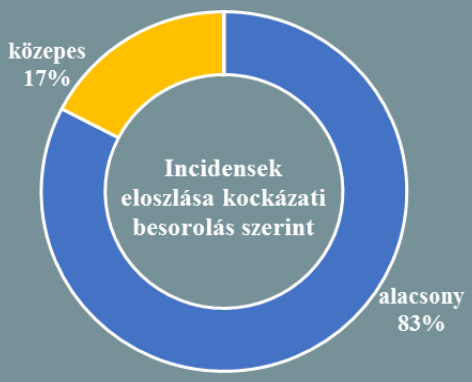
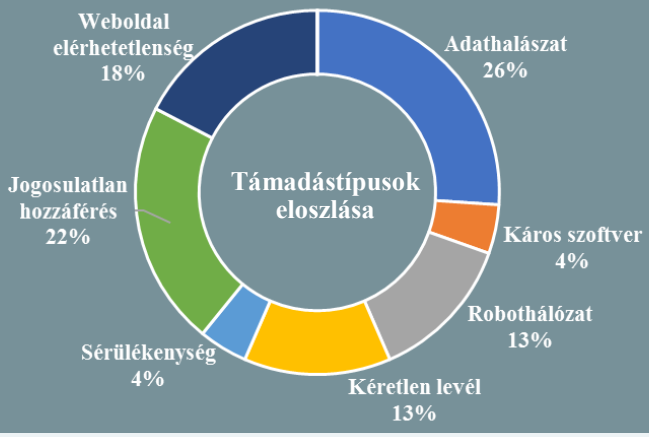
Incidens adatok:
2017.09.27. — 2017.10.03.





Oroszország új internetes kijáratot biztosít Észak-Korea számára

(www.reuters.com)

A Dyn Research jelentette, hogy vasárnap óta észak-koreai internetes forgalmat érzékelnek az orosz TransTeleCom-on keresztül. Elemzések szerint az összes hálózati forgalom körülbelül 60%-a irányul erre, a maradék továbbra is a már ismert útvonalon, a kínai China Unicom-on keresztül routolva jut el a külvilágba. A TransTeleCom hivatalosan nem erősítette meg, hogy új szerződést kötöttek volna a rezsimmel, helyette egy 2009-es megállapodásra hivatkoznak. Ismert, hogy az ország internetes hozzáférései limitáltak – körülbelül a néhány száz és a kicsivel több, mint ezer között mozognak – amelyek Bryce Boland, a FireEye műszaki vezetője szerint ugyan javarészt nem eredői a rezsim által indított kibertámadásoknak, azonban létfontosságúak azok koordinálásához, így ezek rendelkezésreállásának növelése közvetve a rezsim által jelentett kiberfenyegetési potenciálra is hatással van. **Bővebben...**

Új biztonsági termék a Google-től

(www.firstpost.com)

A Bloomberg által közzétett jelentés szerint, az Alphabet Inc. új biztonsági termék (Advanced Protection Program) bevezetését tervezi október során, amely az illetéktelen hozzáférésektől védené a Google felhőben tárolt fiókokat és fájlokat, azonban a legmagasabb szintű biztonsághoz továbbra is szükség lesz egy USB, valamint egy második fizikai kulcsra is. A kiszivárgott hírek szerint a szolgáltatást első körben főleg a célzott támadásoknak fokozottan kitett felhasználóknak szánják, mint például a vállalati vezetők, politikusok vagy hírességek és további funkciókat is tartalmazni fog. A Google részéről hivatalos megerősítés még nem történt. **Bővebben...**

Európai Kiberbiztonsági Hónap

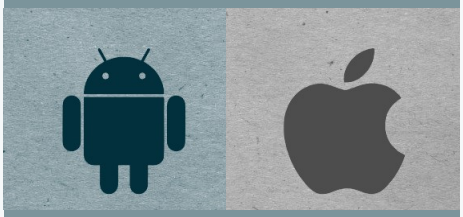
(www.kiberhonap.hu)

Az ENISA idén októberben is megszervezi nemzetközi kiberbiztonsági kampányát a European Cyber Security Month – ECSM-et, melynek célja a kiberbiztonsági tudatosság növelése, valamint a kibertérben megjelenő fenyegetések széles körben történő ismertetése, így az ECSM keretein belül az Uniós tagországok képzéseket és előadásokat tartanak. Az idei kampány kiemelt témái közé tartozik az IT biztonság megvalósítása munkahelyi és otthoni környezetben, az adatvédelmi kihívások és a szabályzások, valamint a kiberbiztonsági képességek. Az ECSM kampányról és az októberre tervezett hazai és nemzetközi eseményekről **bővebben...**

Amerikai kiber hadműveletek Észak-Korea ellen

(www.washingtonpost.com)

Donald Trump amerikai elnök még hivatalba lépése kezdetén hozott rendeletet az Észak-Korea elleni stratégiai nyomásgyakorlásról. Ennek részeként diplomáciai eszközök bevetése mellett az amerikai kiberparancsnokság is utasítást kapott internetes támadások indításához az észak-koreai katonai hírszerző ügynökség (Reconnaissance General Bureau) ellen, amelyek – értesülések szerint vélhetően túlterheléses támadások során – az internetes hozzáférésben okoztak zavarokat. Ezzel kapcsolatban az érintett szerv, vagy a Fehér Ház részéről hivatalos állásfoglalás nem érhető el, azonban egyes amerikai tisztviselők a támadásokat „nem pusztító célúnak” jellemezték, melyek hatásukat tekintve csupán átmeneti problémát okoztak. Több, még az Obama adminisztráció idején kiber területen tisztséget betöltő szakértő üdvözölte az intézkedést, egyesek azonban egy lehetséges válaszcsapást kiváltó, felesleges provokációnak minősítették. **Bővebben...**



Így lehet még biztonságosabb a Signal

(www.securityaffairs.co)

Új módszerrel végezné az Open Whisper Systems a már eddig is sokak által a legbiztonságosabbnak kikiáltott kommunikációs platform, a Signal esetében a kapcsolati adatok felderítését. A jelenlegi metódust – amely szerint a Signal kliens, a felhasználó készülékén található kapcsolati adatok hash-elt értékeit hasonlítja össze az OWS szerverén lévőkkel – egy, az Intel által gyártott újgenerációs chipekben már támogatott eljárás (Software Guard Extensions) bővítenék ki. Az SGX megoldás keretében egy dedikált memóriaterületet használnak, amihez még az operációs rendszer sem férhet hozzá. **Bővebben...**

IT biztonsági Tanács

Az Android 6.0 vagy ettől újabb verziót futtató eszközökön beállítható, hogy az alkalmazások mely funkciókhoz vagy adatokhoz férhetnek hozzá.

Célszerű az alkalmazás engedélykéréseket rendszeresen felülvizsgálni, például a rendszer-, illetve alkalmazásfrissítések után, mert előfordulhat, hogy a korábban beállított hozzáférési lista módosulhat.

Európai Uniós fellépés az illegális tartalmak ellen

(www.euractiv.com)

Az Európai Bizottság szeretné elérni, hogy az illegális tartalmakat nagyobb mértékben távolítsák el a Facebook-hoz hasonló internetes platformok. Ennek érdekében a múlt hét során publikálták azon elvárásokat, amelyek a tech cégek számára irányadóak a jogsértő tartalmak gyors és hatékony felderítéséhez. Többek között javaslatokat fogalmaznak meg a bíróságokkal és a hatóságokkal való kapcsolattartás módjáról, illetve a káros tartalmak jelentésére szolgáló dedikált csatornák létesítésének fontosságáról. Egyelőre nem kötelező érvényű a megfelelőség kialakítása, de amennyiben az ajánlások nem érik el a kellő hatást, az EB jogszabályban is rögzítené azokat 2018 során. Nem titkolt cél az sem, hogy a tagországok egyedi szabályozásai helyett – mint az történt Franciaország, valamint Németország esetében – egy koherens EU-s jogszabály szülessen. **Bővebben...**

Részben automatizált e-ügyintézés

(www.zdnet.com)

A szingapúri GovTech technológiai ügynökség múlt hét elején jelentette be, hogy az online ügyintézés megkönnyítése céljából az elektronikus kormányzati portálon (SingPass) regisztrált felhasználók számára automatikus űrlapkitöltő funkciót vezetnek be. Ehhez legkésőbb 2017 végéig minden SingPass felhasználó rendelkezni fog egy személyes információkat tároló MyInfo profillal, amin keresztül az adott személyre vonatkozó összes személyes információ lekérdezhető, amely kormányhivatali ügyintézés során valamelyik szervnél regisztrálásra került, anélkül, hogy egy központosított adatbázisra lenne szükség. A GovTech szóvivője hangsúlyozta, hogy a rendszert iparági ajánlásokat követve többszintű védelemmel látják el. **Bővebben...**

Egyre kevesebb tudás kell a kiberbűnözéshez

(www.zdnet.com)

A zsarolóvírus támadások mellett szinte minden eltörpült eddig 2017-ben, ami elsősorban annak köszönhető, hogy még mindig ez az egyik legkönnyebb módja a gyors profitszerzésnek. További problémát jelent, hogy mára felnőtt korba lépett a hacking eszközöket az alacsonyabb technikai felkészültségűek számára is elérhetővé tevő 'CaaS' (Crime-as-a-service) üzleti modell, abban az értelemben is, hogy ezeket a szervezett bűnözés tervezetten igénybe veszi. Ahhoz, hogy mindezzel sikeresen fel lehessen venni a harcot, a hatóságoknak jóval több erőforrást kell befektetniük, figyelmeztet az Europol, az internetes fenyegetéseket összegző éves jelentésében. **Bővebben...**

Szigorú tartalomellenőrzés a közösségi oldalakon

(www.techcrunch.com)

Németországban hatályba lépett a „NetzDG”, a közösségi médiaplatformokon megjelenő gyűlöletkeltő tartalmak visszaszorítását célzó törvény. Ez alapján a káros tartalomról érkező bejelentések után a szolgáltatóknak az egyértelmű esetekben 24 óra áll rendelkezésre az eltávolításhoz, a mélyebb értékelést igénylő posztok kapcsán pedig egy hét a türelmi idő. Emellett minden érintett vállalatnak – beleértve a kisebbeket is – ki kell jelölniük egy kapcsolattartót Németországban, aki mind a felhasználói panaszokat, mind a hatóságoktól érkező kéréseket hivatott kezelni. A jogszabálynak való nem megfelelés komoly (akár 50 millió eurós) bírságot vonhat maga után. Habár a felügyelettel megbízott minisztérium már indított is ellenőrzéseket, a vállalatoknak 2018. január 1-ig még van idejük felkészülni. **Bővebben...**