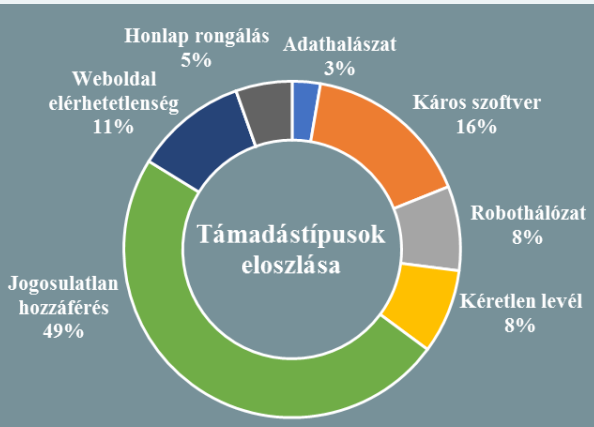
Incidens adatok:
2017.07.05. — 2017.07.11.



Osztrák jogszabálytervezet a titkosítás megkerüléséről

(www.zdnet.com)

Több európai ország mellett már Ausztria is vizsgálja egy új jogszabálytervezet létrehozásának lehetőségét, amely felhatalmazná a bűnüldöző hatóságokat a valós idejű titkosított alkalmazásokon (például WhatsApp és Skype) történő beszélgetések visszafejtésére. A tervezet jelenleg felülvizsgálat alatt áll, az osztrák kormány politikai, technológiai, polgári és jogi szakértőket kért fel e célból. Az ilyen jellegű megfigyeléseket csak bírói engedéllyel és kizárólag terrorcselekményekkel, vagy minimum öt év börtönbüntetéssel büntetendő bűncselekményekkel kapcsolatban végzett nyomozás során alkalmaznák. A kivitelezés módja még nem tisztázott, mindazonáltal Ronald Deibert, a torontói Citizen Lab biztonsági kutató csoport vezetője szerint a kémszoftverek célzott használata mellett teszi le a lándzsát több bűnüldöző hatóság és hírszerző ügynökség is. **Bővebben...**

Mindennaposak a kibertámadások

(www.bizreport.com)

2017. második negyedévére az Egyesült Királyságban 52%-kal nőtt a vállalatokat ért támadások száma – derült ki az ISO Beaming által készített vizsgálat jelentéséből. Az elmúlt három hónap során több mint 65 000 internetes támadás érte az Egyesült Királyságot, melyek főleg az IoT és beágyazott eszközöket (pl.: CCTV kamerák), valamint az épületek vezérlőrendszereit célozták (68%). Szembeötlő különbség még az első negyedévhez képest, hogy a vállalati adatbázisok kompromittálására irányuló kísérletek száma a második negyedévre jelentősen (673%-kal) emelkedett. A nagy nyilvánosságot kapott támadások – mint például a WannaCry – egyébként csekély mértékben befolyásolták az összképet. **Bővebben...**

Kétfaktoros azonosítás SMS-ben

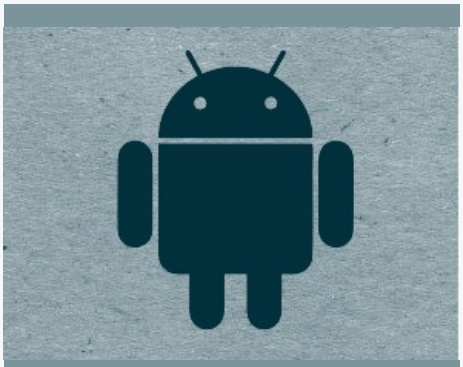
(www.nakedsecurity.sophos.com)

Egy új típusú (ún. SIM swapping) támadás során a támadó social engineering technikák alkalmazásával az áldozatnak kiadva magát megpróbálja letiltatni az áldozat SIM kártyáját (például elvesztésre hivatkozva) és aktiváltatni egy, a birtokában lévő újat. Amennyiben ezt sikerül kiviteleznie, támadást indíthat a jellemzően már korábban felderített érzékeny adatok (például jelszavak) felhasználásával az áldozat valamely fiókja ellen. 2016 augusztusa óta a NIST sem tekinti megfelelő biztonságúnak az SMS-útján történő kétfaktoros autentikációt az amerikai kormányzat számára. Az SMS helyett javasolt inkább egy authenticator alkalmazás-t használni. **Bővebben...**

A techóriások terroristagyanú esetén betekintést engednek a privát üzenetekbe

(www.helpnetsecurity.com)

Az európai kormányzatok nyomására a Facebook, a Twitter és a Google intézkedéseket hoztak az extrémizmus online terjedése ellen. Ennek szellemében az említett cégek moderátorai ellenőrizhetik az olyan felhasználók profilját – valamint akár privát üzeneteit is – akik terrorista cselekményre utaló tartalmakat osztanak meg. A postok megjelölését algoritmus végzi, azonban minden egyes üzenet esetében humán operátor ellenőrzi ennek a jogosságát és dönt az eltávolításról, vagy – amennyiben a fenyegetés mértéke megkívánja – a hatóság értesítéséről. Az operátori csapat legfontosabb feladata az ISIS és Al-Qaida 'utazó harcosainak' azonosítása, amely belső forrás szerint egy nap alatt megtörténik. **Bővebben...**



Új biztonsági megoldás Androidra

(www.news.softpedia.com)

Az XDA Developers szerint az Android 7.1-es verziójában elérhető egy hasznos biztonsági funkció, amelynek célja a különböző malware-ek (leginkább a telefont zároló zsarolóvírusok) elleni védekezés. Eszerint a "vissza" gombot négyszer lenyomva aktiváldik az ún. "pánikmód", amely leállítja az összes futó folyamatot (beleértve a zárolást is) és az eszköz visszaáll a kezdőképernyőre, így a felhasználónak lehetőséget biztosítva, hogy el tudja távolítani a káros kódot. A hírek szerint a funkció alapértelmezetten nincs bekapcsolva és a gyártóknak is aktiválniuk kell készülékein. A Google hivatalosan nem jelentette be a funkciót. **Bővebben...**

IT biztonsági Tanács

A Gmail-ben számtalan biztonsági beállítás létezik, melyekről a következő webhelyen tud tájékozódni:

https://myaccount.google.com

Íme néhány tipp:

Kövesse nyomon a fiókkal kapcsolatos aktivitásokat; ellenőrizze mely appok férnek hozzá fiókjához; illetve változtasson jelszót nagyobb adatszivárgások után.

Új biztonsági funkcióval bővül a G Suite

(www.blog.google.com)

A Google üzleti levelezése a meglévő biztonsági komponensek mellett bevezeti az OAuth applikációk fehérlistázását. Ennek segítségével megadhatjuk, hogy mely alkalmazások férhetnek hozzá a G Suite-ban tárolt adatainkhoz, ezáltal védve a vállalati információkat az esetleges rosszindulatú applikációktól. A funkció 2017.07.06-án, a közlemény nyilvánosságra hozatalakor még nem volt éles, a tervezett indítás a következő napokban várható. **Bővebben...**

Biztonságosabb lesz a katonák levelezése

(www.motherboard.com)

Annak ellenére, hogy a nagyobb online e-mail szolgáltatók már évek óta használnak titkosító algoritmusokat a levelezés biztonságosabbá tételére, az Amerikai Védelmi Minisztérium csak most jelentette be, hogy a 2018 júliusától használatba lépő új levelező infrastruktúrában már implementálnák az alapfokú titkosítást. Egy 2015-ös vizsgálat kimutatta, hogy az amerikai hadsereg levelezése (mail.mil) jelen formában potenciálisan sérülékeny. A 'STARTLS'-ként hivatkozott technológia azonban már több, mint tíz éve ismert és széles körben alkalmazott. **Bővebben...**

Cyber Intelligence Europe 2017

(www.intelligence-sec.com)

5th September 2017

2017. szeptember 5-én kerül megrendezésre Romániában az ötödik Cyber Intelligence Europe konferencia, ahol a kormányzati szféra vezető felelősei vitathatják meg kiberbiztonsági stratégiájukat, terveiket és az aktuális képességeiket. A konferencián részletes esettanulmányok kerülnek bemutatásra a közelmúlt fenyegetéseiről, támadásairól és az ezekkel kapcsolatban hozott válaszintézkedésekről, ezzel elősegítve az európai kormányzatok közötti együttműködést és információcserét. **Bővebben...**

Mintaértékű összefogás

(www.straitstimes.com)

Összefogást hirdetett a magánszektor és a szingapúri kiberbűnözés elleni központ (Singapore Police Cybercrime Command) az Interpol World 2017 konferencia megnyitóján. Az együttműködés máris lehetővé tette a hatóságok számára olyan bankszámlák befagyasztását, amelyek kapcsolatba hozhatók illegális tevékenységekkel, valamint sikerült megakadályozniuk egyes tengerentúli káros tranzakciókat. A szövetség mintegy 40 tagból áll, amelyek között IT vállalatok, telekommunikációs szolgáltatók, e-kereskedelmi platformok és bankok találhatók. A kapcsolat valójában már február óta fenn áll, a tagok szerint hatékonyan elősegítve az információáramlást. **Bővebben...**

Zárulnak a kínai kiskapuk

(www.gadgets.ndtv.com)

A kínai kormány rendeletben utasította az állami tulajdonban lévő telekommunikációs vállalatokat, hogy legkésőbb 2018. február 1-ig blokkolniuk kell a magánszemélyek VPN hálózatokhoz való hozzáférését, amiben jelenleg a China Mobile, a China Unicom és a China Telecom érintett. Ennek oka, hogy a VPN szolgáltatások lehetőséget nyújtanak az állami cenzúra által tiltott tartalmak (például Gmail, Facebook, Twitter) elérésére és ezzel széles körben éltek is. A technológiát több vállalkozás is alkalmazza a napi ügymenete során, így kérdéses az is, hogy rájuk mekkora hatással lesz az új intézkedés. A Kína területén működő cégeknek ráadásul meg kell birkózniuk a rendkívül szigorú új kiberbiztonsági törvénnyel is. **Bővebben...**