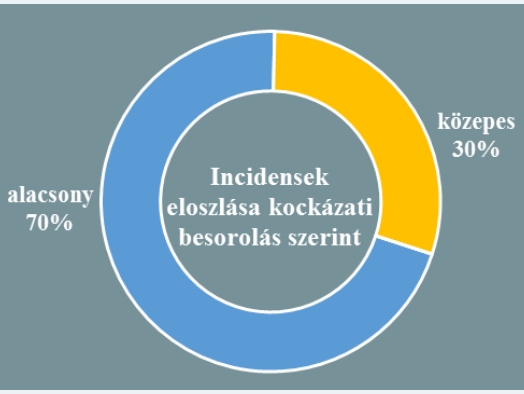
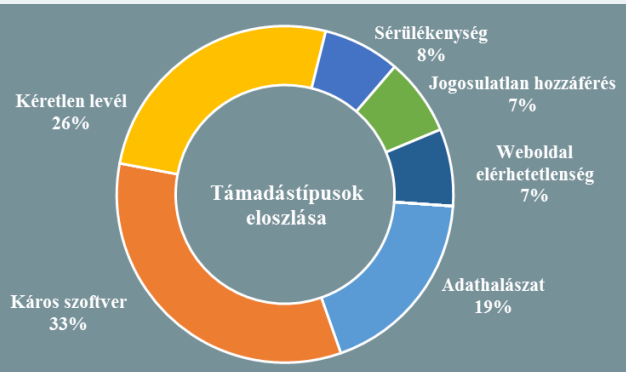
Incidens adatok:
2018.02.16. - 2018.02.22.





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

Az amerikai hatóságok nemsokára még több személyes adathoz férhetnek hozzá

(www.theregister.co.uk)

35 amerikai államügyész írt alá egy nyílt levelet a Clarify Lawful Overseas Use of Data (CLOUD) törvényjavaslat elfogadásának sürgetéséről. Ily módon lehetővé válik a szövetségi hatóságok számára, hogy egy bírói határozat birtokában hozzáférhessenek az állampolgárok tengerentúli szervereken tárolt e-mailjeihez és egyéb személyes kommunikációjához. Mindez a gyakorlatban azt jelenti, hogy az FBI jogi felhatalmazást kérhet például egy kaliforniai bíróságtól, hogy megszerezhessen egy fájlt egy olyan San Franciscó-i szerverről, mely fizikálisan Franciaországban van, ezzel megkerülve a francia adatvédelmi törvényeket és jogrendszert. Emellett egy adatmegosztási megállapodás értelmében a törvényjavaslat a külföldi kormányok számára is lehetővé tenné, hogy azok az Államokban tartózkodó, nem-amerikai állampolgárokról információt kérjenek. Emberi és internetes jogokkal foglalkozó csoportok határozottan ellenzik a jogszabály elfogadását, arra hivatkozva, hogy ezzel az Egyesült Államok a világ minden táján megkönnyíti az állampolgárok utáni kémkedést. Maguk az államügyészek is úgy vélték, hogy a törvény túl nagy hatalmat biztosít a kormányok számára, ezért az utolsó bekezdésben megjegyzést tettek, miszerint az új jogszabály nem befolyásolhatja negatívan az elektronikus távközlési adatvédelmi törvény azon folyamatban lévő módosításait, melyek a fogyasztók védelmét erősítik. **Bővebben...**

A brit önkormányzatokat percenként 37 kibertámadás éri

(www.theregister.co.uk)

A Big Brother Watch (BBW) az elmúlt öt évben Nagy-Britannia helyi önkormányzatait ért internetes támadások elemzéséről adott közre összefoglalót. Eszerint a válaszoló 395 önkormányzat közel harmada jelentett be legalább egy

alkalommal incidenst és mintegy 25 önkormányzat nyilatkozta, hogy az incidensek során adatszivárgás is történt. Az önkormányzatok fele azonban elismerte, hogy egyáltalán nem tesz bejelentést a bekövetkezett incidensekről. A bevallott esetek alapján a közigazgatási szektor ellen összesen körülbelül 98 millió internetes támadás történt, ami alatt a károkozást vagy a rendszerekhez, hálózatokhoz és eszközökhöz történő jogosulatlan hozzáférést értjük. A BBW arra figyelmeztet, hogy ez a szám a jövőben csak nőni fog a kormányzat adathalmozó szemlélete miatt. A személyzet biztonsági képzésével kapcsolatban is komoly hiányosságokat találtak, csak minden második önkormányzat különít el erre a célra a saját költségvetéséből. **Bővebben...**

Kína a legaktívabb a kiberkémkedés terén

(www.infosecurity-magazine.com)

A Center for Strategic and International Studies (CSIS) nonprofit szervezet és a McAfee az online biztonság és a kiberbűnözés aktuális állapotáról készített közös elemzést. A "The Economic Impact of Cybercrime – No Slowing Down" című összefoglaló szerint a kiberbűnözés ma globálisan közel 600 milliárd dolláros kárt okoz évente. A vizsgálat során kiberbűnözés kategóriába elsősorban a számítógépes hálózatokhoz anyagi előnyszerzés, szándékos károkozás vagy érzékeny adat megszerzésének érdekében történő illegális hozzáférést számították. Kiderült az is, hogy bár Oroszország és Észak-Korea számít a legveszélyesebbnek az eddig elkövetett kiberháborús cselekmények elkövetői között, mégis Kína folytatja a legtöbb kiber-kémkedési műveletet. A leggyorsabban növekedő fenyegetést a zsarolóvírusok jelentik, köszönhetően a „kiberbűnözés, mint szolgáltatás” (CaaS) üzleti modell, valamint a kriptopénz rendszerek előretörésének, melyek nagymértékben elősegítik az anonimitást. **Bővebben...**

Android a biztonság tükrében

(www.securityweek.com)

A G Data jelentése szerint az androidos kártevők számát tekintve enyhe csökkenés volt megfigyelhető tavaly a megelőző évhez képest, azonban így is több, mint 3 millió mintát azonosítottak. Ez önmagában nem feltétlenül mérvadó a biztonságot tekintve – hiszen az Android számít messze a legnépszerűbb mobil platformnak, ami a támadók számára nyilvánvaló vonzerőt jelent – amellett azonban mindenféleképpen komoly érv, hogy a Google biztonsági funkcióit kiegészítve egy vírusvédelmi szoftver is alkalmazásra kerüljön. Az összefoglaló emellett kitér arra is, hogy tavaly 841 sérülékenységet találtak androidos rendszerekben, amelyek közül a legtöbb CVSSC (Common Vulnerability Scoring System Calculator) szerinti 9-10-es (azaz kritikus) besorolású sérülékenység a Pixel/Nexus eszközöket érintette. Meg kell azonban említeni a tech óriás által bevezetett újdonságokat is, mint például a Project Treble, amelynek hála a gyártók sokkal gyorsabban képesek a biztonsági frissítéseket a készülékekre juttatni. **Bővebben...**

IT biztonsági Tanács

Okostelefonunk elvesztése vagy ellopása esetén használhatjuk a telefon megkeresése, zárolása, illetve a telefonon tárolt adatok törlése funkciókat, melyekre Android és iOS operációs rendszert futtató telefonok esetében is van lehetőség, azonban ehhez több beállítást is eszközölni kell, amelyekről a következő hivatkozásokat követve olvashatnak bővebben:

- https://support.apple.com/en-us/HT205362
- https://upport.google.com/accounts/answer/6160491

NIST tanulmány az IoT eszközök biztonságának megteremtéséhez

(www.securityweek.com)

Az amerikai szabványügyi hivatal egy új tervezetet (NISTIR 8200) adott közre, amely az IoT környezetek kiberbiztonsági aspektusait veszi számba a jövőbeli szabványok támogatásához. Ennek során például különböző funkcionális területeket határoztak meg úgy, mint: összeköttetésben álló eszközök, fogyasztói IoT, egészségügyi és orvosi eszközök, okos épületek, valamint okos gyártás, mely utóbbiba beletartoznak az ipari vezérlőrendszerek is. Úgy találták, hogy alapvetően kicsi a különbség ezek biztosítása és más típusú rendszerek között, habár a klasszikus 'CIA' követelményrendszerből (bizalmasság, sértetlenség, elérhetőség) az IoT eszközök számára az első számú szempont az elérhetőség biztosítása, hiszen például a rendszerek leállása a betegellátásban akár emberéleteket is követelhet. Drew Koenig, a Magenic biztonsági kutatója szerint a legnagyobb veszélyt az IoT eszközök limitált frissítési lehetősége jelenti, illetve kritikaként azt is kiemelte, hogy nagy problémának tartja, hogy a NIST csupán ajánlásokat fogalmaz meg, valódi szabályozó erővel nem bír. **Bővebben...**

Szigorúbb tartalomszűrést alkalmaz a Twitter

(www.techcrunch.com)

Múlt héten biztonsági közleményt jelentetett meg a Twitter, miszerint a felhasználók immár jelenthetik azokat a tweet-eket és fiókokat, amelyek öngyilkosságra vagy önsértésre biztatnak. Az új irányelv alapján ezek olyan káros tevékenységnek minősülnek, amiket a vállalat tiltani fog. A frissített házirend alapján az első szabálysértését követően átmenetileg kizárják a felhasználót fiókjából, a többször elkövetett szabályszegés pedig a fiók felfüggesztésével is járhat. Mindemellett segítséget is szeretnének nyújtani azon felhasználóinak, akik öngyilkossággal vagy önbántalmazással kapcsolatos gondolatokkal küzdenek, emiatt már korábban létrehoztak egy dedikált csoportot, akik felveszik a kapcsolatot a veszélyeztetett felhasználókkal. A Twitter súgójában létrehozott új szakaszban („Glorifying self-harm and suicide") leírás található arról, hogy mit tehet az, aki ilyen jellegű tartalommal találkozik. A kibővített intézkedések ellenére továbbra is sok kritika éri a vállalatot, egyesek szerint ugyanis a platform még mindig nem tesz eleget a káros magatartásformák kiszorításáért. **Bővebben...**

Külön szervezet az amerikai energetikai infrastruktúra kiberbiztonságáért

(www.helpnetsecurity.com)

Az Egyesült Államok kormánya egy új kiberbiztonsági szervezet (Cybersecurity, Energy Security, and Emergency Response - CESER) létrehozását tervezi az Amerikai Energiaügyi Minisztérium részeként, melynek feladata az energiaszektor védelme, azáltal, hogy lehetővé teszi a természeti, illetve a humán fenyegetésekkel szembeni koordináltabb felkészültséget és reagálási képességet. A javaslat szerint a CESER a K+F-re összpontosít majd, amely segítségül szolgálhat a kritikus rendszerek ellenálló képességének növeléséhez. Ebbe beletartoznak a kiberbiztonsági vezérlőrendszerek-, komponensek és eszközök következő generációjának fejlesztései, de célként jelenik meg a biztonsági események során feltárt idő-kritikus adatok ipari szereplők közötti megosztásának javítása is. Mivel az elmúlt évek során világszerte többször lehetett tapasztalni kritikus infrastruktúrákat ért támadásokat – mint például az ukrán energiaszektort ért Black Energy, vagy a Triton/Trisis káros kód támadások – Európában is egyre több kezdeményezés irányul a létfontosságú infrastruktúrák biztonságának javítására (lásd például NIS irányelv). **Bővebben...**