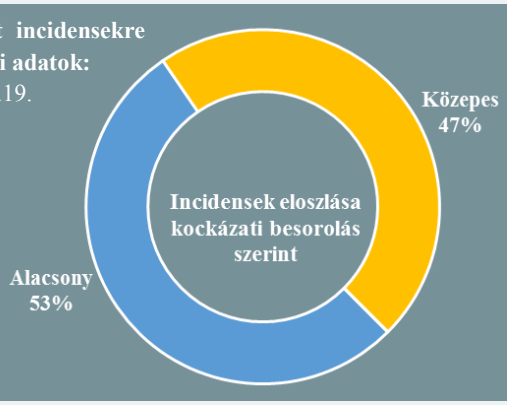
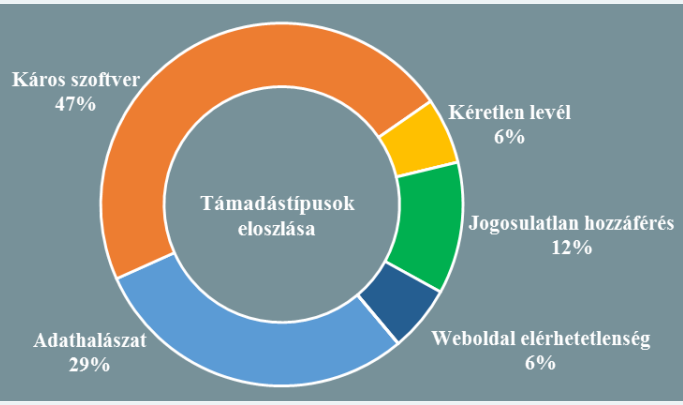
NEMZETI KIBERVÉDELMI INTÉZET
GOVCERT

Nemzetközi IT-biztonsági sajtószemle

2018. 51. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2018.12.14. - 2018.12.19.





Kövessen minket online az itbiztonsag.govcert.hu oldalunkon!

A Twitter szerint állami hackerek állhatnak egy nemrég felfedezett támadás hátterében

(securityweek.com)

Múlt hónap során a Twitter felfedezett egy biztonsági hibát az egyik online hibabejelentő űrlapjuk vonatkozásában, amelynek kihasználásával átmenetileg visszakereshető volt a felhasználók telefonszámának ország kódja, valamint megállapítható volt, hogy a fiók zárolt állapotban van-e. A Twitter ezzel kapcsolatos közleménye szerint miközben a hiba okának felderítésén dolgoztak, szokatlan forgalomra lettek figyelmesek az érintett form API-ját érintően, ugyanis nagy mennyiségben érkeztek kérések egyes kínai és szaúdi IP címekről. **Bővebben...**

Amerikai hadsereg: Nem akarunk kiber atombombát

(heise.de)

A kibertérben jelenleg szabályok nélkül folyik a hadviselés, és ezt a problémakört mindenképpen rendezni kellene – hangzott el egy Berlinben megrendezett konferencián. Tisztázni kellene számos fogalmat a kiberhadviselés terén – kezdve azzal, hogy pontosan mit jelent a „megtámadás" kifejezés –, ugyanis a vonatkozó normák, így a Genfi Konvenció szabályai sem adnak választ ezen kérdésekre. **Bővebben...**

Csehország is beállhat az USA mögé Huawei-ügyben

(securityaffairs.co)

A cseh kiberbiztonsági ügynökség (NCISA) közleményt adott ki, amelyben a Huawei és ZTE technológiák biztonsági kockázatára hívja fel a figyelmet. Az indoklás elsősorban a hatályos kínai politikai és jogi környezetre alapoz, miszerint a kínai vállalatoknak kötelezően együtt kell működniük az ország hírszerző szolgálataival. **Bővebben...**

IT biztonsági Tanács

Elérhető egy **pedagógiai kiberbiztonsági keretrendszer** (PCF — Pedagogic Cybersecurity Framework), amelynek célja segítséget nyújtani a kiberbiztonság nem programozási témaköreinek kategorizálásához és oktatásához. Mindehhez a hétrétegű eredeti OSI protokoll modellt újabb további 3 absztrakciós réteggel egészíti ki (szervezeti, kormányzati, nemzetközi), valamint ─ Glenn Surman 2002-es **munkája** nyomán ─ azonosítja a kapcsolódó főbb kockázatokat és sérülékenységeket.

Kibertámadás érte a francia külügy egy rendszerét

(securityaffairs.co)

Franciaország külügyminisztériuma közleményben tudatta, hogy hackerek illetéktelenül hozzáfértek az Ariane rendszer regisztrációs weboldalához, amelyen keresztül külföldi tartózkodások idejére biztonsági értesítésekre lehet feliratkozni. **Bővebben...**

Ezúttal Ukrajnát és NATO tagállamokat céloz az új APT kampány

(www.securityaffairs.co)

A Palo Alto Networks biztonsági szakemberei új, feltehetően az orosz érintettségű, hírhedt kiberkémkedési csoporthoz (APT28/Sofacy) köthető támadási kampányt fedeztek fel, amely a NATO tagállamok és Ukrajna kormányzati szerveit célozza. **Bővebben...**

Kibertámadások miatt adott ki figyelmeztetést a BSI német vállalkozások számára

(reuters.com)

A német Szövetségi Információs Biztonsági Hivatal ─ az Egyesült Államoktól származó információkra alapozva ─ figyelmeztetést adott ki egyes német vállalkozások számára, amelyek feltételezhetően kibertámadások célpontjaivá válhattak. **Bővebben...**