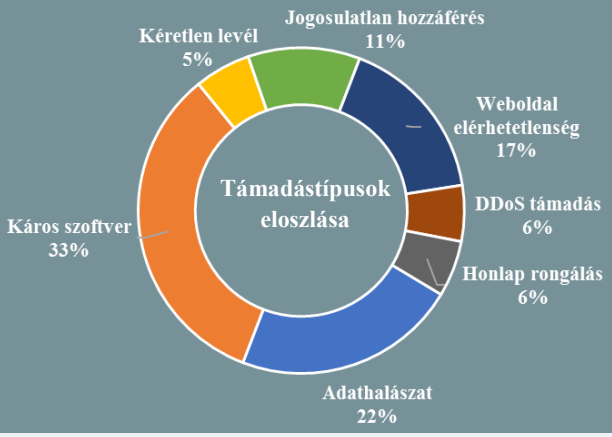
Incidens adatok: 2017.11.15. — 2017.11.21.



A Pentagon által végzett megfigyelések adatai szivárogtak ki

(www.bleepingcomputer.com)

Egy biztonsági kutató jelentette, hogy az Amerikai Védelmi Minisztériumhoz (DOD) tartozó, nyilvánosan elérhető adatokra bukkant. Az Amazon S3 szervereken tárolt adatbázisok mintegy 1,8 milliárd arab és angol nyelvű közösségi média és fórum posztot tartalmaztak, amelyekhez bármilyen – akár egy ingyenesen regisztrálható – Amazon AWS fiók birtokában hozzá lehetett férni. A felfedező, Chris Vickery szerint az esetet könnyű volt az amerikai kormányzathoz kötni, mivel az elnevezések is igazán beszédesek voltak („centcom-backup", „centcom-archive" és „pacom-archive"), amelyek alapján következtetni lehet arra, hogy a DOD mely katonai egységéhez tartozhatnak. Eszerint érintett lehet a Pentagon két katonai műveletekért felelős parancsnoksága, a Central Command (CENTCOM) és Pacific Command (PACOM). Vickery a felfedezést követően értesítette a DOD-t és röviddel ezt követően az adatbázisokat biztonságossá tették. **Bővebben...**

Új európai kiberbiztonsági kutatóintézetek

(www.euractiv.com)

Európai Uniós tagországok a héten egyeztetnek olyan új kiberbiztonsági kutatóközpontok felállításának tervéről, amelyek tevékenységében kiemelt szerepet kapnak a titkosítási technológiák. A javaslatot először idén szeptemberben terjesztették fel, a részletes tervezetet pedig 2018 derekán hozzák nyilvánosságra. Habár több európai állam részéről is komoly nyomásgyakorlás érte, az Európai Bizottság továbbra is kitart amellett, hogy nem fogja jogszabályban rögzíteni a titkosított kommunikációt megkerülő backdoor-ok telepítését. Ehelyett inkább nagyobb pénzügyi támogatásban részesítenék az Europolt a titkosítást megtörő eljárások kifejlesztésére, valamint segítenék egy olyan hálózat létrehozását, amelyen keresztül a tagállamok bűnüldöző hatóságai felvehetnék egymással a kapcsolatot és megvitathatnák az alkalmazott eljárásokat. **Bővebben...**

Lassan a boltokban is lehet kriptovalutával fizetni

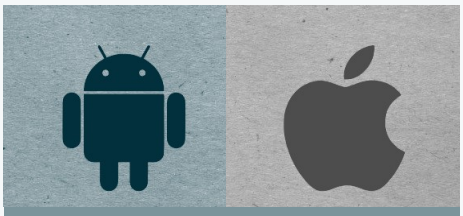
(www.bitdefender.com)

A kriptovaluta váltó London Block Exchange (LBX) a Visával együttműködve egy olyan kártyát készül kibocsátani, amely a kriptovaluta birtokosok számára lehetővé teszi, hogy a digitális pénzekkel vásárolhassanak az Egyesült Királyságban. A "Dragoncard" nevű kártyával igénybe vehető szolgáltatás az első olyan megoldás kriptopénz a vásárláskor történő átváltására, amit a brit pénzügyi szabályozó szerv (Financial Conduct Authority – FCA) engedélyezett. „Ha egy üzletben elfogadják a Visa kártyát, az mostantól azt jelenti, hogy ott a Bitcoin, az Etherum, a Litecoin vagy a Ripple is elfogadott fizetőeszköz." – foglalta össze az LBX vezérigazgatója, Benjamin Dives. A szolgáltatás nem lesz ingyenes, minden tranzakciót 0,5%-os átváltási illeték terhel, továbbá egy egyszeri díj (20 font). **Bővebben...**

Helymeghatározási adatok engedély nélküli gyűjtése

(www.thehackernews.com)

A Quartz elemzése szerint a Google 2017 januárjától az összes Android eszközről gyűjti a felhasználói készülékek helyadatait, abban az esetben is, ha a helymeghatározási szolgáltatást a felhasználó letiltotta. Mindehhez SIM kártyára sincs szükség, csupán arra, hogy a készülék csatlakozzon az internethez. Az is kiderült, hogy az androidos készülékek a környező mobil cellainformációkat is begyűjtik és ezek is továbbításra kerülnek. A Google szerint az eljárást abból a célból alkalmazták, hogy az üzenetek továbbítását meggyorsítsák, azonban a tervek szerint november végén felhagynak vele. **Bővebben...**



Egyik ágazatot sem kímélik a mobil malware-ek

(www.itwire.com)

A Check Point mobileszközöket célzó rosszindulatú támadásokról készített tanulmánya szerint – mely a 2016. július 1. és 2017. július 1. közötti időszakot öleli át – szervezetenként átlagosan 54 volt a malware támadások száma és nem csupán az Android, hanem az iOS, valamint egyéb rendszerek is érintettek voltak. Az ágazatok szerinti eloszlást vizsgálva azt találták, hogy leginkább a pénzügyi (29%) és a kormányzati szektor (26%) álltak a kiberbűnözők érdeklődésének középpontjában, ezen kívül a technológiai (18%), a telekommunikációs (8%) és a gyártási (7%) iparágak szenvedték el a legtöbb támadást. A tanulmány szerint arra lehet számítani, hogy a pénzügyi szféra marad az elsődleges célpont, emellett a támadások földrajzi eloszlása idővel kiegyenlítődik majd és minden régióban jellemző lesz a támadások számának megugrása. **Bővebben...**

IT biztonsági Tanács

Ünnepi és akciós szezon idején fokozottan figyeljünk az internetes vásárlásaink során.

Lehetőleg csak olyan cégtől vásároljunk, amelyet ismerünk és amelyben megbízunk. Számítsunk rá, hogy megszaporodhatnak a webáruházak online marketing kampányához hasonló adathalász tevékenységek is. Kerüljük az irreálisnak tűnő ajánlatokat.

Dán kibervédelmi célok

(www.reuters.com)

Dánia több erőforrást fektetne a kibertámadások elleni védekezésbe egy új stratégia szerint, amelynek részleteit jövő év folyamán hozzák nyilvánosságra. A már kiszivárgott információk szerint a kormány a korai figyelmeztető rendszerét érintően tervez bővítéseket. Claus Hjort Frederiksen, dán pénzügyminiszter a Reutersnek elmondta, hogy a meglévő rendszert bővítenék ki a stratégiai infrastruktúrával és a magán vállalkozásokkal, valamint a dán kibervédelmi központ képességeit is fejlesztenék. Azt is kiemelt célként kezelik, hogy mélyebb együttműködést építsenek ki a hatóságok és a magánszektor szereplői között, mivel a vállalatok sok esetben vonakodnak az őket ért támadásokról szóló információ megosztásától, attól tartva, hogy az negatív hatással van az üzleti tevékenységükre. **Bővebben...**

Mikor tartják vissza az információt?

(www.threatpost.com)

Az Egyesült Államok kormányzata a nagyobb átláthatóság érdekében múlt hét szerdán nyilvánosságra hozta a felfedezett sérülékenységekről szóló információ megosztás folyamatának (Vulnerabilities Equities Process – VEP) szabályzását. Ebben meghatározásra került, hogy a kormány mely esetekben hozza nyilvánosságra és mikor tartja vissza – nemzetbiztonsági célból – a szoftveres sebezhetőségekkel kapcsolatos információkat. A szabályzat továbbá előírja a feltárt, a nyilvánosságra hozott, illetve a visszatartott hibák számáról történő éves beszámolást. A VEP felülvizsgálati testülete a nyilvánosságra hozásról született döntésről a magánszektor vállalatait – amennyiben lehetséges – 7 munkanapon belül értesíti. **Bővebben...**

Minősített kormányzati adatok a Felhőben

(www.bleepingcomputer.com)

Az Amazon cég a héten bejelentette, hogy az amerikai hírszerző ügynökségek és alvállalkozóik számára létrehoz egy dedikált felhőszolgáltatást (AWS Secret Region). A cél a hírszerző műveletek támogatása gyorsabb adathozzáférés biztosításával, ami lehetővé teszi, hogy előzetesen jóváhagyott szervereken minősített (akár titkos és szigorúan titkos minősítési szintű) adatokat is kezelhessenek. Nem ez az első szolgáltatás, amit az Amazon nyújt az amerikai kormányzati szektor számára, már korábban elindították a GovCloud-ot, azonban az bizalmas információk kezelésére nem alkalmas. Az Amazon nincs egyedül ezen a piacon, ugyanis a Microsoft a múlt hónap során jelentette be egy hasonló szolgáltatását, az Azure Government Secret-et. **Bővebben...**

A kínai adatgyűjtés adatvédelmi jogokat sért

(www.indianexpress.com)

A Human Rights Watch (HRW) emberjogi szervezet arra kéri a kínai kormányt, hogy állítsák le a rendfenntartási platformok kiépítését, amelyekben egyre több érzékeny információt tárolnak állampolgáraikról. A megfigyelési technológiákat aktivisták, disszidensek és etnikai kisebbségek tevékenységeinek nyomon követésére használják és a HRW szerint több száz millió állampolgárról gyűjtenek és tárolnak információkat. A HRW felhívja a figyelmet arra, hogy a nemzetközi adatvédelmi előírások meghatározzák a magánszemélyek személyes adatainak gyűjtését, tárolását és rendészeti célokra történő felhasználását. Eszerint a megfigyelésekre csak akkor kerülhetne sor, ha az adott személy valódi fenyegetést jelent a közérdek számára – azonban a kínai gyakorlat ezeknek az adatvédelmi normáknak nem felel meg. **Bővebben...**