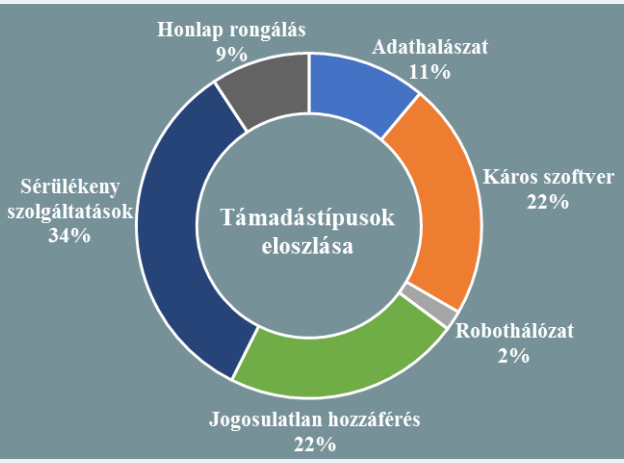
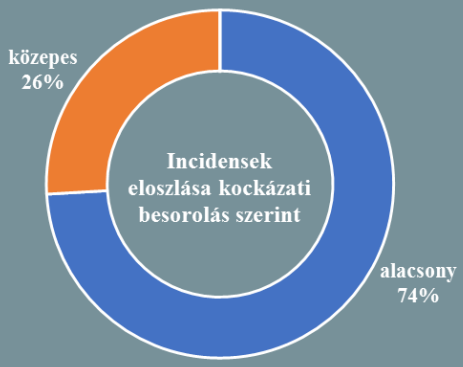
Nemzetközi IT-biztonsági sajtószemle

Incidens adatok:
2017.05.31. — 2017.06.06.





Az európai IT munkaerőpiac helyzete és jövője

(www.infosecurity-magazine.com)

Az (ISC)2 készített tanulmányt a témában, amely szerint az európai vállalatok tesznek a legtöbbet a 2022-re már 350,000-esre prognosztizált IT biztonsági szakemberhiány betöltéséhez. A tanulmány kimutatta, hogy lényeges eltérés tapasztalható abban, hogy a felek mely képességeket ítélik fontosabbnak. A munkáltatók inkább a magas kommunikációs (66%), és elemző képességeket (59%) keresik, a munkavállalók ezzel szemben a felhő alapú technológiák terén szerzett tapasztalatokat és az általános biztonsági ismereteket (60%), valamint a vezetői (41%) képességeket érzik fontosabbnak, a közös halmaz pedig csupán 20%. **Bővebben...**

Az incidens kezelés hatékonyságának növelése

(www.helpnetsecurity.com)

Az IDC több száz amerikai és európai biztonsági szakember bevonásával kutatást végzett, amelyből kiderült, a támadások mértéke jó részt meghaladja a biztonsági csapatok felkészültségét. Fontos tapasztalat továbbá, hogy a szervezetek több, mint fele (53%) szerint a kiberbiztonsági képességek legnagyobb visszafogó tényezője, hogy az erőforrásokat nagyrészt lekötik a rutin feladatok és az incidensek kivizsgálása. A fenyegetések egyre növekvő volta miatt elengedhetetlen a hatékonyság növelése, például minél szélesebb körű automatizálással, stratégiai tervezéssel, megfelelő erőforrás -allokációval. **Bővebben...**

Google: gépi tanulással az adathalászat ellen

(www.pctechmag.com)

A biztonság növelése céljából a Google három új biztonsági funkciót is bevezet a vállalati Gmail szolgáltatásban (G suite), ezek az adathalász támadások korai észlelése, a klikkeléskor történő figyelmeztetések gyanús URL-ek esetén, valamint a külső forrásból származó üzenetekre való válaszolás esetén történő értesítések. Minderre azért van szükség, mert a keresőóriás saját becslései szerint a Gmail által fogadott levelek 50-70%-a spam. A biztonsági funkciókhoz a gépi tanulást is integrálták, amellyel elmondásuk szerint 99,9%-os pontossággal képesek a kéretlen leveleket blokkolni. **Bővebben...**

Következetlenség a nemzetközi szabályzásban

(www.searchsecurity.techtarget.com)

Az új kínai kiberbiztonsági törvény rávilágít arra, hogy az országhatárokon átívelő adatvédelmi szabályok harmonizációja mennyire hiányos. Egyes rendelkezések ország-specifikusak, mások az iparra koncentrálnak, a technológiából fakadóan mégis jellemzően globális hatókörrel bírnak. Elemzők szerint a nagyvállalatoknak ebben az összetett környezetben elsősorban az adatbiztonságra, az adatkezelési irányelvekre, biztonságtudatosítási képzésekre kell koncentrálniuk, emellett olyan biztonsági keretrendszert választani, ami a lehető legtöbb követelményre tekintettel van. **Bővebben...**

Új beállítási lehetőség az iOS11-en

(www.techcrunch.com)

A szeptemberben megjelenő iOS11 új beállítási lehetőségével korlátozni tudjuk az eszköz helyadatainak hozzáférését. Egyes alkalmazások, mint az Uber vagy a Waze folyamatosan lekéri a készülék helyadatait, akkor is ha az alkalmazás nincs használatban. Egy új beállítási lehetőséggel a helyadatok csak akkor kerülnek megosztásra, ha az alkalmazások használatban vannak. Ez nem csak a felhasználói adatvédelem szempontjából fontos, hanem növelheti a készülék akkumulátorának élettartamát. **Bővebben...**

IT biztonsági tanács

A pszichológiai manipuláció (Social engineering) segítségével a támadók képesek különböző módszerekkel rávenni a felhasználókat védett adataik felfedésére.

A támadások megelőzése a biztonságtudatos magatartásra épül: ne nyissunk meg gyanús linkeket és csatolmányokat és legyünk kritikusak azzal kapcsolatban, hogy kivel osztunk meg bizalmas információkat

Újabb brit internetes szabályzás a láthatáron?

(www.forbes.com)

Theresa May brit miniszterelnök továbbra is kiáll az új internet szabályzás mellett, amelynek központi eleme a titkosítás eltörlése. May a Kínai Nagy Tűzfalhoz hasonlóan egyszerűen kitiltaná azon alkalmazásokat, amelyek titkosítást alkalmaznak. A szombati terrortámadást követően nemzetközi együttműködést sürgetett az extrémizmus online terjedésének feltartóztatásához. **Bővebben...**

Kiberbiztonságon innen és túl

(www.forbes.com)

A közeljövőben új szabályzások várhatók a megnövekedett kiberbiztonsági kockázatokat ellensúlyozandó, amilyen az európai polgárok személyes adatainak védelmében, 2018. során hatályba lépő GDPR rendelet is. A vállalatok számára a megfelelőség biztosításán túl azonban többre van szükség: átfogó koncepcióváltásra. Ennek megfelelően a korábbi gyakorlattal szemben a hálózatbiztonság mellett új szempontok érvényesítése is kulcsfontosságú lesz, úgy mint az adatok titkosítása, a hozzáférések korlátozása és az adatok nyomonkövethetőségének biztosítása. **Bővebben...**

A sikeres adathalász támadások okai

(www.threatpost.com)

Egy német egyetemi hallgatókból álló csoport a közelmúltban készített tanulmányt a célott adathalász támadások sikerességének okairól. A felmérés egyrészt megmutatta, hogy a sikeres támadások hátterében a felhasználók kíváncsisága, illetve a hamis biztonságérzetük áll. Az is kiderült, hogy a dolgozók sok esetben azért hagyják figyelmen kívül az e-mailekre vonatkozó biztonsági előírásokat, mert minél gyorsabban szeretnék feldolgozni a kapott üzeneteket. **Bővebben...**

Alkalmazásvédelmi trendek

(www.helpnetsecurity.com)

2017. első negyedévére az 'Inforsecurity Europe 2017' eseményen a High-Tech Bridge összefoglaló jelentést adott ki az alkalmazás biztonsági trendekről. A nyílt forrásból származó adatok elemzése alapján megfigyelhető, hogy a magán és a közszférában is hasonló gondokkal küzdenek. A jelentés kitér a magas kockázatú biztonsági résekre, valamint a mobilalkalmazások, a webes interfészek és az ember okozta kockázatok súlyosságára is. **Bővebben...**

Az elkövetkezendő 5 év során 8 trillió dolláros kárt okozhat a kiberbűnözés

(www.welivesecurity.com)

A Juniper Research kutatása szerint világszerte növekvő kockázatot jelent az egyre szélesebb körben elérhető internet-hozzáférés, valamint a nem megfelelő vállalati biztonságpolitika. A 2017-2022-ig tartó időszakra vonatkozó kiberbiztonsági trendekről készült kiadványuk 2017. során mintegy 2,8 milliárd személyes adat ellopását jósolja, amely 3 évvel később megduplázódik. A jelentés emellett kitér arra is, hogy a vállalatok nem minden esetben hajtják végre megfelelően az új és régi rendszerek integrációját. **Bővebben...**