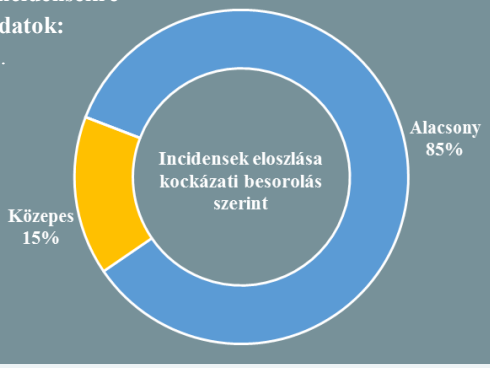
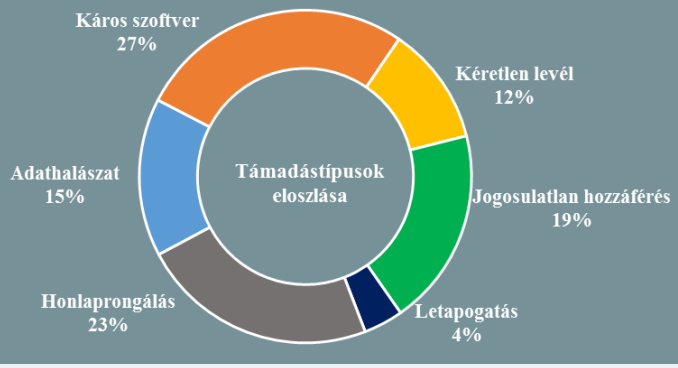
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.08.10. - 2018.08.16.





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

Ausztrália komoly lépést tett a titkosítás megkerülésének ügyében

(www.techradar.com)

Az ausztrál kormányzat 2017 júliusában már kinyilvánította, hogy olyan jogszabályt kíván létrehozni, amely a vállalatokat arra kényszerítené, hogy a végponti tikosítást feloldják, most pedig már a részletek is napvilágot láttak. Habár az ausztrál vállalkozások ez idáig is szolgáltattak felhasználói adatokat a helyi hatóságoknak egyes, magas szinten szervezett bűnözéssel kapcsolatos nyomozások során, azonban a nagy tech cégek, mint az Apple, vagy a Google már nem voltak ilyen együttműködőek. A most tárgyalt jogszabály (Assistance and Access Bill) azonban minden olyan cég esetében előírhat bizonyos fokú együttműködési kötelezettséget, amelyik Ausztrálián belül végzi a tevékenységét, vagy szolgáltatásai elérhetőek az országban. A jelenleg még csak egy vitaanyagban elérhető információk szerint ennek részeként egyes magas rangú biztonsági tisztségviselőknek lehetőséget kell biztosítani a titkosított kommunikációhoz való hozzáféréshez is. Ugyan a törvényjavaslat szerint az érintett digitális szolgáltatók nem kötelezhetők arra, hogy ehhez rendszerszintű sérülékenységet alkalmazzanak, jelenleg tisztázatlan, hogy a cégek milyen „hátsó ajtókat” (backdoors) nélkülöző megoldással felelhetnének meg a követelménynek. **Bővebben...**

A Crowdfense felpörgetné a „legális exploit piacot”

(www.motherboard.vice.com)

A dubai székhelyű Crowdfense vállalat ─ amely nulladik napi sérülékenységeket kihasználó kódok (exploitok) felvásárlásával, majd kormányzatok részére történő továbbértékesítésével foglalkozik ─ most elindítja webes portálját (Vulnerability Research Platform), amin keresztül a biztonsági szakemberek és kutatók egyszerűen és kényelmesen adhatják el az általuk fejlesztett exploitokat. A portál anonim feltöltést biztosít, végponttól végpontig tartó titkosítást alkalmaz üzenetküldéskor, valamint a feltöltők figyelemmel kísérhetik az általuk beküldött sérülékenységek feldolgozottsági állapotát is. A vállalat vezetője, Andrea Zapparoli Manzoni, a Black Hat 2018 konferencián adott nyilatkozata szerint a cég olyan exploitokat is vár, amelyek önmagukban nem elegendőek egy eszköz kompromittálásához, így reményeik szerint azokat a szakembereket is elérhetik, akik eddig nem jelentek meg a piacon. **Bővebben...**

Rendkívül sérülékenyek a műholdrendszerek

(www.securityweek.com)

Ruben Santamarta, folytatva egy 2014-es, műholdas infokommunikációs rendszerek ellen potenciálisan végrehajtható támadásokat felmérő kutatását, újabb sérülékenységeket fedezett fel, amelyekről a Black Hat 2018 konferencián számolt be. A sérülékeny satcom rendszerek között légügyi, tengerészeti és katonai rendszerek is megtalálhatóak, a vizsgálatok során pedig többek között nem biztonságos protokollokat, backdoorokat, elégtelen konfigurációkat tárt fel, amelyek közül olyan is akadt, ami a támadók számára lehetőséget biztosít arra, hogy az érintett eszközök felett teljes kontrollt nyerjenek. Mindemellett a tengerészeti és katonai szektorok tekintetében jelentős károkozással járó fenyegetéseket azonosított: a támadók felfedhetik harcászati egységek pontos helyzetét, zavart kelthetnek a fedélzeti kommunikációkban, vagy akár az ún. „nagy intenzitású elektromágneses tér” (HIRF) technológia felhasználásával fizikai károkat okozó támadásokat is végrehajthatnak. **Bővebben...**

Újabb támadási módszer fenyegeti az Android felhasználókat

(www.bleepingcomputer.com)

Man-in-the-Disk (MitD) névre keresztelték a Check Point kutató csapata által felfedezett új támadási módszert, amely során a támadók a káros kódokat a külső tárhelyre juttatva fertőzik meg az ott található alkalmazásokat, és lehetetlenítik el azok működését. A mobilkészülékek véges belső memóriakapacitása okán, egyes Androidos alkalmazások esetén lehetőség van az applikációk külső tárhelyen történő telepítésére. A kutatók a tesztek során egy káros kódokat tartalmazó zseblámpa alkalmazást hoztak létre, amely engedélyt kért az adatok külső tárhelyen történő tárolására, majd ezt kihasználva további, a külső tárolón található alkalmazásfájlok felcserélésével összeomlottak az applikációk. A MitD támadás alkalmas lehet a versenytársak alkalmazásainak működésképtelenné tételéhez, de hátsó ajtók (backdoors) is biztosíthatóak további káros kódok rendszerbe történő bejuttatásához, másrészt a frissítésnek álcázott műveletek során az appok lecserélhetők rosszindulatú változataikra. **Bővebben...**

IT biztonsági Tanács

A NOVA Labs ingyenes digitális platformja különböző interaktív játékokat, kvízeket és videókat tesz elérhetővé többek között **informatikai biztonsági** témakörben is.

A Cybersecurity Lab oldalon a játékosnak egy vállalkozás informatikai üzemeltetőjének szerepében, több „kihíváson” keresztül kell megvédenie a céget a támadásoktól, miközben játékos módon olyan témakörökkel kerül kapcsolatba, mint a vírus- és pszichológiai manipulációs támadások, kódolás és jelszótörés.

Az angol nyelvű oktató játék a szórakoztatás mellett hozzájárul a felhasználók biztonságtudatosságának növeléséhez.

Faxon keresztül is támadhatók a szervezetek

(www.hackread.com)

A CheckPont által végzett „Faxploit” elnevezésű kutatás eredményei szerint a faxkészülékek és az all-in-one nyomtatók által használt protokollok sebezhetőségeit kihasználva, a támadók a faxszám birtokában és a telefonvonal használatával képesek lehetnek hozzáférést szerezni a szervezeti hálózatokhoz. A támadás során egy káros programokat tartalmazó, speciálisan létrehozott képfájlt küldenek a célkeresztben lévő faxkészülékre, ami dekódolja a fájt, majd ezt követően betölti a memóriába, így a káros kódok tovább terjeszthetőek a hálózatban. A tesztelést egy HP Officejet Pro 6830 all-in-one nyomtatón végezték el, de a feltárt sebezhetőség nem adott eszközhöz, hanem az eszközök által használt protokollokhoz köthető, így a sérülékenységben számos hasonló készülék és online faxszolgáltatás is érintett lehet. **Bővebben...**

Egyszerű, de hatékony adathalász támadás kerüli meg az Office 365 védelmét

(www.securityaffairs.co)

Az Avanan felhőbiztonsági cég egy új masszív adathalász támadási kampányt azonosított az utóbbi két hétben (PhishPoint), ami képes megkerülni a Microsoft Office 365 által bevezetett Advanced Threat Protection (ATP) védelmi mechanizmust. A támadás során az áldozatok egy SharePoint dokumentumra mutató hivatkozást tartalmazó e-mail üzenetet kapnak, ami a linkre való kattintás után több lépésben tovább irányítja őket előbb egy OneDrive fájlra, majd azon keresztül a hamis Office 365 bejelentkezési felületre. A módszer azért működőképes, mert a Microsoft védelme nem képes végigkövetni a hivatkozási láncot, csak az első szintet ellenőrzi, ami ebben az esetben csupán egy SharePoint dokumentum szabványos meghívása. A technika egyszerű, ám az ellene való védekezés több problémát is felvet, ugyanis még ha a rendszer vizsgálná is a dokumentumok tartalmát, találat esetén azzal a dilemmával szembesülne, hogy vagy az összes SharePoint-os fájlt kitiltja ─ ezzel a legitimeket is ─ vagy csak a káros oldal URL-jét teszi tiltólistára, ami azonban csak ideig-óráig jelent védelmet, hiszen a támadók könnyen létrehozhatnak egy újat. A szakértők fokozott óvatosságot javasolnak az olyan sürgető hangnemű e-mailek esetében, amelyek hiperhivatkozást tartalmaznak, valamint javasolják a kétfaktoros hitelesítés alkalmazását, és a bejelentkezési oldalak webcímének ellenőrzését. **Bővebben...**

Indiai bank a hackerek célkeresztjében

(www.bleepingcomputer.com)

Hackertámadás érte India második legnagyobb szövetkezeti bankját (Cosmos Bank), amelynek során 13,5 millió dollárnak megfelelő rúpiát tulajdonítottak el. Bár az incidens kivizsgálása még folyamatban van, a bank képviselői elárulták, hogy a támadást három hullámban hajtották végre. Az első szakaszban 11 millió dollár értékű ATM átutalás történt a VISA, két órával később 400 000 dollárnyi a Rupay, végül 2 millió dollár értékű a SWIFT rendszeren keresztül, összesen közel 30 000 tranzakció során. A bank közleménye szerint az ügyfelek számláit elvileg nem érintette az incidens, a hiány pótlásáról pedig ─ a nemzetközi banki szabványoknak megfelelően ─ a bank gondoskodni fog. A nyomozás jelen állása szerint a támadás Kanadából érkezett, ám vélhetően ez csak egy köztes lépcsőfok volt, amivel a valódi forrást kívánták elrejteni. **Bővebben...**

Amerika a jövőben nagyobb hangsúlyt fektet a KKV-k kibervédelmére

(www.infosecurity-magazine.com)

Az amerikai kisvállalatok hamarosan komoly segítséget kapnak a Nemzeti Szabványügyi és Technológiai Intézet (NIST) által kiadott kiberbiztonsági keretrendszerek és ajánlások implementálásához, miután Donald Trump amerikai elnök augusztus 15-én elfogadta az erre vonatkozó törvényjavaslatot (NIST Small Business Cybersecurity Act). **Bővebben...**