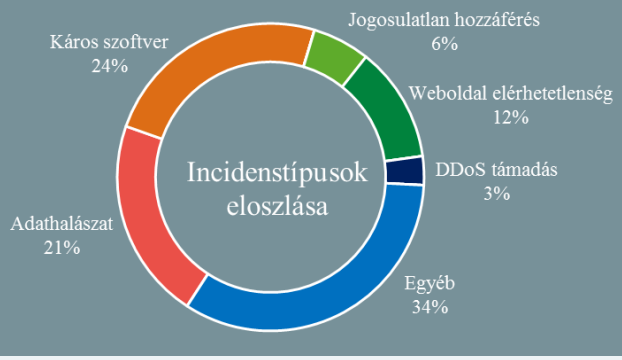
Nemzetközi IT-biztonsági sajtószemle

2021. 22. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.05.28. - 2021.06.03.



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

Legyünk óvatosak a digitálisan hitelesített PDF fájlokkal (is)!

(thehackernews.com)

A Ruhr-University Bochum kutatói két új veszélyes támadási technikát mutattak be a 42. alkalommal megrendezésre került IEEE Biztonsági és Adatvédelmi Szimpóziumon (IEEE S&P 2021), amelyek lehetővé tehetik rosszindulatú vagy megtévesztő tartalmak megjelenítését digitálisan hitelesített dokumentumokon. Az „**Evil Annotation Attack**” (EAA) és a „**Sneaky Signature Attack**” (SSA) névre keresztelt támadási módszerek a különböző szintű szerkesztési engedélyek rosszindulatú felhasználását mutatják be. Mint kiderült, nem csupán megjegyzésekkel juttatható káros tartalom egy már aláírt tanúsítvánnyal ellátott pdf dokumentumba (EAA), hanem a szabadon paraméterezhető aláírási elemek segítségével új, megtévesztő tartalom beszúrására is mód adódik (SSA). **Bővebben...**

Meghátrált a WhatsApp

(blog.malwarebytes.com)

A WhatsApp nem csupán a felhasználói közösségtől kapott hideget-meleget, amiért szűk egy hónapja bejelentették, hogy csak erősen korlátozott funkciókkal használhatják az appot azok, akik nem fogadják el az új adatvédelmi irányelveket, hanem egyes adatvédelmi hatóságok eljárást is indítottak ennek megakadályozására. A csevegő app friss közleménye szerint egyelőre mégsem tervez korlátozásokat, azonban időközönként figyelmeztetni fogja az érintett felhasználókat.

IT biztonsági Tanács

Az NBSZ NKI weboldalán egyszerű tippeket olvashat arról, miként védheti meg androidos eszközeit a hackerektől.

BIAS: Új Bluetooth sebezhetőségekre világítottak rá kutatók

(thehackernews.com)

Biztonsági kutatók nemrég olyan hiányosságokat fedeztek fel a Bluetooth Core és a Mesh Profile specifikációkban, amelyeket kihasználva támadóknak lehetőségük nyílhat úgynevezett „közbeékelődéses” (Man-in-the-middle) támadások végrehajtására. A **Bluetooth Impersonation AttackS** (BIAS) sebezhetőségek lehetővé tehetik kiberbűnözők számára, hogy egy másik eszközt megszemélyesítve kapcsolatot hozzanak létre az áldozat készülékével, megkerülve a Bluetooth hitelesítési mechanizmusát. **Bővebben...**

Kibertámadás érte a világ legnagyobb húsfeldolgozó vállalatát

(therecord.media)

A brazil JBS Foods a legnagyobb hústermelő vállalatának számít globálisan, amely a világ számos pontján működtet üzemeket, az Egyesült Államokon kívül például Ausztráliában, Kanadában, Egyesült Királyságban. A vállalat szűkszavú hétfői közleménye szerint a cég egyes ausztrál és észak-amerikai IT rendszereit „célzott kibertámadás érte”, azonban a biztonsági mentési rendszerek nem érintettek, és érzékeny adatok kompromittálódására utaló nyomokat mindeddig nem észleltek. **Bővebben...**

„Nukleáris memóriajáték” – avagy hogyan NE memorizáljunk belső eljárásrendeket!

(securityweek.com)

A szigorú katonai rezsimszabályok és biztonsági protokollok megjegyzése sokszor nem könnyű, hiszen esetenként intézkedések hosszú sorát kell fejben tartani. Márpedig egyes helyzetekben nem megengedett a hibázás, különösen, ha valaki éles nukleáris rakétatölteteket őriz. Ezért bizonyos szempontból érthető, hogy az Egyesült Államok hadseregének egyes katonái úgy érezték, egy kis memória tréning nem árthat, azonban a kivitelezés biztonsági szempontból hagyott „némi” kivetnivalót maga után. **Bővebben...**