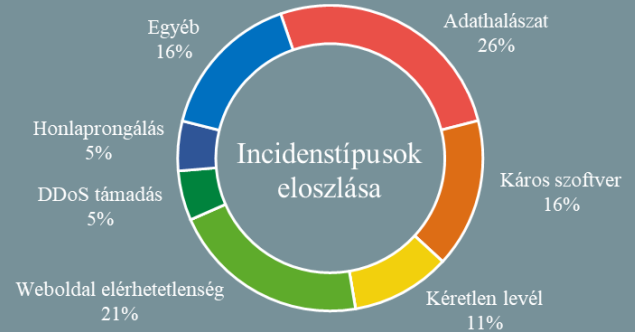


Az NKI által kezelt incidensekre  
vonatkozó statisztikai adatok:  
2021.08.06. - 2021.08.12.



Kövessen minket megújult [weboldalunkon](#), ahol friss IT biztonsági hírek kerülnek publikálásra!

## Kritikus infrastruktúrákat érintő TCP/IP sérülékenységeket fedeztek fel

([thehackernews.com](#))

A JFrog és a Forscout kutatói 14, az InterNiche Technologies vállalat NicheStack TCP/IP megoldását érintő sérülékenységet [fedeztek fel](#), amelyre összefoglaló néven **INFRA:HALT**-ként hivatkoznak. A népszerű TCP/IP implementációt beágyazott (IoT) eszközökön alkalmazzák jellemzően OT (Operational Technology), azaz gyártórendszerek területén, és kritikus infrastruktúrákban. Mivel a TCP/IP egy alacsony szintű protokoll, ezért a biztonsági rés súlyos támadásokra adhat módot, mint például: távoli kód futtatás, szolgáltatás megtagadás, adatszivárgás, TCP spoofing, és DNS cache poisoning. **Bővebben...**



## Több, mint 140 országban terjed egy androidos trójai vírus

([securityaffairs.co](#))

Zimperium szakértői egy új androidos trójai vírust [azonosítottak](#), amely Facebook fiókok feltörését végzi. A **FlyTrap**ként elnevezett káros kód 2021 márciusa óta már több, mint 10 000 áldozatot szedett, legalább 144 országban. A malware-t különböző csaló alkalmazásokon keresztül terjesztették a Google Play-en, ahonnan az eddig észlelt 9 káros app (lásd: lenti felsorolás) szerencsére már eltávolításra került, azonban nem hivatalos alkalmazásboltokon továbbra is megtalálhatóak. **Bővebben...**

## Több millió routert érint egy kritikus sérülékenység

([bleepingcomputer.com](#))

Néhány nappal ezelőtt a Tenable egy kritikus biztonsági hibát ([CVE-2021-20090](#)) [hozott nyilvánosságra](#) az *Arcadyan firmware*-t illetően, amely több tucatnyi különböző típusú konsumer és ISP-k által alkalmazott hálózati eszközön megtalálható. Az ún. *könyvtár bejárásos* sérülékenység sikeres kihasználása **illetéktelen hozzáférésre** adhat módot a támadó számára. A hiba legalább 10 éve megtalálható a szoftverben, így becslések szerint több millió eszköz is érintett lehet. **Bővebben...**

## Kubernetes biztonsági irányelvek az NSA-tól és a CISA-tól

([bleepingcomputer.com](#))

A Kubernetes egy közkedvelt szabadfelhasználású rendszer, ami a konténereken működő alkalmazások futtatását, skálázását és menedzselését automatizálja. Népszerűségéhez hozzájárul a könnyű kezelhetőség és rugalmasság. Elterjedtségéből adódóan azonban gyakran kiberbűnözők kedvelt célpontjává váik, főképp adatlopás, számítási-kapacitás lopás, és szolgáltatás megtagadás (DoS) keretében. Például egyre jellemzőbb, hogy a támadók kriptovaluta bányászatra használják a rossz védelemmel rendelkező Kubernetes szervereket. **Bővebben...**

## Mozilla Firefox 91 – sütitörles, ahogy kell!

([blog.mozilla.org](#))

A héten vált elérhetővé a Firefox böngésző 91-es verziója, amely többek közt újítást hoz a böngészési adatok alaposabb törlése érdekében. Miközben böngészünk, a weboldalak a böngészőn keresztül adatokat mentenek le az eszközünkre (ezek az ún. „süti”), aminek számos oka van. Ennek segítségével – csak néhány példát említve – tudunk bejelentkezve maradni egy weboldalon, a böngészők így „emlékeznek” az egyes oldalakra vonatkozó egyedi beállításokra. A süti azonban marketing célra is felhasználhatóak, hirdetési cégek ezek segítségével nyomon tudják követni, hogy milyen oldalakat látogattunk meg. **Bővebben...**

## IT biztonsági Tanács



Az NBSZ NKI [weboldalán](#) hasznos információkat olvashat az otthoni Wi-Fi routerek frissítésével kapcsolatban.