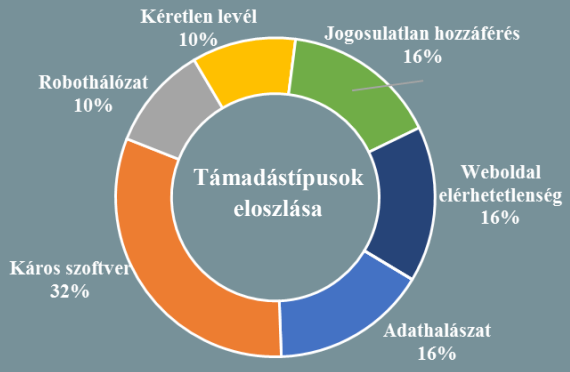
Incidens adatok: 2017.11.22. — 2017.11.28.



Titkosított felhőszolgáltatást indított a GMX és a Web.de

(www.heise.de)

A német GMX és a Web.de e-mail szolgáltatók végponti titkosítás biztosításával bővítik ki a felhő szolgáltatásukat (Cloud made in Germany). A két szolgáltató mintegy 30 millió ügyfelének nincs szüksége különösebb szakértelemre, hogy érzékeny adatait a szolgáltatók által a felhőben biztosított biztonságos tárolóban helyezhesse el. A szolgáltatás igénybevétele ingyenes, melyhez 2GB tárhely jár, ami akár 1TB-ig is bővíthető. A szolgáltatók ígérete szerint a felhasználók részéről csupán egy – megfelelően erős – jelszó megadása szükséges a telepítés során és a felhasználói adatok titkosításáról innentől az alkalmazás gondoskodik. **Bővebben...**

Jogszerű kibertámadásokra törekszik Németország

(www.reuters.com)

A német belügyminisztérium egy munkatársa szerint alkotmánymódosításra van szükség, hogy az országot érő kibertámadások esetében jogszerűen válaszcsapást indíthassanak. Magas rangú hírszerző tisztek a múlt hónap során már nagyobb jogi felhatalmazást kértek, arra hivatkozva, hogy a hálózatbiztonságot veszélyeztető újszerű támadások offenzív képességek fejlesztését kívánják meg. Úgy tűnik az előrelépésre már nem kell sokat várni, ugyanis a jogszabályi környezet legkésőbb a jövő év végéig pozitív változáson fog átesni – nyilatkozta Klaus Vitt államtitkár a Reutersnek. Arne Schoenbohm, a BSI elnöke ugyan nem fedte fel a jogi tervezet pontos részleteit, azonban elárulta, hogy a szerverek elleni támadások a tervezett intézkedéseknek csupán 0,01 %-át tennék ki. **Bővebben...**

Kínaiak kémkedhettek amerikai cégek után

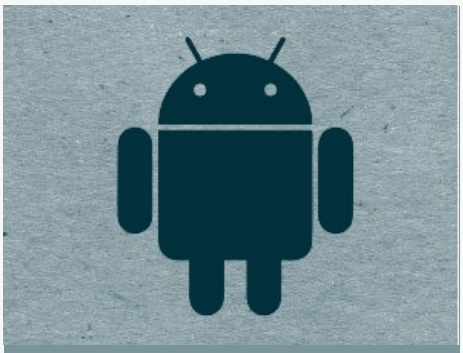
(www.zdnet.com)

Az amerikai igazságügyi minisztérium bejelentette, hogy ipari kémkedéssel vádolnak három kínai személyt. Wu Yingzhuo, Dong Hao és Xia Lei egy internetes biztonsági cégnél, a Guangzhou Bo Yu Information Technology-nél (Boyusec) álltak alkalmazásában és a vádirat szerint 2011 és 2017 májusa között illetéktelenül hozzáfértek több amerikai cég rendszeréhez. A feltételezett áldozatok között van a Moody's Analytics, a Trimble és a Siemens is. A hírek szerint több száz gigabájtnyi adatot sikerült ellopniuk, a támadások során belső dokumentumokat, felhasználói hitelesítő adatokat és egyéb bizalmas személyes információkat is megszereztek. Amennyiben minden vádpontban bűnösnek találják őket, 42 évnyi börtönbüntetésre számíthatnak. **Bővebben...**

Az EU az Internet blokkolásával védi meg a fogyasztókat?

(www.eff.org)

Múlt héten az Európai Parlament jóváhagyta „a fogyasztóvédelmi jogszabályok végrehajtásáért felelős nemzeti hatóságok közötti együttműködésről és a 2006/2004/EK rendelet hatályon kívül helyezéséről” szóló, az Európai Parlament és az Európai Tanács közös rendeletét, mely felhatalmazza a nemzeti fogyasztóvédelmi szervezeteket arra, hogy az internetszolgáltatókat, weboldal kiszolgálókat és az internetes domain regisztrátorokat kötelezhessék arra, hogy blokkoljanak vagy töröljenek weboldalakat – mindezt bírósági határozat nélkül. A rendelet célja az volt, hogy könnyebbé váljon azon oldalak blokkolása vagy tiltása, melyek megsértik az európai fogyasztóvédelmi törvényeket. A hatóságok kontroll nélkül alkalmazható tiltásainak kockázatát azonban jól mutatja az a 2014-es eset, amikor egy ausztrál szervezet véletlenül 250 000 weboldalt blokkolt, miközben csupán néhány oldal tiltása állt szándékában. **Bővebben...**



A mobilunk is szólni fog, ha figyelik a kijelzőt

(www.cnet.com)

A Google kutatói olyan biztonsági funkciót dolgoztak ki, mely a mesterséges intelligencia és az arcfelismerés segítségével segít megvédeni a mobileszközök tulajdonosait a zsúfolt helyeken gyakran előforduló ún. kifigyeléstől (Shoulder Surfing) és az ily módon elkövetett adatlopásoktól. Az előlapi kamerát használva az új biztonsági funkció képes érzékelni, ha rajtunk kívül más is nézi a képernyőt, ilyenkor a kijelző átvált az első kamerára és egy szivárvány megjelenítésével figyelmeztet a leselkedőre. Amint az idegen elveszi pillantását a kijelzőről, a képernyő visszavált az eredeti tevékenységre. A kutatók a decemberi Neural Information Processing Systems (NIPS) konferenciára tervezik az új szoftver bemutatását, azonban a Google egyelőre még nem jelentette be a funkció integrálását. **Bővebben...**

IT biztonsági Tanács

Engedélyezze az Office 365 Exchange Online Protection (EOP) biztonsági tippjeit, melyek előugró párbeszédpanelen jelennek meg az e-mail üzenetek egyszerű és vizuális biztonsági ellenőrzésének segítése céljából.

A biztonsági tippek testreszabhatóak a vállalat irányelveihez és házirendjeihez.

Bővebb információkért keresse a Microsoft Windows weboldalát.

Az első éves összefoglaló a eIDAS-ról

(www.enisa.europa.eu)

Egy évvel az eIDAS rendelet hatályba lépését követően, az ENISA közzétette éves összefoglaló jelentését, mely szerint 2016 második felében mindössze egy incidenst vettek nyilvántartásba, mely egy TSP-t érintett és az elektronikus aláírási szolgáltatáshoz tartozó minősített tanúsítványok ellenőrzésével állt kapcsolatban. A szolgáltató szerencsére hamar intézkedett a javításról. **Bővebben...**

Betilthatják a személyes készülékek használatát a Fehér Házban

(www.thestar.com)

Egyes, anonimitásukat kérő tisztviselők szerint a szigorítás elsődleges oka nem a média felé történő információ szivárogtatások, hanem jól felfogott hálózatbiztonsági érdek. Információk szerint ugyanis túl sok személyes eszköz csatlakozik a belső vezeték nélküli hálózathoz, amelyek nem rendelkeznek olyan védelemmel, mint a szövetségi kormány által kiadott eszközök. Bizonyos korlátozásokat ugyanakkor már régebb óta alkalmaznak: a találkozókra nem lehet bevinni telefonokat, emellett a hivatal hálózatáról kitiltásra kerültek egyes weboldalak, mint például a Gmail és a Hangouts. A javaslat ellenzői arra hivatkoznak, hogy a kormányzati adatmegőrzési követelmények miatt a hívások rögzítésre kerülnek és nyilvánosságra hozhatóak, illetve, hogy a hivatalnokoknak ezután egyáltalán nem lesz lehetőségük hozzáférni a privát fiókjukhoz a teljes munkaidő alatt. **Bővebben...**

Észtországban megkezdődött a NATO kibervédelmi gyakorlata

(www.ncia.nato.int)

A NATO legnagyobb kibervédelmi gyakorlata, a Cyber Coalition a napokban zajlik Észtországban. A gyakorlatban több, mint 25 szövetséges és NATO partnerország vesz részt, az Európai Unió, az ipar és különböző oktatási intézmények képviseletében. Ennek során – immár tizedik alkalommal – a szövetség partnereinek lehetőségük van a NATO és az egyes nemzetek informatikai infrastruktúrájának védelmét gyakorolni. A gyakorlat előkészítése során a szervezők nagy hangsúlyt fektettek arra, hogy minél realisztikusabb kihívásokat állítsanak a résztvevők elé, így azok szembesülnek többek közt káros kóddal való fertőződéssel, közösségi hálózaton megjelenő fenyegetésekkel, mobil eszközöket célzó támadásokkal éppúgy, mint a hibrid hadviselés kihívásaival. A három napos gyakorlat a NATO észtországi kiber gyakorlóterén zajlik, amihez a résztvevők nagy része otthonról fér hozzá. **Bővebben...**

Továbbra sem megfelelő biztonsági szintűek az Egyesült Államok kormányzati portáljai

(www.infosecurity-magazine.com)

A leggyakrabban látogatott amerikai kormányzati weboldalak többsége még mindig nem felel meg az amerikai kormányzat által meghatározott biztonsági és technikai követelményeknek, valamint iparági szabványoknak – állapította meg az Informatikai és Innovációs Alapítvány (ITIF) jelentésében. A vizsgált 469 kormányzati weboldal 91%-nál a kulcsfontosságú mérési szempontok (mint terhelhetőség, mobil kompabilitás, biztonság és hozzáférhetőség) közül legalább egy esetében hiányossággal szembesültek a kutatók. Daniel Castro az ITIF alelnöke szerint annak ellenére, hogy köztudomású, hogy a kormányzati weboldalak elmaradnak a követelményektől, az elmúlt egy évben mégsem történt lényeges előrelépés a weboldalak javítása és korszerűsítése terén. **Bővebben...**