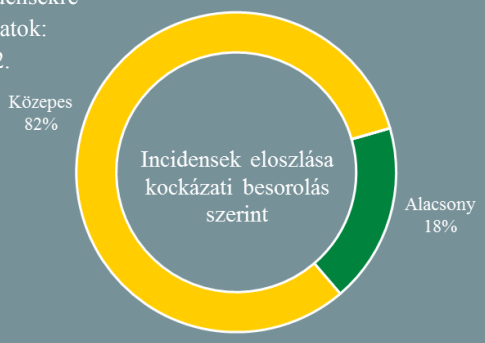
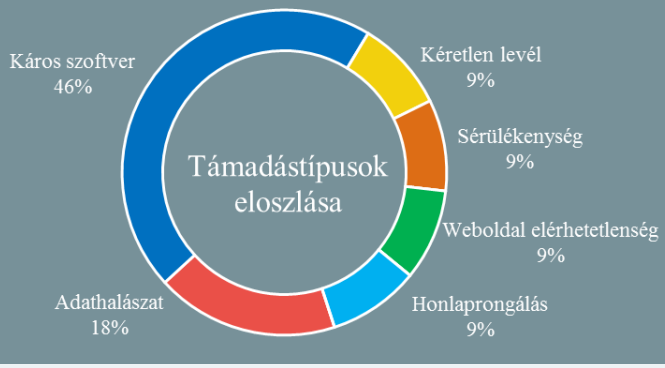
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.09.06. - 2019.09.12.





Kövessen minket megújult weboldalunkon, ahol friss IT-biztonsági hírek kerülnek publikálásra!

Ezekre fókuszál majd az NSA új kiberbiztonsági igazgatósága

(csoonline.com)

Anne Neuberger lesz a vezetője az NSA október elsején megalakuló új, kiberbiztonsági igazgatóságának, amelynek feladata, hogy az ügynökség hírszerző tevékenységét és kiberműveleteit összehangolja. Neuberger közölte: az új divízió az állami támogatású ─ ezen belül is elsősorban a Kína, Észak-Korea, valamint Oroszország és Irán által jelentett ─ kiberfenyegetések mellett a zsarolóvírusok elleni védelemre különösen nagy hangsúlyt kíván helyezni. Az utóbbi időszakban ugyanis egy új trend látszik kirajzolódni: a ransomware-ek célpontjai egyre kevésbé az egyes személyek, hanem sokkal inkább a szervezetek, ami a közelgő választásokra nézve is jelentős kockázatot vetít elő. Egy másik kiemelt terület az internetes hálózatok, ezen belül pedig a globális DNS rendszer védelmének erősítése, e tekintetben olyan kezdeményezést tart követendőnek, mint a brit kibervédelmi központ NCSC-féle Protective DNS (PDNS).

Lekapcsolták az egyik legnagyobb orosz nyelvű hacker site-ot

(securityaffairs.co)

Fehéroroszország belügyminisztériuma bejelentette, hogy az ország rendőrsége sikeresen lekapcsolta az XakFort, az egyik legnagyobb orosz nyelvű, a kiberbűnözők körében igen népszerű hacker fórumot. A 2012-óta aktív site ─ ellentétben a hasonló oldalakkal ─ nem olyan anonimizált hálózaton került megosztásra, mint a Tor, vagy az I2P. A lekapcsoláskor 28 000 regisztrált fiókkal rendelkezett, a tagok többsége kezdő hacker volt. A portálon elsősorban nem kifejezetten szofisztikált malware-eket lehetett beszerezni, amelyek sok esetben maguk is backdoort tartalmaztak.

Oroszország törvénysértéssel vádolja a Facebookot és a Google-t

(engadget.com)

Oroszország a szeptember 8-i regionális választások napjára, illetve az azt megelőző időszakra tilalmat vezetett be az online politikai hirdetésekre vonatkozóan, a Roskomnadzor szerint azonban a Facebook, valamint a Google ebben az időszakban is engedélyezték platformjaikon a politikai hirdetések megjelenését. Az orosz médiafelügyeleti hatóság arra figyelmeztet, hogy mindezt az ország nemzeti szuverenitásának megsértéseként is értékelhetik, ugyanakkor válaszlépéseket – eddig – nem hoztak. Az érintett vállalatok közül a Google már korábban beleegyezett a hirdetések eltávolításába.

Több százezer GPS nyomkövető rendkívül könnyen válhat hackelés áldozatává

(securityaffairs.co)

Az Avast arra figyelmeztet, hogy legalább 600 000, kínai gyártmányú GPS nyomkövető érhető el a neten, amelynek az alapértelmezett jelszava „123456”. Az Avast vizsgálata a kínai Shenzhen i365-Tech által gyártott T8 Mini GPS trackerre fókuszált, azonban kiderült, hogy a gyártó 29 különböző nyomkövető modellje közül több csak a termék nevében különbözött. A legjelentősebb felfedezett hiányosság, hogy az eszköz webes admin fiókjának felhasználóneve az IMEI számból eredt, ami az összes eszköz esetében kitalálható, mindez pedig az alapértelmezett jelszóval együtt jelentős kitettséget jelent. Az Avast jelentésében részletezett eszközök tulajdonosainak tehát mindenképp javasolt megváltoztatniuk a webes fiókhoz tartozó jelszót.

Újabb kémprogram bukkant fel a Play Store-ban

(securityaffairs.co)

A Google biztonsági szakértői 24 alkalmazást távolítottak el a Play Store alkalmazásboltból, mivel azok a Joker nevű kémprogrammal fertőződhettek meg. A kémprogram lehetővé teszi az SMS üzenetek, a névjegyzék és az eszközinformációk ellopását, így a támadók különböző prémium szolgáltatásokra jelentkezhetnek az áldozatok nevében. A káros kódot felfedező Aleksejs Kuprins elemzésében 24 érintett alkalmazásról számolt be, amelyeket mintegy 472 000 felhasználó telepített eszközére, 37 különböző országban. A fertőzött alkalmazások telepítését követően az alkalmazás logója jelenik meg, miközben a háttérben különböző inicializálási folyamatok kerülnek végrehajtásra. A szakértők felhívják a felhasználók figyelmét arra, hogy minden esetben javasolt felülvizsgálni a telepíteni kívánt alkalmazások által kért hozzáférési engedélyeket.

IT biztonsági Tanács

Az Internet egyik alapvető fontosságú technológiája, a DNS (Domain Name System) rendszer komoly biztonsági hiányosságokkal küzd. Az NBSZ NKI weboldalán röviden bemutatásra kerül egy régebbi (DNSSEC) és két aktuális kezdeményezés (DNS-over-HTTPS, DNS-over-TLS), főbb jellemzői, elsősorban biztonsági és adatvédelmi szempontból. Ezek előnyeinek és hátrányainak megismerése kiemelten fontos egyes technológiai nagyvállalatok törekvéseinek (lásd a Mozilla, valamint a Google ehhez kapcsolódó közleményeit) átfogó értelmezéséhez és a lehetséges kockázatok felméréséhez.

Adatvédelmi hibát fedeztek fel a Telegram alkalmazásban

(securityaffairs.co)

Újabb biztonsági hibát fedeztek fel az üzenetküldő alkalmazás működésében, ezúttal a képek törlése kapcsán. A Telegram lehetővé teszi felhasználói számára a tévesen, vagy véletlenül elküldött képek törlését a címzettek eszközeiről, azonban Dhiraj Mishra biztonsági szakértő felfedezte, hogy a képek, bár a chat felületről eltávolításra kerülnek, a címzettek belső tárhelyén továbbra is elérhetőek maradnak. A szakértő az alkalmazás Androidra kiadott legújabb verzióján (5.10.0 (1684)) végezte el vizsgálatát, azonban feltételezi, hogy a Telegram iOS-re és Windows-ra kiadott verzióiban is fennáll a hiba. Dhiraj a probléma javításáig alternatív megoldásként az „új titkos csevegés” funkció használatát javasolja, ekkor ugyanis a csevegés során az eszközökön nem kerülnek tárolásra hasonló adatok.

Nem patchelt tűzfal okozott incidenst egy amerikai energiaszolgáltatónál

(darkreading.com)

2019. március 5-én incidens történt egy amerikai villamosenergia szolgáltató cég egy vezérlő központjában, amelynek hátterében a North American Electric Reliability Corporation (NERC) jelentése szerint egy tűzfal hiba állt. A támadók ezt a sérülékenységet használták fel arra, hogy a szervezet határvédelmi eszközeinek folyamatos újraindításával szolgáltatás megtagadásos kondíciót (DoS) teremtsenek. A támadás 10 órán keresztül zajlott és habár az okozott kiesések nem tartottak tovább 5 percnél ─ és az erőmű működésében sem okoztak fennakadást ─ ahhoz elegendőnek bizonyultak, hogy az amerikai energiaügyi minisztérium segítségét kelljen kérni. Az incidens kivizsgálása feltárta, hogy a szervezet elmulasztott telepíteni egy fontos firmware frissítést, a támadás pedig csak a patch telepítése után szűnt meg.

FireEye jelentés a főbb kiberbiztonsági trendekről

(fireeye.com)

A FireEye közreadta a 2018-as év főbb kiberbiztonsági tendenciáit összefoglaló jelentését. Értékelésük szerint a globális trendeket tekintve a megelőző év(ek) hez képest nem történt jelentős változás, mindazonáltal megfigyelhető, hogy a kormányzatok a kibertámadások kapcsán egyre gyakrabban vádolnak más nemzeteket nyilvánosan. Pozitív változás, hogy a fenyegetések detektálásáig eltelt idő jelentősen lerövidült, tavaly átlagosan 78 nap telt el egy káros tevékenység felfedezésig, ami a korábbi 101 naphoz képest komoly előrelépés. **Bővebben...**

A kibertámadások többsége az emberi interakcióra támaszkodik

(helpnetsecurity.com)

A kibertámadások több mint 99%-a a felhasználókat célozza az informatikai rendszerek és infrastruktúrák helyett, derült ki a Proofpoint biztonsági vállalat által végzett kutatásból. Kevin Epstein a vállalat alelnöke szerint mindez annak köszönhető, hogy a felhasználók ellen irányuló támadási módszerek jóval egyszerűbben és alacsonyabb költséggel kivitelezhetőek, mint az informatikai rendszerekkel szembeni kifinomult kihasználási módok kifejlesztése. A jelentés megállapításai között szerepel az is, hogy a felhasználókat leggyakrabban beágyazott makrókkal, fájlok és dokumentumok megnyitásával, valamint linkekre történő kattintással tévesztik meg, leginkább a Windows termékek sérülékenységeit kihasználva. **Bővebben...**