a propaganda kampányok elleni hatékony intézkedések kidolgozásához. **Bővebben...**

Lassú a CVE számkiosztás, most már azt is lehet tudni miért

(www.bleepingcomputer.com)

Az amerikai kormányzat javítani szeretné a sérülékenységek azonosítására és visszakereshetőségének biztosítására szolgáló, biztonsági szakemberek, cégek és szoftverek által világszerte használt Common Vulnerabilities and Exposures (CVE) rendszert, mivel az utóbbi években egyre több visszajelzés érkezett azzal kapcsolatban, hogy túl hosszú idő telik el, amíg a jelentett biztonsági hibák megkapják a CVE azonosítójukat. Még súlyosabb képet fest egy 2016-os jelentés, mely szerint 2015-ben 6 000 felfedezett sérülékenység egyáltalán nem kapott azonosítót. Mindez odáig vezetett, hogy szakemberek egy csoportja idő közben létrehozott egy alternatív sérülékenység nyilvántartó adatbázist, amely a Distributed Weakness Filing (DWF) névre hallgat. **Bővebben...**

Nemzeti LoRaWAN hálózatot épít Skócia

(www.ukauthority.com)

A skót kormányzat 6 millió fontos beruházást irányozott elő egy IoT eszközök számára készülő, nagy hatótávolságú, szélessávú hálózat (LoRaWAN) kiépítésére. Az „IoT Scotland” nevű hálózat 3G, 4G és Wi-Fi független kommunikációt tesz majd lehetővé, és a tervek szerint mind a köz-, mind a magánszektor igényeit kiszolgálja majd. A Centre for Sensors and Imaging Systems (CENSIS) innovációs intézet vezérigazgatója, Ian Reid szerint az ilyen alacsony energiaigényű szélessávú hálózatok a közeljövőben alapvető szerepet fognak betölteni az IoT berendezések számára. **Bővebben...**