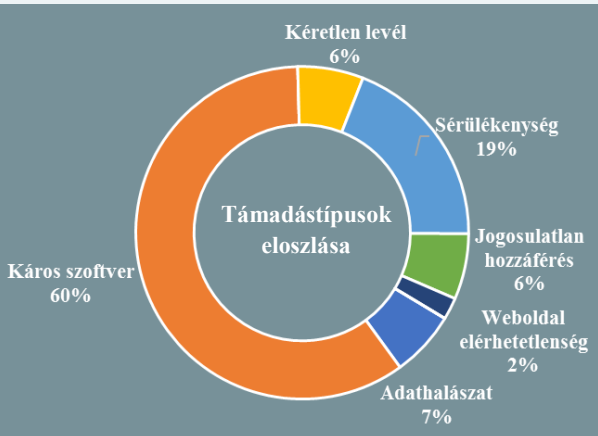
Incidens adatok: 2017.11.08. — 2017.11.14.



Irányelvek a kiberbiztosítás nyelvi egységesítéséhez

(www.enisa.europa.eu)

Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (ENISA) kiberbiztosításra vonatkozó ajánlásokat tett közzé (Recommendations on cyber-insurance), melyben a kockázatkezelési terminológia egységes használatára tesz javaslatokat. Az ENISA szerint a nyelvi harmonizáció sok szempontból hasznos lenne, többek között segítséget nyújthat a szabványosítási törekvésekhez, lehetővé teheti a számítógépes kockázatok jobb megértését és modellezését. Udo Helmbrecht, az ügynökség vezetője kiemelte, ez a teljes kiberbiztosítási piacra jótékony hatást gyakorolna, például a kiberbiztonsági termékek vásárlására, hiszen a vevők számára sokkal könnyebb lenne a termékek összehasonlítása. **Bővebben...**

Egyre több az online bűncselekmény

(www.latesthackingnews.com)

Az Egyesült Királyság a számítógépes bűnözés gyakoriságáról készített legutóbbi jelentésében – mely a 2016 júliusa és 2017 júniusa közötti időszakot öleli át – 55 000 internetes bűncselekményről számoltak be, ami azt jelenti, hogy az elmúlt évben átlagosan napi 150 esetet tapasztaltak az országban. A bejelentett bűncselekmények többségét a zaklatások és a zsarolások teszik ki, de hangsúlyosan jelennek meg az adathalász támadások és a zsarolóvírusok is. Az Egyesült Királyság Nemzeti Statisztikai Hivatala a tendenciák alapján a káros internetes tevékenységek gyakoriságának folyamatos emelkedését prognosztizálja, amennyiben a hatóságok nem fejlesztenek ki új módszereket az anonimitás leküzdésére. Komoly nehézségeket okoz például a névtelenséget biztosító Tor hálózat, de ide sorolhatók a VPN szolgáltatások is. **Bővebben...**

Vállalati mobil eszközök és a GDPR

(www.helpnetsecurity.com)

A Lookout biztonsági cég felmérést végzett a vállalati mobil eszközök okozta kockázatról az Európai Unió Általános Adatvédelmi Rendeletének (GDPR) tükrében. A vizsgálat eredményei szerint a résztvevő amerikai IT vezetők 84%-a véli úgy, hogy a dolgozók mobil eszközein keresztül elérhető szenzitív adatok a vállalat számára problémát okozhatnak a GDPR-nak való megfelelés szempontjából. Ezt alátámasztja az is, hogy a munkavállalók 64%-a mobil eszközein keresztül is eléri a vállalati szenzitív adatokat, ami különösen aggasztó, annak fényében, hogy kiderült, 70%-uk ugyanazt az eszközt használja magáncélra is. Az is lényegesen növeli a kockázatot, hogy az alkalmazottak a munkavégzésre szánt eszközökre sokszor harmadik féltől származó alkalmazásokat is letöltenek. **Bővebben...**

A felhasználói fiókok kompromittálódásának okai

(www.security.googleblog.com)

Az internethasználók több, mint 15%-a szenvedett már el valamilyen – e-mail vagy közösségi média fiókot érintő – kompromittálódást. A Google a probléma mélyebb megértését tűzte ki célul és a Kaliforniai Egyetemmel karöltve 2016 márciusától egy éven át kiterjedt vizsgálatot folytattak a feketepiacok tanulmányozásával. Ennek során azt találták, hogy mintegy 788 000 hitelesítő adatot loptak el billentyűzetleütést figyelő szoftverrel, 12 milliót adathalászat útján és mintegy 3,3 milliárd azonosító kompromittálódott harmadik félnél történt adatszivárgási incidensek következtében. Sok esetben olyan érzékeny adatok is célpontok lehetnek, amelyek a személyazonosság meghatározásában játszhatnak szerepet: IP címek, tartózkodási hely információk, telefonszámok stb. A felhasználókra nézve legmagasabb kockázatúnak az adathalászatot minősítették , a keyloggerek, és az adatszivárgások csak ezután következnek. **Bővebben...**

Szigorít a Google az androidos felhasználók védelmében

(www.bleepingcomputer.com)

A tech cég e-mailben tájékoztatta androidos fejlesztőit, hogy minden olyan applikációt el fog távolítani a Google Play Store-ból, amelyek nem az előírásoknak megfelelően alkalmazzák az Android Accessibility API-t. A fejlesztőknek 30 napjuk van átlátható magyarázatot adni a funkció használatának okáról, vagy eltávolítani a szolgáltatáshoz való hozzáférési igényt. A felhasználói interakciót helyettesítő, kiegészítő programot eredetileg abból a célból hozták létre, hogy segítsék a fogyatékkal élő felhasználók számára létrehozott alkalmazások működését. A funkcióban rejlő lehetőségeket azonban káros kódok – jellemzően banki trójaik – fejlesztői is felismerték. Az intézkedéstől azt várják, hogy a káros szoftverek nehezebben szivárognak majd be a Play Store-ba. **Bővebben...**

IT biztonsági Tanács

A már használaton kívüli eszközeink (telefon, tablet, SD kártya) olyan érzékeny információkat tartalmazhatnak (jelszó, számlaszám), amelyek jogosulatlan kezekben visszaélésre adhatnak lehetőséget.

Ha úgy véljük, hogy adatainkra későbbiekben szükségünk lehet, készítsünk biztonsági mentést, ezt követően töröljünk róla minden adatot, és állítsuk gyári állapotba a készüléket. Ezt követően ellenőrizzük, hogy sikeres volt-e az adatok törlése.

Orosz kibertevékenység az Egyesült Királyságban

(www.nytimes.com)

Az elmúlt 12 hónapban orosz hackerek folyamatosan támadásokat intéztek brit energia-, távközlési és média iparági szereplők ellen, nyilatkozta Ciarna Martin, a brit Nemzeti Kibervédelmi Központ (NCSC - National Cyber Security Center) vezetője. Eszerint a nyugati kormányok és iparágak elleni orosz kibertevékenység a korábban feltételezettnél sokkal kiterjedtebb. Az esetről tartott sajtótájékoztatón felszólalt Theresan May, brit miniszterelnök is. **Bővebben...**

Az online propaganda új szintre lépett

(www.infosecurity-magazine.com)

Mára egyre szélesebb azon államok köre, akik – orosz és kínai mintára – aktívan igyekeznek aláásni a demokratikus folyamatokat a rivális országokban, azáltal, hogy megnehezítik a szavazók számára a tényszerű híreken és hiteles vitákon alapuló választás lehetőségét. A Freedom House által készített 2017-es 'Freedom on the Net' jelentés szerint az elmúlt egy évben legalább 18 országban próbálták befolyásolni a választásokat közösségi oldalakon terjesztett álhíreken keresztül, valamint egyéb propaganda eszközök – például fizetett kommentátorok és automatizált hozzászólások – felhasználásával. Az utóbbi időben több országban is szigorították az internetes szabályzókat és szolgáltatásokat, azonban Sanja Kelly, a vizsgálat vezetője szerint a megoldás nem az internet cenzúrázásban rejlik, hanem a dezinformáció felderítésében és elhárításában, ami azonban sokszor nehezebb mint a direkt támadások kezelése. **Bővebben...**

Fontos az önállóság a kiberháborúk korában

(www.itwire.com)

Greg Austin, a New South Wales Egyetem Kiberbiztonsági Központ ügyvezető igazgatója az ausztrál honvédelmi miniszter geopolitikai események gazdasági hatásairól szóló jelentése kapcsán fejtette ki a véleményét. Eszerint az ország háború esetén nem számíthat arra, hogy legnagyobb szövetségese, az Egyesült Államok lényeges támogatást nyújtson egy összetett kibertámadás kivédéséhez, mivel az túlontúl elfoglalt lenne a saját rendszerei védelmével.

A professzor azt is megjegyezte, hogy bár az ausztrál védelmi erők már megkezdték a kiberhadviselésre való felkészülést, azonban az mintegy két évtizedes késésben van, amiért elképzelhető, hogy súlyos árat kell fizetni. Javaslatai között kiemelt szerepet kap az oktatás és egy olyan nemzeti innovációs stratégia kidolgozása, ami biztosítja a független kibervédelmi képességeket és a túlélést egy katonai offenzíva esetén. **Bővebben...**

Egyre inkább fókuszba kerül az IoT eszközök biztonsága

(www.bleepingcomputer.com)

Az Avira Safe Things Sentinel egy olyan szoftveres megoldást nyújt az IoT eszközök védelmére, amelyet az internetszolgáltatók és a hálózati forgalomirányítók gyártói implementálhatnak eszközeikbe, annak érdekében, hogy figyelemmel kísérhessék az IoT eszközök viselkedését és szükség esetén közbeavatkozhassanak. A program a háttérben fut, miközben elemzi a csomagok fejlécét és szükség esetén érvényesíti a definiált védelmi szabályokat. A routeren található Sentinel az összegyűjtött meta adatokat továbbítja (adatvédelmi szempontból semmilyen érzékeny információt nem továbbít) az Avira Safe Things Protection Cloud-ba elemzésre, amely mesterséges intelligenciát is használva képes detektálni az anomáliákat. **Bővebben...**