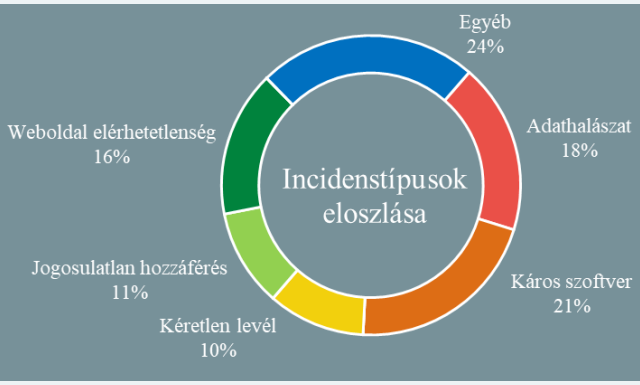
# Nemzetközi IT-biztonsági sajtószemle

2021. 48. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.11.26. - 2021.12.02.


**Kövessen minket weboldalunkon, ahol friss IT biztonsági hírek kerülnek publikálásra!**

## „Agresszív" adatgyűjtés miatt kapott bírságot az Apple és a Google

**(bleepingcompuet.com)**

Az Autorità Garante della Concorrenza e del Mercato (AGCM) olasz verseny- és piacfelügyeleti trösztellenes hatóság 10 millió eurós bírságot szabott ki a két techóriásra, a cégek „agresszív" adatgyűjtési gyakorlatai miatt, valamint amiért nem adnak egyértelmű tájékoztatást a személyes adatok kereskedelmi célú felhasználására vonatkozóan. Az AGCM által felhozott érvek szerint mindkét cég lényeges információkat hagy ki a felhasználói fiókok létrehozása során megismerhető adatkezelési tájékoztatóból arra vonatkozóan, hogy milyen adatokat gyűjtenek, és azokat hogyan használják fel. **Bővebben...**

## Ravasz technikával telepítenek káros kódokat Androidra

**(thehackernews.com)**

2021. augusztus és november között négy különböző banki trójai kampány terjedt a Google Play alkalmazásboltban, a különböző dropper alkalmazások (olyan telepítőcsomag, amely önmagában nem tartalmaz kártékony komponenst, azokat a telepítés után tölti le, így a támadók megkerülhetik a vírusvédelmi megoldásokat) több mint **300 000** fertőzést eredményeztek. A szóban forgó – kimondottan okostelefonokra tervezett – káros programok az **Anatsa** (más néven TeaBot), az

## Újabb funkcióval bővül a VirusTotal

**(securityaffairs.co)**

A VirusTotal bemutatta új szolgáltatását, a **VirusTotal Collections**-t, amely lehetővé teszi a regisztrált biztonsági kutatók számára, hogy megosszák egymással az általuk feltöltött fertőzöttségi indikátorokat (indicators of compromise – IoC). A biztonsági szakértők gyakran használnak különböző fórumokat tapasztalataik és az incidenskivizsgálások során általuk feltárt adatok, IoC-k megosztására, amit ezentúl a VirusTotal weboldalán is megtehetnek. **Bővebben...**

## Kibertámadás alatt az IKEA

**(bleepingcomputer.com)**

Az IKEA alkalmazottak közötti belső kommunikációt nehezíti az áruházláncot érintő, és jelenleg is folyamatban lévő kibertámadás, amelynek során a támadók egy egyszerű, de rendkívül veszélyes adathalász technikát alkalmaznak. A támadók a közelmúltban a ProxyShell és ProxyLogin sérülékenységek kihasználásával sikeresen feltörtek IKEA-s belső Exchange levelezőszervereket, és a belső hálózaton küldött, valódi e-mailek felhasználásával káros hivatkozást tartalmazó üzeneteket terjesztenek a dolgozók között. A technika (reply-chain, magyarul **válaszlánc támadás**) lényege, hogy a támadó egy kompromittált e-mail fiókról, egy valódi e-mailre válaszul küld káros tartalmat a célszemélynek. **Bővebben...**

## Mennyire kompromittálhatók a felhőszolgáltatások?

**(heise.de)**

Elérhetővé vált a Google biztonsági osztálya által készített Google Cloud Platform nemrég feltört 50 felhasználói fiókjának elemzésén alapuló jelentés, amely a felhőszolgáltatások kompromittálhatóságának okait vizsgálta. Eszerint a támadókat elsősorban a pénzszerzés motiválta, a felhasználói fiókok kompromittálódása pedig általánosságban a felhasználók hanyagsága miatt történt. Körülbelül az esetek felében **gyenge jelszavak**, illetve **hitelesítés nélkül használt API-k** tették lehetővé a támadást, a fiókfeltörések több mint negyede pedig harmadik féltől származó szoftverek biztonsági résein keresztül történt. **Bővebben...**

## IT biztonsági Tanács

Az NBSZ NKI weboldalán izgalmas karácsonyi kiberkihívásokról olvashat bővebben.