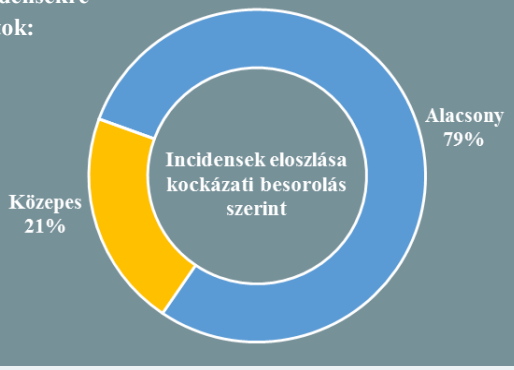
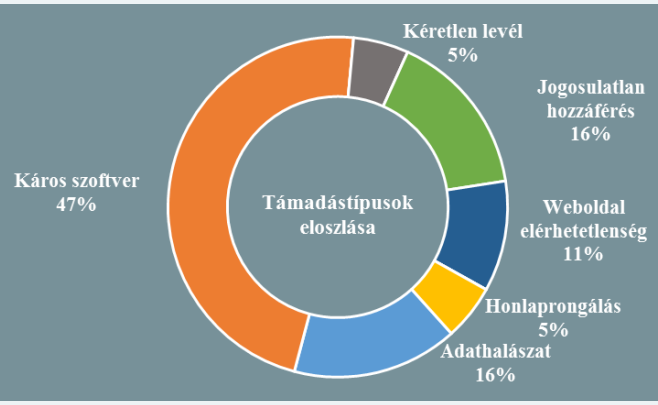
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2018. 19. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.05.04. - 2018.05.10.





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

Hivatalosan is önálló egység lett az amerikai kiberparancsnokság

(www.engadget.com)

A Pentagon kiberhadviselési egysége, a Cyber Command független katonai parancsnoksággá vált, melynek élére Paul Nakasone parancsnok került kinevezésre, aki egyúttal az NSA irányítását is átveszi. A szervezeti struktúraváltozás egy Integrált Kiber Központ létrehozására való felkészülés jegyében történt, ami az Egyesült Államok és a szövetséges nemzetek számára lehetővé fogja tenni a kibertámadásokra adott összehangolt válaszokat. Az új vezetéssel szigorodás várható az USA online fenyegetésekkel szembeni fellépésben, ugyanis Nakasone – egy márciusi meghallgatáskor tett nyilatkozata alapján – agresszívabb ellenintézkedéseket kíván tenni, függetlenül a támadások származási helyétől. **Bővebben...**

GDPR-t megkerülő megoldást kínál egy vállalat

(www.bleepingcomputer.com)

Nem minden vállalat kíván megfelelni az Európai Unió május végétől életbe lépő új általános adatvédelmi rendeletének (GDPR). A jellemzően kisebb árbevételű cégek – akik számára komoly anyagi kihívást jelent a megfelelőség kialakítása – sok esetben vagy abban reménykednek, hogy a szabálysértésük észrevétlen marad majd, vagy úgy döntenek, hogy inkább teljes egészében elhagyják az EU-s piacot. Egy cég ez utóbbiban felfedezve az üzleti lehetőséget, létrehozta a „GDPR Pajzs” elnevezésű szolgáltatást, amellyel a vállalkozások blokkolhatják a webes szolgáltatásaik EU-s térségből való hozzáférhetőségét. A havidíjas formában működő szolgáltatás elsősorban azon cégeknek lehet vonzó, akik saját maguk nem rendelkeznek az IP tartományok blokkolásához szükséges technikai tudással. Szakértők szerint az elkövetkező időszakban egyre több hasonló szolgáltatást nyújtó weboldal megjelenésére lehet számítani. **Bővebben...**

Még a szabályozók sem készültek fel a GDPR-ra

(www.reuters.com)

A Reuters hírügynökség olyan szervezeteket keresett meg, akik a május végén életbe lépő adatvédelmi rendelet kapcsán hatósági feladatot látnak majd el. Összesen 24 hatóság jelezett vissza, a válaszok alapján pedig az látszik kirajzolódni, hogy a felelős szervek nem rendelkeznek elegendő erőforrásokkal – többek között pénzügyi támogatással – hogy képesek legyenek elvégezni a feladataikat, egyes országokban ráadásul még az új szabályok a nemzeti jogba történő leképezése sem történt meg. Mindettől függetlenül a legtöbb válaszadó jelezte, hogy érdemben ki fogják vizsgálni a bejelentéseket, illetve proaktívan vizsgálják majd a megfeleléseket és a legsúlyosabb szabálysértéseket fogják szankcionálni. Arról azonban nem nyilatkoztak, hogy az erőforrás problémák vélhetően milyen feladatokra gyakorolnak majd leginkább negatív hatást. **Bővebben...**

A Google támogatja a biztonságos applikáció fejlesztést

(www.securityaffairs.co)

A tech cég nyilvánosságra hozta az Asylo névre keresztelt nyílt forráskódú fejlesztői platformját, mely a cég közleménye szerint lehetővé teszi az alkalmazások és az adatok bizalmasságának és integritásának megőrzését fejlesztéskor is. A keretrendszer az ún. megbízható végrehajtási környezet (trusted execution environment – TEE) felhasználásával biztosítja a teljes izolációt. **Bővebben...**

Az Android P szigorúbban kezeli majd a hálózati adatokat

(www.zdnet.com)

A Google a közeljövőben javít egy olyan biztonsági hibát, amely eddig lehetővé tette, hogy bármelyik applikáció monitorozza a hálózati aktivitást a felhasználó tudta nélkül. A probléma – bár a fejlesztők már egy éve tudnak róla – azonban csak az Android következő verziójában (Android P) kerül korrigálásra, azáltal, hogy a hálózatra vonatkozó információkat tároló /proc/net könyvtár hozzáférhetőségét néhány VPN alkalmazásra korlátozzák. Ugyanakkor a SELinux szabályokon eszközölt változtatást felfedező XDA Developers arra hívja fel a figyelmet, hogy 2019-ig a legtöbb app továbbra is eléri majd a hálózati adatokat, mivel csak ekkortól követelik meg az új (28-as) API szint használatát. **Bővebben...**

IT biztonsági Tanács

A biztonságtudatosság, a szervezeti kultúrába történő integrálásában a következők hatékony segítséget nyújthatnak:

- Lássuk el a fenyegetésekről elegendő információval a munkatársakat, így könnyebben magukénak érezhetik a biztonsági intézkedéseket.
- Ne retorziók kilátásba helyezésétől várjuk az eredményt – az incidens bejelentési hajlandóságra ez inkább kontraproduktívan hat – a cél a meggyőzés.
- Ne csak évi egy alkalommal tartsunk belső IT biztonsági képzést, hanem folyamatosan, és igyekezzünk azt minél inkább gyakorlatiassá tenni.

Titkosíthatóak lesznek a Twitteren küldött közvetlen üzenetek

(www.securityaffairs.co)

A „Secret Conversation”-re keresztelt új szolgáltatás végponttól végpontig terjedő titkosítás alkalmazásával teszi biztonságosabbá a platformon történő kommunikációt. Jelenlegi információk szerint azonban a titkosítás nem alapértelmezetten működik majd, hanem – a Facebook Messenger-éhez hasonlóan – a felhasználó üzenetküldéskor megválaszthatja majd, hogy titkosított üzenetet szeretne-e küldeni. Mindez jelenleg még teszt fázisban van és csupán néhány felhasználó számára érhető el. Ilyen például a Massachusettsi Egyetem egyik hallgatója, Jane Manchun Wong, aki elsőként adott hírt az újításról. A szakértő szerint a funkció a Twitter asztali verziójában nem lesz elérhető. **Bővebben...**

Az atommegállapodás felmondása kibertámadást indukálhat

(www.zdnet.com)

A Recorded Future szakértői szerint az atomalku felbontására Irán nagy valószínűséggel hónapokon belül – vagy ennél is hamarabb – nyugati országok, illetve egyéb nyugatbarát nemzetek (pl.: Szaúd-Arábia és Izrael) kritikus rendszereit célzó kibertámadással reagálhat. A kutatók szerint a fenyegetést az is jelentősen növeli, hogy ezeket a pusztító célú támadásokat az állam, mint megrendelő sem tudja könnyen ellenőrzés alatt tartani, ami az ország kiberműveleti modelljéből fakad. Teherán még 2009-ben a „Zöld Forradalom” után kezdte kiépíteni informatikai támadó képességeit, melynek során elsősorban anyagi motiváltságú fiatalok vállaltak munkákat, akikkel szemben azonban nagy volt a bizalmatlanság. Éppen ezért a struktúra úgy alakult ki, hogy egy központi, ideológiailag is motivált, megbízható csoport szervezi ki a részekre bontott feladatokat, miközben versenyezteti is a jelentkezőket. **Bővebben...**

Lejárt a NIS irányelv implementálására biztosított idő

(www.euractiv.com)

Május 9-én járt le az Európai Unió hálózatbiztonsági irányelvének (NIS Directive) azon határideje, ami a tagországok számára időt biztosított a szabályok a nemzeti jogba való átültetésére. A NIS többek között rendelkezik arról, hogy az alapvető szolgáltatásokat nyújtó szervezeteknek (víz-, energia-, közlekedés-, egészségügy- és banki szolgáltatók) tájékoztatniuk kell a kijelölt nemzeti hatóságokat a rendszereiket érintő kritikus kiberbiztonsági eseményekről. A jelentési kötelezettség elmulasztása pénzbírságot von maga után, aminek mértékéről a tagállamok döntenek. Eddig azonban mindössze az Egyesült Királyság hirdette ki az irányelv alapján megállapított összeget, aminek felső határa 19 millió font. **Bővebben...**

Kihirdették a netsemlegesség visszavonásának dátumát

(www.motherboard.vice.com)

A szabályok eltörléséről még tavaly decemberben határozott a Szövetségi Kommunikációs Bizottság (FCC), azonban ez ténylegesen csak június 11-től lép életbe. A hatályba lépéshez ugyanis az FCC-nek még ki kellett hirdetnie a döntést a kormányzati közlönyben, valamint egy formális jóváhagyásra is vártak az Igazgatási és Költségvetési Hivataltól, ám egyes vélemények szerint szándékosan késleltették a változtatást. Ettől függetlenül a Kongresszusban és a bíróságokon továbbra is határozott szándék mutatkozik a döntés elleni harcra. **Bővebben...**