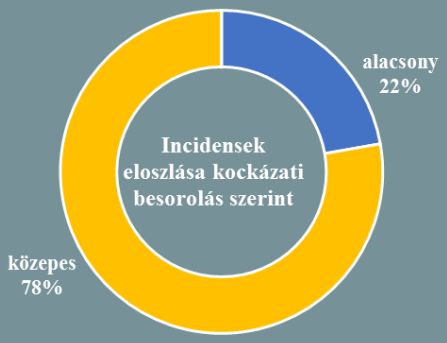
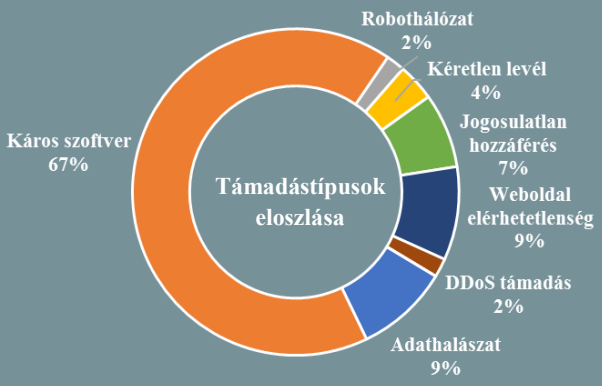
Incidens adatok: 2017.10.25. — 2017.10.31.





Az üzleti tevékenységre is pozitív hatással lehet a GDPR

(www.globalsecuritymag.com)

Az Európai Unió általános adatvédelmi rendeletének (GDPR) hatására a vállalatoknak felül kell vizsgálniuk adatkezelési gyakorlatukat és mélyreható szinten ismerniük kell a felhasználóik adattípusait. Azonban nem csak az előírások miatt fontos a megfelelés kialakítása, ugyanis a Gemalto által végzett felmérés szerint a fogyasztók 64%-a nem venne újra igénybe szolgáltatást olyan cégtől, amelytől korábban felhasználói adatok szivárogtak ki. **Bővebben...**

Vizsgálat alatt a Heathrow Airport adatszivárgása

(www.securityaffairs.co)

Egy ismeretlen személy talált rá séta közben arra az USB pendrive-ra, amely az Egyesült Királyság legnagyobb repteréről tartalmazott bizalmas dokumentumokat. A Heathrow repülőteret végül a The Sunday Mirror értesítette, miután a megtaláló eljuttatta hozzájuk az adathordozót. A nyilvánosságra hozott információk szerint legalább 174 szenzitív dokumentum volt beazonosítható, változatos tartalommal, köztük biztonsági őrjáratok ütemezései, biztonsági kamerák helye, biztonsági jelvény-típusok a zárt körletekbe való belépéshez, csatornák, térképek, VIP személyekre vonatkozó protokollok, sőt, a királynő egyéni útvonalai is. Az eset kapcsán már megkezdték a kivizsgálásokat. Egyesek a dokumentumok minősítésére használt elnevezések alapján úgy vélik, ezek már vélhetően elavult információkat tartalmaznak, noha ezek ismerete továbbra is komoly veszélyt jelenthet, hiszen következtetni lehet belőlük a jelenlegi szabályokra is. **Bővebben...**

Android és iOS felhasználókat célzó adathalász kampány

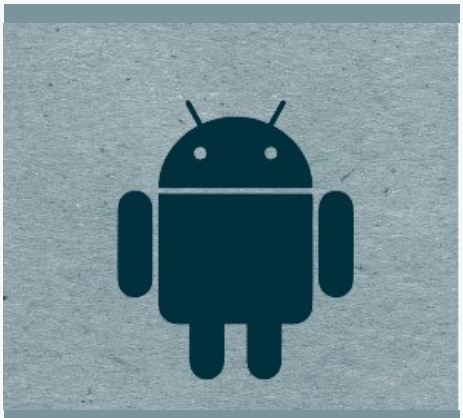
(www.bleepingcomputer.com)

Az F-secure egy, a Facebook-on terjedő adathalász kampányra hívja fel a figyelmet, ami Facebook, illetve YouTube fiókok hitelesítő adatait próbálja megszerezni. A finn biztonsági cég által azonosított kampány először Svédországban jelent meg (október 15-én) és onnan terjedt tovább, Finnországba (október 19.), majd Németországba (október 20.), majd ezt követően – igaz kisebb hatásfokkal – más országokban is megjelent. A Facebook-on posztolt vagy direkt Messenger üzenetek útján terjedő adathalász üzenetekre – amelyek egy YouTube videónak néznek ki – eddig közel 200 000-en kattintottak, legnagyobbrészt (80%) a fent említett három országból. Az F-Secure biztonsági cég javasolja a gyanús üzenetet kapott felhasználóknak, hogy módosítsák jelszavukat, beleértve azokat a rendszereket is, melyeken ugyanazt a jelszót használják. **Bővebben...**

Vietnámban tilos kriptovalutával fizetni

(www.zdnet.com)

A vietnámi állami bank múlt héten közleményt adott ki arról, hogy a kriptovaluták – beleértve a Bitcoin-t is – 2018. január elsejétől illegális fizetőeszközöknek minősülnek és a kormányzat szigorúan tiltja azok ilyen célú használatát. Amennyiben a hatóságok ilyen tranzakcióról szereznek tudomást, annak büntetőjogi következménye lehet és pénzbírságot szabhatnak ki, amelynek összege körülbelül 6-9 000 dollár között mozoghat. A szabályzás nem érinti magát a bányászatot, amíg azt nem áruvásárlásra vagy eladásra használják és a virtuális pénzek hagyományos valutára való váltása sem tiltott. **Bővebben...**



A mobilokat is használják "bányászatra"

(www.itwire.com)

A Trend Micro biztonsági cég jelentése szerint egyes, a Google Playen elérhető mobil alkalmazások kriptovaluta bányászatot folytatnak a felhasználók tudta nélkül. A vizsgált appok többféle eljárást alkalmaztak: egyesek a bányászatra használt Coinhive-os JavaScript kódokat dinamikusan töltötték be, míg mások maguk tartalmazták azokat. Utóbbira példaként említik a 'Car Wallpaper HD' alkalmazást, amelyet a Google a többi káros appal egyetemben már eltávolított az áruházából. Kérdéses, hogy ez a módszer mennyire hatékony a profittermelés szempontjából, azonban az eszközök teljesítményére gyakorolt hatása egyértelmű: lassabb működés, csökkenő akkumulátor élettartam, ezáltal gyorsabb elhasználódás. **Bővebben...**

IT biztonsági Tanács

Az online fiókjainkhoz használjunk különböző és lehetőleg minél erősebb jelszavakat. Ezek fejbentartása nehézkes lehet, ezért érdemes egy jelszókezelő szoftvert segítségül hívnunk.

A szoftver kiválasztásakor figyeljünk arra, hogy csak ismert és megbízható jelszókezelőt használjunk, a nem régóta elérhető termékekkel szemben legyünk bizalmatlanok.

Újabb haditerv lopási vádak Észak-Korea ellen

(www.bloomberg.com)

Egy jelentés szerint észak-koreai hackerek 2016 áprilisában titkosított dokumentumokat lophattak a világ legnagyobb hadihajó gyártójától, a dél-koreai Daewoo Shipbuilding and Marine Engineering-től (DSME). Az esetet nyilvánosságra hozó dél-koreai napilap (Dong-A Ilbo) szerint a mintegy 40 000 eltulajdonított dokumentum közül körülbelül 60 volt minősített. Az anyagok olyan érzékeny katonai információkat is tartalmaztak, mint rakétahordozó hadihajók és tengeralattjárók tervrajzai és egyéb műszaki specifikációi. Nem ez az első eset, hogy Észak-Koreát katonai titkok ellopásával gyanúsítják, ugyanis a hónap eleji hírek szerint észak-koreai hackerek az Egyesült Államok és Dél-Korea által közösen készített hadititkokat is megszerezhettek. **Bővebben...**

Újabb internetes korlátozás Oroszországban

(www.securityweek.com)

November elsejétől lép életbe egy új törvény Oroszországban, amely alapján a VPN szolgáltatást nyújtó cégek számára előírhatják bizonyos weboldalak blokkolását. Az intézkedés egyesek szerint elsősorban az újságírókat és ellenzéki aktivistákat érinti majd hátrányosan, amivel egyetért Eva Galperin, az amerikai digitális jogvédő szervezet, az Electronic Frontier Foundation kiberbiztonsági igazgatója is. "Még ha sikerülne is valakinek kerülő megoldást találnia, kétszer is meg fogja gondolni, hogy érdemes-e vállalnia a kockázatot." – nyilatkozta. Azon szolgáltatók, akik nem tesznek eleget az előírásoknak – amit néhányan már előre jeleztek, úgy mint a ZenMate vagy a Private Internet Access – jó eséllyel maguk is feketelistára kerülnek majd. **Bővebben...**

Tömeges megfigyelést tervezhet a holland kormány

(www.bleepingcomputer.com)

Elképzelhető, hogy a Mozilla megvonja a bizalmat egy holland állami tanúsítvány kibocsátó hatóságtól (Staat der Nederlanden Root CA), miután Hollandia megszavazott egy olyan törvényt (Wet op de inlichtingen- en veiligheidsdiensten - Wiv), amely a helyi hatóságok számára lehetővé teszi az internetes kommunikáció lehallgatását, "hamis kulcsok", azaz SSL/TLS tanúsítványok használatával. A Mozilla attól tart, hogy a holland hatóságok ezek segítségével az internetes kommunikációkba való közbeékelődéssel tömeges megfigyelést végeznének, amelyre egy SSL hibaüzenettel hívná fel a felhasználók figyelmét. Vélhetően más böngésző gyártók is hasonlóan fognak reagálni. **Bővebben...**

IoT: Biztonsági szabályozásra van szükség

(www.helpnetsecurity.com)

Nagy lenne az igény az IoT eszközök biztonságának növelésére – világít rá a Gemalto felmérése. Eszerint az egyéni felhasználók kétharmada, valamint a szervezetek közel 80%-a támogatja az elképzelést, hogy az IoT eszközök biztonságát kormányzati közreműködéssel teremtsék meg. Kiderült, a felhasználók jobban félnek attól, hogy illetéktelenek átveszik az irányítást eszközeik felett, mint az adatszivárgástól. Az IT-biztonsági ráfordításokkal kapcsolatban azt találták, hogy a gyártók és szolgáltatók még midig keveset, csupán a büdzsé 11%-át fordítják biztonságra, szerencsére azonban egyre elterjedtebb a koncepció, ami már a tervezéstől figyelembe veszi a biztonsági szempontokat (security-by-design), amit a megkérdezett cégek fele már alkalmaz. **Bővebben...**