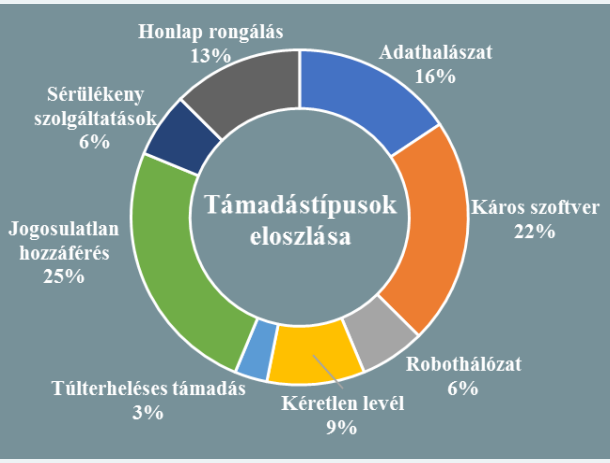
**Incidens adatok:**
2017.05.24. — 2017.05.30.





## A közösségi oldalakon is támadnak a hackerek

**(www.nytimes.com)**

Miközben a vállalatok és a kormányzati szervek világszerte egyre nagyobb figyelmet fordítanak az ismeretlen forrásból származó e-mailekkel kapcsolatos tudatosító tevékenységre, a hackerek egyre gyakrabban támadnak közösségi oldalakon keresztül, ahol a felhasználók nagyobb biztonságban érzik magukat. A Pentagon munkatársai kifejezetten tartanak attól, hogy egyes, állami támogatású hackerek Twitter és Facebook üzeneteken keresztül próbálnak meg hozzáférést szerezni a Védelmi Minisztérium számítógépes hálózatához, amire az utóbbi időben volt is példa. **Bővebben...**

## Sok fejtörést okoz a GDPR

**(www.helpnetsecurity.com)**

A GDPR adatvédelmi rendelet 2018. május 25-én lép hatályba, azonban a szervezetek nem állnak jól a felkészüléssel. A jogszabály többek között arról is rendelkezik, hogy a vállalatok hogyan gyűjtsék, tárolják, kezeljék és védjék az ügyfeleikre vonatkozó adatokat, ennek részeként a felhasználók számára lehetőséget kell biztosítani arra, hogy személyes adataik törlését kezdeményezhessék. Egy új kutatás szerint azonban a szervezetek már azzal kapcsolatban is komoly problémákkal küzdenek, hogy megállapítsák az ügyfeleikről tárolt adatok összes lehetséges előfordulási helyét. A felmérés szerint a szervezetek kb. 10-15% jelenleg nem képes ennek eleget tenni. **Bővebben…**

## Apple átláthatósági jelentés

**(www.cnet.com)**

2016. második felében megduplázódott (kb. 6000-re nőtt) az Egyesült Államok kormányzata által az Apple-höz intézett adatkérések száma, derül ki a cég féléves átláthatósági jelentéséből. Ilyen kérelmek a külföldi hírszerzési tevékenység megfigyeléséről szóló törvény (FISA) alapján, vagy nemzetbiztonsági célból bírói engedély hiányában is készülhetnek, ez utóbbi az ún. National Security Letter (NSL). Erről az érintett vállalatok nem közölhetnek információt, csak miután azok titkosítását feloldották. A tech cégek és civil jogvédő szervezetek régóta kritizálják a gyakorlatot, szerintük az ugyanis túl nagy hatalmat ad az FBI-nak. **Bővebben…**

## Amerikai tech cégek közösen lépnek fel az internetes megfigyelési gyakorlat ellen

**(www.cnet.com)**

USA-beli tech óriások (köztük Alphabet Inc., Facebook, Amazon, Microsoft) közösen kívánnak nyomást gyakorolni az amerikai kongresszusra, hogy változtatásokat eszközöljenek a megfigyelési törvény (FISA) még éppen hatályban lévő, de 2017. december 31-ével lejáró részével (Title VII) kapcsolatban. A törvény leginkább vitatott része (Section 702) lehetővé teszi az amerikai hírszerző ügynökségeknek, hogy külföldiekről nemzetbiztonsági céllal adatot gyűjtsenek. A nagy mennyiségű begyűjtött kommunikáció között azonban amerikai állampolgárok adatai is megtalálhatóak, amelyre a törvény nem ad felhatalmazást. Az iparág képviselői arra kérik a törvényhozó testületet, biztosítson nagyobb átláthatóságot, több biztonsági garanciát és kiterjedtebb bírói ellenőrzést javasolnak. **Bővebben…**

## Zsarolóvírus a mobilokon is

**(www.usa.kaspersky.com)**

A Kaspersky Lab szerint a zsarolóvírus támadások a mobil eszközöket sem kímélik, 2017. első negyedévében ugyanis megháromszorozódott a detektált zsarolóvírus fájlok száma (218,625). Az elmúlt hónapokban a biztonsági cég 11 új ransomware családot, illetve 55,679 új (legtöbb esetben a Cerber családhoz köthető) variánst azonosított. Ezzel együtt a detektált mobil támadások 45%-áért továbbra is egy káros kód a felelős (Trojan-Ransom.Androi dOS.Fusob.h). Az ilyen jellegű támadások ellen a tudatos internet használat, a védelmi szoftverek naprakészen tartása és a rendszeres offline biztonsági mentés készítése jelenthetik a legjobb védekezést, asztali és mobil platformon egyaránt. **Bővebben...**

## IT biztonsági tanács

A weboldalakba ágyazott kártevő kódok általában a rendszerek ismert sérülékenységeit használják ki a támadás során, ezért fontos a böngésző szoftverek naprakészen tartása.

A végpontvédelem kialakítása (tűzfal, vírusirtó), a böngészőkbe épülő biztonsági kiegészítők, hálózati tartalomszűrők és a frissítések alkalmazása csökkenthetik a káros weboldalak által hordozott kockázatokat.

## Még szigorúbbá vált a kínai kiberbiztonsági törvény

**(www.bloomberg.com)**

Egy héttel azelőtt, hogy 2017.06.01-jén hatályba lépne, újabb szigorításokat eszközöltek Kína új kiberbiztonsági törvényén. Egy korábbi módosítás már kibővítette az érintett cégek és szolgáltatások körét: azon szabályok, amelyek megtiltják az adatok Kínán kívülre való mozgatását eredetileg csak a kritikus infrastruktúrák szereplőire vonatkoztak, utóbb azonban hálózatüzemeltetők számára is kötelező érvényűvé tették, ami szinte bármilyen e-szolgáltatást és vállalatot érinthet. A törvény ezzel együtt leginkább a nagyobb külföldi tech cégeket sújtja, mivel, nagyobb az igényük az adatok külföldre mozgatására. **Bővebben…**

## Az egészségipar is tart a támadásoktól

**(www.securityweek.com)**

Egy új tanulmány szerint az orvosi eszközöket gyártó vállalatok 67%-a, orvosi szolgáltatást nyújtó intézmények (healthcare delivery organizations - HDO) 56%-a véli úgy, a gyártott/használt orvosi eszközök a következő 12 hónapban potenciálisan támadás áldozataivá válhatnak. A válaszadók mintegy egyharmada úgy érezte, egy ilyen támadás valamilyen negatív hatással lehet a betegellátásra, ennek ellenére nagyon kevesen voltak, akik jelentős lépéseket tettek a támadások kiküszöbölésére, az arány a gyártók esetében 17%, HDO-k esetében pedig mindössze 15% volt. Több, mint felük a sérülékenységek okaként a nem megfelelő minőségbiztosítást és tesztelést jelölte meg. **Bővebben…**

## Hitelesítés biometrikus fülhallgatóval

**(www.forbes.com)**

A biztonsági szakértők által javasolt kétfaktoros azonosítás egy új technológiája a biometrikus fülhallgató. A NEC által létrehozott fülhallgató esetében otoakusztikus emisszió segítségével történik a felhasználó azonosítása. A fülcsatornába küldött hangok hatására hang képződik a fülben, mely egy beágyazott mikrofonnal vizsgálja a visszapattanó hangok eltéréseit. **Bővebben…**

## A kockázatfelmérés fontossága

**(www.infosecurity-magazine.com)**

A müncheni ISACA EuroCACS konferencián a vállalatokat érő fenyegetésekről tartott előadást Raef Meeuwisse, a Cyber Simplicity igazgatója, amelyben a legnagyobb biztonsági kockázatot hordozó tényezőkkel foglalkozott. A Top 10-es listát a rosszindulatú programok vezetik. Konklúzióként arra hívta fel a figyelmet, hogy a vállalatoknak a kockázatelemzést sokkal komolyabban kell venniük. **Bővebben…**

## Egyre több a HTTPS adathalászati támadás

**(www.threatpost.com)**

A támadók egyre gyakrabban próbálják HTTPS protokollt alkalmazó webhelyekkel megtéveszteni az áldozataikat. Egy, a témával foglalkozó jelentés szerint a biztonságtudatosító képzések hatására a felhasználók ugyan egyre inkább megbíznak a HTTPS kapcsolatokban, ez azonban sajnos annyiban ki is merül, hogy a meglátogatott oldalon megjelenjen a "zöld lakat". A kutatók szerint egy másik probléma, ami felelőssé tehető a trendért, az olyan tanúsítvány kiállító cégek, mint a 'Let's Encrypt', amelyek ingyenesen állítanak ki tanúsítványokat, anélkül, hogy ellenőriznék az igénylőt. **Bővebben…**