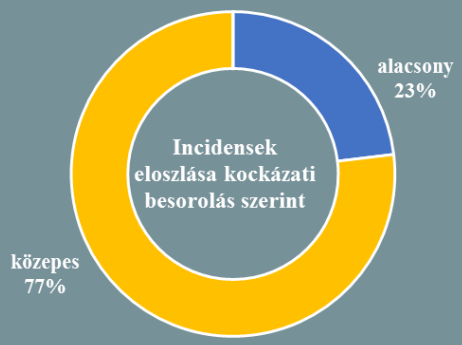
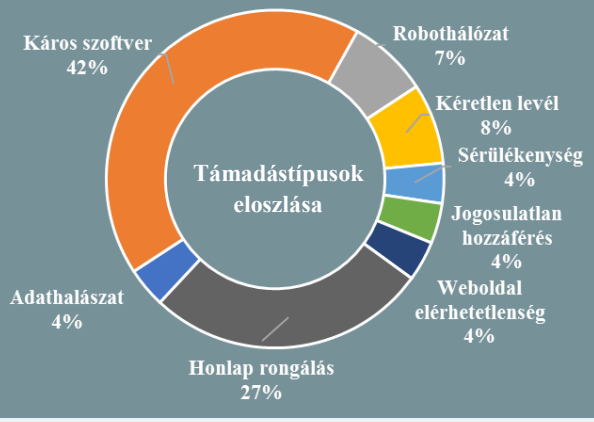
Incidens adatok: 2017.10.11. — 2017.10.17.





Ismertették az új brit internetes stratégiát

(www.informationsecuritybuzz.com)

Az Egyesült Királyság kormánya konzultációs dokumentumot tett közzé az internetes fenyegetésekről és az azok kezelésére vonatkozó intézkedési tervről. Az akadémiai és iparági szakértők bevonásával készült összefoglaló célja egy olyan keretrendszer felvázolása, amely képes lehet hatékony megoldást nyújtani az online fenyegetések széles körére, mint a zaklatás, a különböző megtévesztési formák, illetve az illegális tartalmak terjedése. A felvázolt intézkedések fókuszában a fiatalkorúak védelme áll, amiben – többek között – hangsúlyos szerepet kap az oktatás. A problémakör rendszerszintű kezeléséhez a Koronaügyészi Szolgálattal (Crown Prosecution Service, CPS) szemben elvárás, hogy olyan korszerű jogi útmutatások szülessenek, amelyek megkönnyítik a bírósági eljárások során az ítélethozatalokat. Emellett tervezik egy kifejezetten az online gyűlölet-bűncselekmények kivizsgálására szakosodott rendőrségi központ felállítását is. **Bővebben...**

Lehet, hogy az Ön gépén is kriptovalutát bányásznak

(www.blog.adguard.com)

Az utóbbi hetek során többek között a The Pirate Bay nevű, népszerű Torrent weboldalról is kiderült, hogy a site-ot meglátogatók számítógépeinek erőforrásait a felhasználók hozzájárulása nélkül kriptopénz bányászatra használják. Az AdGuard biztonsági cég megpróbálta felmérni, hogy nagyságrendileg hány hasonló oldal működhet még és megdöbbentő felfedezésre jutottak. A vizsgálatot az Alexa toplistáját alapul véve a 100 000 legnépszerűbb weboldalon végezték és olyan, bányászatra használt kódokat kerestek, amelyeket a legnépszerűbb platformok – mint a CoinHive és a JSEcoin – használnak. Ennek eredményeként 220 site esetében tudták igazolni a tevékenységet, ami hozzávetőlegesen félmilliárd embert érinthet. A relatíve kis szám (a vizsgált oldalak mindössze 0.22%-át érintette) ellenére a tevékenység hozama így is jelentős, több, mint 43 000 dollárra becsült. **Bővebben...**

A szorosabb együttműködés segíthet a "zsarolóvírus járványok" kezelésében

(www.informationsecuritybuzz.com)

A Lengyelországban tartott CyberSec európai kiberbiztonsági fórumon Julian King európai biztos megjegyezte, hogy nagyobb együttműködést vár az uniós tagállamoktól a számítógépes támadások elleni védekezésben. A fenyegetés nagyságrendjére utalva elmondta, tavaly átlagosan naponta 4 000-nél is több zsarolóvírus támadás történt az EU-ban. Ezzel összecseng Chris Ross, a Barracuda alelnökének véleménye, aki szerint a támadók egyre kifinomultabb módszerekkel dolgoznak. Egyetért azzal, hogy a ransomware támadási kampányok elleni küzdelem leghatékonyabb módja a tagállamok biztonsági szakértőinek együttműködése. Erre jó példaként említi a No More Ransom kezdeményezést, amit az Európai Kiberbűnözés Elleni Központ, a holland rendőrség, valamint több biztonsági cég hozott létre annak érdekében, hogy segítse a zsarolóvírus támadások áldozatait. **Bővebben...**

Az Apple válasza az adatvédelmi aggályokra

(www.engadget.com)

Al Franken amerikai szenátor levélben fordult az Apple vezérigazgatójához, Tim Cook-hoz, hogy aggodalmát fejezze ki az iPhone X készülékkel bevezetett új biometrikus arcfelismerő azonosító rendszerrel (Face ID) kapcsolatban. Ebben felvilágosítást kér a felhasználókról tárolt adatokhoz való hozzáférés biztonsági garanciáiról, kiemelve a harmadik féltől származó alkalmazások általi hozzáféréseket, legyen az akár egy bűnüldöző hatóságok általi adatkérés. Az Apple válaszában kifejti, hogy az azonosításra szolgáló érzékeny adatok soha nem hagyják el a készüléket, emellett titkosítva kerülnek letárolásra. Ezekhez harmadik féltől származó alkalmazások sem férnek hozzá direkt módon, pusztán az azonosítás eredményéről kapnak visszajelzést. **Bővebben...**

IT biztonsági Tanács

Okostelefonunk egyre gyakoribb célpontja az e-mail vagy SMS útján terjedő, kártékony kódra vagy adathalász tartalomra mutató hivatkozásokat tartalmazó üzeneteknek.

Ezért eszközünk védelme érdekében a rendszeres biztonsági mentés készítésén felül javasolt a megfelelő vírusvédelem alkalmazása, ezáltal csökkentve az adatlopás kockázatát.

Számítógépes zaklatás az iskolákban

(www.infosecurity-magazine.com)

Az amerikai szülők és az iskolai informatikai szakemberek körében végzett internetes zaklatásról szóló tanulmány szerint a megkérdezett IT szakemberek 35,3% azt állítja, hogy az internetes zaklatás okozta incidensek száma a 2017/2018-as tanévben növekedni fog. A Lightspeed Systems által végzett kutatás felhívja a figyelmet arra, hogy a számítógépes zaklatás egyre komolyabb probléma, mivel a mai fiatalok könnyedén hozzáférhetnek a technológiai eszközökhöz. A felmérés azt is megmutatja, hogy mindez gyakrabban fordul elő az iskolákban, mint 5 évvel ezelőtt. **Bővebben...**

Ukrajnában egy újabb pusztító kibertámadástól tartanak

(www.thestar.com)

Az ukrán kormány – amely idén már áldozatául esett egy nagyobb volumenű informatikai támadásnak – múlt hét pénteken arra figyelmeztette az ukrán szervezeteket és vállalkozásokat, hogy erősítsék meg hálózati védelmüket, mert feltehetően egy újabb támadás közeleg. Az Ukrán Biztonsági Szolgálat (SBU) és a kormányzati CERT egy, a NotPetya-hoz mérhető, lehetséges új támadásról adott hírt, amelyet előzetesen az október 13. és 17. közötti időszakra prognosztizáltak, az október 14-ei ukrán állami ünnep – Ukrajna védőjének napja – miatt. Az elmúlt időszak eseményeinek hatására Ukrajna az állami intézmények és a nagyvállalatok számítógépes biztonságának védelmében egy nemzeti stratégia kidolgozására törekszik. **Bővebben...**

Észak-Korea folytatja a bankok elleni támadásokat

(www.reuters.com)

A BAE Systems hadiipari cég szerint az Észak-Koreához kötött Lazarus APT csoport lehet a felelős egy tajvani pénzintézetet (Far Eastern International Bank) ért informatikai támadásért, amit egy, a SWIFT pénzügyi üzenetközvetítő hálózat elleni globális támadássorozat részének tartanak. Nem ez az első eset, hogy a rezsimet ilyen tevékenységgel gyanúsítják, a Bangladesh Bankot ért tavalyi incidenst is hozzájuk köti több biztonsági cég, köztük a Kaspersky Lab és a Symantec is. Adrian Nish, a BAE Systems kiberbiztonsági részlegének vezetője szerint a támadók komoly kiber arzenállal rendelkeznek és minden valószínűség szerint folytatni is fogják a műveleteket. A tajvani központi hírügynökség szerint habár az eltulajdonított 60 millió dollár nagy részét sikerült visszaszerezni, így is félmilliós kár keletkezett. **Bővebben...**

Máris pozitív hatással van a GDPR a biztonság megítélésére

(www.helpnetsecurity.com)

Az Európai Unió általános adatvédelmi rendeletének (GDPR) implementálásának határidejéhez közeledve az európai vállalkozások egyre komolyabbnak értékelik az informatikai biztonsági kockázatokat. Egy új felmérés során mintegy 1 300 vezetőt kérdeztek meg a témával kapcsolatban, akik 65%-a válaszolta azt, hogy jelenleg a kiberbiztonságot tekintik a legnagyobb kockázati tényezőnek, ami jelentős növekedést mutat a tavalyi felmérés eredményeihez képest, amikor csupán 32% sorolta azt az első öt közé. A felmérés szerint a szervezetek többsége növelte – vagy a közeljövőben növelni fogja – a védelmi és kockázatkezelési beruházásokat, azonban csupán 8%-uk állította, hogy már most megfelelnek a követelményeknek. **Bővebben...**