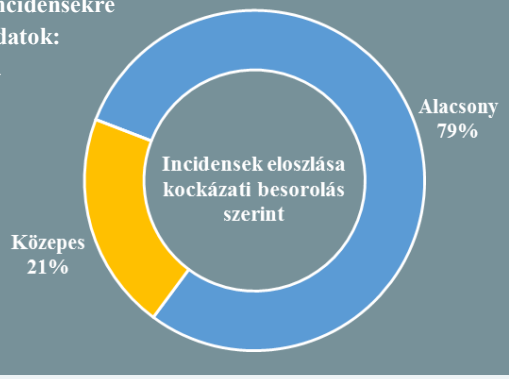
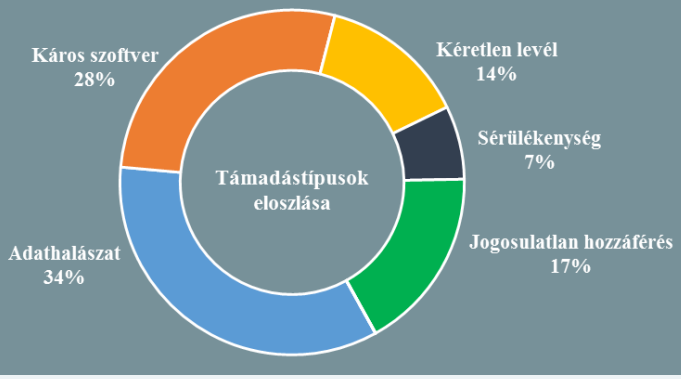
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.07.06. - 2018.07.12.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon, ahol naponta olvashatja legújabb híreinket!

A kiberbiztonság helyzete Észtországban

(www.ria.ee)

A 2017-es év sok kihívást tartogatott Észtország számára, például több millió felhasználói azonosító szivárgott ki, és az észt digitális állam is súlyos csapást szenvedett el az elektronikus személyi igazolványokkal kapcsolatos sérülékenységek miatt. Az elmúlt évben a hatóságok mintegy 11 000 kiberbiztonsági incidenst rögzítettek, ami harmadával több, mint az előző évi. A regisztrált esetek közül 122 biztonsági esemény volt létfontosságú rendszerekkel kapcsolatos, ám ez még mindig kevesebb, mint az elmúlt három évben bármikor. Összességében elmondható, hogy az azonosított kiberincidensek száma évről évre növekszik Észtországban, amely azonban több tényező eredménye. Az okok között említhető, hogy a bűnözők egyre inkább kihasználják a „digitális életstílust", emiatt egyre több a támadás, ezzel párhuzamosan a detektáló képesség is sokat fejlődött az országban, több vizsgálat pedig több találatot eredményez. Mindezek mellett azonban fontos kiemelni azt is, hogy a cégek egyre biztonságtudatosabbak, és egyre több anomáliát jelentenek. **Bővebben...**

Egy új véletlenszám-generátor megreformálhatja az internetbiztonságot

(www.phys.org)

Új szabadalom alapján készült az a kvantum véletlenszám-generátor (QRNG), ami a fejlesztők ígérete szerint amellett, hogy száz százalékosan megbízható kvantumalapú biztonságot nyújt az elektronikus kommunikáció során, végre alkalmas lesz a széleskörű felhasználásra is. A véletlen számok különös fontossággal bírnak az információtechnológiában, amely alatt azonban sok esetben ún. „álvéletlen" (pszeudo-random) számokat értünk, ám amikor a biztonság a tét, már tényleges véletlenszerűségre van szükség. A kvantummechanikán alapuló eddigi megoldások, bár komoly előrelépést jelentettek, különböző korlátozó tényezők – például a méretük, vagy az előállítás költsége – miatt az általános alkalmazásuk eddig nem volt lehetséges. A Quantum Base eszközének egyik előnye, hogy a hagyományos QRNG-khez képest jóval kisebb méretű, nagyobb sebességű, az integrálási költsége pedig rendkívül alacsony, így tökéletes megoldást jelenthet az okos eszközök biztonságossá tételéhez. **Bővebben...**

Brit-francia információ-technológiai együttműködési megállapodás született

(www.zdnet.com)

Az Egyesült Királyság és Franciaország kormánya múlt héten jelentette be a gyorsan fejlődő technológiák, mint például a mesterséges intelligencia (MI) fejlesztését és implementálását támogató együttműködési megállapodásukat, amely magában foglalja a kutatási és finanszírozási kezdeményezéseket, valamint a két ország közötti kiberbiztonsági kooperációt is. Egyes vélemények szerint Franciaországnak nagyobb megtérülést hozhat a konvenció, mivel az Egyesült Királyság a gépi tanulás és a mesterséges intelligencia fejlesztés terén már egy kiterjedt iparral rendelkezik. Az öt évre kiterjedő egyezség továbbá a két ország netsemlegesség iránti elkötelezettségét is rögzíti. **Bővebben...**

Úgy tűnik még a legkézenfekvőbb területen sem honosodott meg a biztonságtudatos felhasználói magatartás

(www.ibtimes.co.in)

A Kaspersky legutóbb a mobil készülékek biztonságával kapcsolatban végzett felmérést, amely aggasztó eredménnyel zárult. Azt találták ugyanis, hogy bár manapság a legtöbb ember a mobil készülékére hagyatkozik, amennyiben internetezésről, online bankolásról, e-mailezésről, vagy közösségi oldalon végzett aktivitásról van szó, a felhasználók kevesebb, mint fele (48%) védi készülékét jelszóval, és csupán 14%-uk titkosítja a készülékén tárolt adatait. Szintén rossz arány jelenik meg a biztonsági mentések tekintetében, ezzel mindössze 41% foglalkozik, lopás-elleni funkciókat pedig ennél is kevesebben (22%) használnak. A biztonsági szakemberek igyekeznek felhívni a felhasználók figyelmét arra, hogy mekkora kár érheti őket, amennyiben a készülék nincs ellátva legalább az alapvető biztonsági funkciókkal. **Bővebben...**

IT biztonsági Tanács

Az SPF (Sender Policy Framework) rekord lehetőséget biztosít az e-mailek hitelesítésére, és használatával lényegesen megnehezíthető, hogy rosszindulatú harmadik felek hamisított IP címek útján e-maileket küldjenek szervezetünket megszemélyesítve.

Az SPF rekord létrehozásával, valamint annak helyes beállításával kapcsolatban az eszkoztar.govcert.hu weboldalon talál segítséget.

Mennyire tartozik a kiberháború a katonaságra?

(www.isnblog.ethz.ch)

Myriam Dunn Cavelty, az ETH Zürich svájci technológiai intézet munkatársa legutóbbi publikációjában a kiberháború kérdéskörével foglalkozik, a tekintetben, hogy milyen fokú állami beavatkozás lehet elvárt egy ilyen esemény bekövetkezésekor, illetve hogy melyik szektor feladata a kihívásokkal való megbirkózás. A „kiberháború" kifejezést félrevezetőnek tartja, mert bár a kibertámadások mögött egyre gyakrabban jelenik meg politikai motiváció, illetve a kiberbiztonságot lassan egy évtizede már nemzetbiztonsági kockázatként tartják számon, az államok közötti kiberkonfliktusok alapvetően inkább hírszerzési jellegűek, ezért nem feltétlenül a katonaság hatáskörében kezelendőek. Az sem szól a hadsereg mellett, hogy az, mint biztonságpolitikai eszköz a kiber fenyegetések kezeléséhez sem jogi, sem műveleti szempontból nem rendelkezik elégséges kapacitással, szerepét elsősorban a saját rendszereinek védelmében látja. **Bővebben...**

Jelképes összegért árulták a Reaper drón kézikönyvét a Darkneten

(www.forbes.com)

A Recorded Future beszámolója szerint 150 és 200 dollár közötti értékben próbálták a sötét weben eladni az amerikai kormányzati ügynökségek használatában álló Reaper drón ellopott dokumentumait. Az elkövető a biztonsági cégnek elárulta, hogy egy ismert Netgear router sérülékenység kihasználásával szerzett hozzáférést a nevadai légierő-bázis Reaper állomásának egy kapitányához tartozó számítógéphez, ahonnan képes volt ellopni a Reaper karbantartási kézikönyveit, valamint egy listát azon pilótákról, akik vezérelhetik a drónt. Mindezt később további dokumentumok követték, amelyek például a rögtönzött robbanóeszközök hatástalanításával, vagy épp az M1 Abrams tank működtetésével kapcsolatban tartalmaznak leírásokat. A Recorded Future kutatója, Andrei Bareseyvich szerint ezek, bár nem voltak minősített anyagok, mégis rengeteg szenzitív katonai információt tartalmaztak, amelyek illetéktelenek – például terrorista csoportok – kezébe kerülve komoly károkat okozhatnak az amerikai haderőnek. **Bővebben...**

Mi az alapvető gond a Gmaillel adatvédelmi szempontból?

(www.protonmail.com)

A Gmailt-t legutóbb egy, a The Wall Street Journalben nemrég publikált cikk miatt érte komoly kritika, amelyben arra hívták fel a figyelmet, hogy külsős alkalmazás fejlesztők hozzáférést kapnak a Gmail ügyfelek e-mail üzeneteihez, a felhasználók tudta nélkül. A Protonmail blogján fejtette ki véleményét az esettel kapcsolatban. A biztonságos levelezési szolgáltatásáról híres cég szerint sajnálatos, hogy a cikk utáni vita kizárólag arra koncentrálódott, hogy a Google nem képes megfelelő felügyeletet alkalmazni a külsős applikáció fejlesztők által végzett tevékenységek felett, valamint hogy nem képes a biztonsági szabályoknak érvényt szerezni. Ezek ─ bár szintén fontos aggályok ─ elvonják a figyelmet a valódi problémáról, hogy a Google a felhasználók e-mailjeit a vállalat saját tulajdonaként kezeli, és az ügyfelek személyes információit profitszerzésre használja. Ugyan a sorozatos kritikák miatt a tech óriás 2017-ben közölte, hogy felfüggeszti a felhasználók mailboxainak az átvizsgálását, azonban azt már elmulasztotta nyilvánosságra hozni, hogy más cégeknek továbbra is engedélyezi mindezt. **Bővebben...**