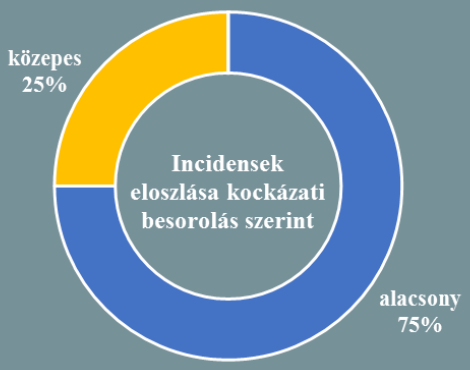
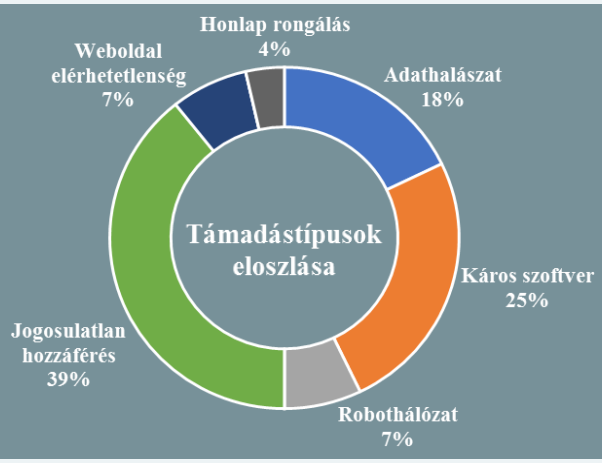
Nemzetközi IT-biztonsági sajtószemle

Incidens adatok:
2017.08.02. — 2017.08.08.





Célkeresztben Németország

(www.csoonline.com)

A Bitkom (Németország digitális iparági egyesülete) elemzése szerint a német vállalkozások mintegy fele (53%) már esett áldozatául gazdasági kiberkémkedésnek, ami évente összesen közel 55 milliárd eurós kárt okoz. Egy lényeges mutatószám szerint a válaszadók 62%-a jelezte, hogy történt olyan incidens, amely belső alkalmazotthoz köthető. A német Szövetségi Alkotmányvédelmi Hivatal (BfV) is közzétett egy összefoglalót, amely a 2016-os évre vonatkozóan veszi számba a főbb nemzetbiztonsági veszélyforrásokat. Ezek között jelenik meg a nemzeti hátterű kiberkémkedés, amely szerintük növekvő tendenciát mutat. Kiemelik Oroszország, Kína és Irán vezető szerepét a német érdekszférát érintő fenyegetésekben, amelyek sajátos motivációkkal bírnak. Míg Oroszország elsősorban saját politikai narratívájának terjesztését végzi, addig Kína fő érdeklődési körében az ipari technológiák, a kutatás és a fegyveres erők állnak, Irán pedig a kritikus infrastruktúrákra fókuszál, sok esetben kifejezetten szabotázs céllal. **Bővebben...**

Különösen sérülékeny a gyártóipar

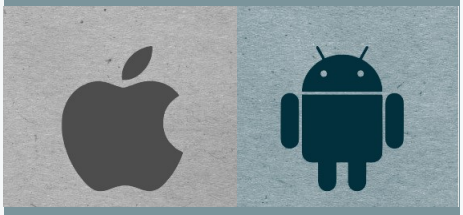
(www.helpnetsecurity.com)

A német NTT Security által kiadott 'Q2 Threat Intelligence' jelentés szerint a számítógépes támadások gyakorisága és kifinomultsága továbbra is növekvő tendenciát mutat világszerte. Az eredmények alapján a leginkább szembetűnő megállapítások: összességében 24%-kal nőtt a kibertámadások száma a második negyedévre; a támadások gyakorisága exponenciálisan nő, amint egy megvalósíthatósági példa (proof-of-concept) nyilvánosságra kerül; a malware támadások 67%-a adathalász e-mail üzeneteken keresztül ér célba, illetve hogy a gyártóipar még mindig kiemelt célpontnak számít. Az NTT Security szerint nagy probléma, hogy a gyártók rendszereiből a támadók képesek lehetnek az ellátási láncon keresztül akár a felhasználókat is elérni. Emellett aggasztó, hogy még mindig magas azon gyártók száma (37%), akik elismerték, hogy egyáltalán nem rendelkeznek incidenskezelési tervvel. **Bővebben...**

Egyenlőre nem lesz telefonos megfigyelés Ausztriában

(www.zdnet.com)

Az osztrák kormánykoalíció vezető pártja (SPÖ) vétót gyakorolt a telefonos online kommunikációk megfigyelését lehetővé tévő tervezet ellen. A koalíciós partner ÖVP elképzelése szerint a hatóságok felhatalmazást kaptak volna a mobil készülékekre történő kémprogramok telepítésére, nem csupán olyan személyek esetében, akiket minimum öt év szabadságvesztéssel büntetendő bűncselekménnyel gyanúsítanak, hanem kiterjesztették volna a velük kapcsolatban álló személyekre is. Az SPÖ indoklása szerint a javaslat túllépte a megállapodásuk kereteit és túl sok állampolgárt érintett volna. A 'Bundestrojaner' (szövetségi trójai) legkorábban 2019 augusztusától léphetett volna életbe, mivel az érintett szerveknél az üzemeltetéshez szükséges képesség még nem áll rendelkezésre. Szemben Németországgal, ahol az év végén már meg is kezdődhet az adatgyűjtés. **Bővebben….**



Mobil adathalászat - egy jelentős fenyegetés

(www.wandera.com)

Mobil eszközökkel kapcsolatban a malware-ek, az adatszivárgások és a közbeékelődéses támadások állnak az elemzések középpontjában, a Wandera új jelentése szerint azonban legalább ennyire jellemzőek az adathalász támadások. A kutatók egyes ismert adathalász domainek felé történő kommunikációk elemzésével megvizsgálták, hogy milyen típusú applikációkhoz és szolgáltatásokhoz volt köthető káros linkek terjesztésére. Eszerint elsősorban játékokat, levelezésre szolgáló, és sport alkalmazásokat, valamint hír és időjárás szolgáltatásokat használnak megtévesztésre. **Bővebben...**

IT biztonsági Tanács

A vállalat biztonsági stratégiájának tervezésekor vegyük figyelembe a belső fenyegetéseket is.

A jogosultságok kiosztásakor alkalmazzuk a legkissebb jogosultság elvét, emellett fontos a tervezett időközönkénti felülvizsgálat, hogy a már szükségtelen jogosultságok visszavonásra kerüljenek. A távozó munkaerő hozzáféréseit pedig minél előbb zároljuk.

Nagyobb kontroll a webes adatok felett

(www.thestar.com)

Új adatvédelmi törvényjavaslatot nyújtottak be Egyesült Királyságban, amely célja – összhangban az Európai Unió adatvédelmi stratégiájával – hogy a felhasználók nagyobb kontrollt gyakorolhassanak online személyes adataik felett. Ennek segítségével az olyan nagy tech cégekkel szemben, mint a Facebook vagy a Google könnyebben érvényesíthetik majd a személyes adataik törlését. Továbbá a vállalkozásoknak fel kell hagyniuk az ügyfelek online adatainak alapértelmezetten való gyűjtésével, hacsak nem kapnak tőlük erre vonatkozóan felhatalmazást. **Bővebben...**

Hiányosságok az ausztrál nagykövetségek védelmének kialakításában

(www.watoday.com.au)

A National Audit Office a tengerentúli ausztrál diplomáciai létesítményekre vonatkozóan végzett vizsgálatot külföldi titkosszolgálatok hírszerző tevékenysége, illetve adatszivárgások kapcsán. Ennek során többek között a stratégiai tervezéssel, a biztonsági intézkedések szervezésével, valamint a munkatársak képzésével kapcsolatban is hiányosságokat állapított meg. A jelentésben felsorolásra kerültek olyan esetek is, amikor az ausztrál Külügyi és Kereskedelmi Minisztérium (DFAT) az érzékeny, minősített adatokat sem kezelte megfelelően. A DFAT ugyan nem ért egyet valamennyi megállapítással, azonban a javaslatokat – köztük elsősorban egy átfogó stratégiai terv készítését – elfogadta. **Bővebben...**

Németországban betiltották a keyloggerek alkalmazását a munkahelyeken

(www.bleepingcomputer.com)

A német Szövetségi Munkaügyi Bíróság úgy döntött, hogy a vállalatok nem alkalmazhatnak keyloggereket az alkalmazottak megfigyelésére, mert az sérti a személyes adatok védelmét. 2015 áprilisában egy német médiaügynökségtől bocsátottak el egy fejlesztőt, mert munkaidőben magáncélú tevékenységet folytatott vállalati eszközökön. Az elbocsátást követően pert indított a cég ellen, ahol azzal is érvelt, hogy a billentyűleütések naplózásáról nem tájékoztatták előzetesen és ennek során személyéhez fűződő privát információkhoz (pl. jelszavak) is hozzáfértek, ezzel megsértve a magánszférájához való jogát. A bíró egyetértett a fejlesztővel, azonban megállapította, hogy vállalatoknak is lehetővé kell tenni az ilyen jellegű szoftverek használatát akkor, ha felmerül a gyanú a munkavállaló törvénysértő tevékenységet folytat. **Bővebben...**

Az ENISA töltené be a vezető kiberbiztonsági központ szerepét

(www.euractiv.com)

Az EU kiberbiztonsági ügynöksége (ENISA) átfogó javaslatot terjesztett az Európai Bizottság elé a kiberbiztonsági események hatékonyabb kezeléséhez. Ennek kulcs eleme, hogy az ügynökség nagyobb, központi koordináló szerepet játszana a kiberbiztonsági feladatok kapcsán. A javaslatok között szerepelt – az egységes szabályalkotás jegyében – egy dedikált szabványügyi koordinációs testület felállítása, emellett szükségesnek tartanak egy gyorsított eljárás bevezetését, amely lehetővé tenné a gyorsan fejlődő technológiák (például IoT eszközök, egyéb internetes termékek) kiberbiztonsági rangsorolását. Felvetik még annak a kérdését, hogy a vállalatok legyenek-e felelősségre vonhatók abban az esetben, ha nem jelzik az őket ért adatszivárgási incidenseket. **Bővebben...**