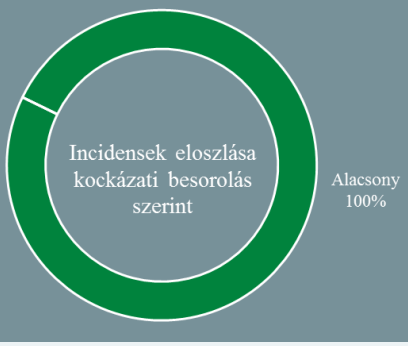
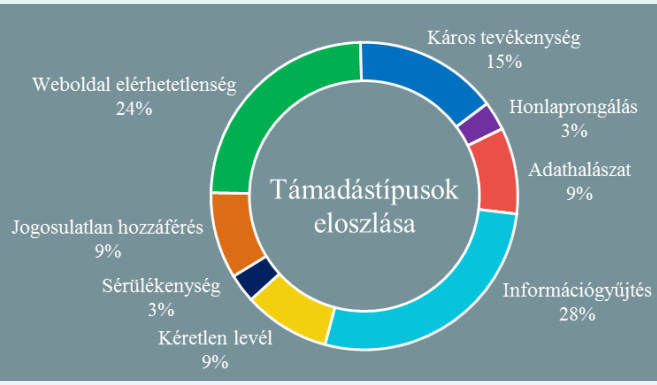
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 32. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.07.31. - 2020.08.06.





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

Súlyos hibát találtak a hivatalos WordPresses Facebook Chat pluginban

(wordfence.com)

A Wordfence biztonsági csapata egy súlyos sérülékenységet azonosított a The Official Facebook Chat Pluginban, amit több, mint 80 000 WordPress oldalon alkalmaznak. Ez az egyszerű bővítmény lehetővé teszi, hogy a WordPress oldalon megjelenjen egy Facebook chat ablak, aminek segítségével a látogatók kommunikálhatnak az oldal tulajdonosával, annak Facebook fiókján keresztül. A biztonsági rés azonban lehetővé tehette, hogy bárki csatlakoztassa saját Facebook Messenger fiókját bármelyik, sérülékeny plugint használó site-hoz és chatelni tudjon az érintett oldal látogatóival. Mindez lehetőséget adhatott arra, hogy egy támadó magát az oldal tulajdonosának adja ki a támadott oldalon megjelenő chat felületen, ezzel pedig potenciálisan érzékeny információkat csalhatott ki az áldozatoktól. **Bővebben...**

Android 8/9-en használ Twittert? Jobban teszi, ha frissíti az alkalmazást!

(zdnet.com)

A Twitter arra kéri androidos felhasználóit, hogy mielőbb frissítsék az alkalmazást, amennyiben azt Android 8 (Oreo), vagy 9 (Pie) verzión használják, ugyanis egy biztonsági rés lehetővé teszi, hogy más alkalmazások hozzáférjenek személyes Twitter adataikhoz, beleértve a privát üzeneteket (Direct Messeges) is. A biztonsági okokból nem részletezett sebezhetőség csak az Android nevezett két verzióját érinti, a Twitter webes felülete és az iOS-es változat nem sérülékeny. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a Windows 10 frissítések kapcsán felmerülő problémák javításáról.

Kínához köthető káros kódra figyelmeztetnek amerikai kormányügynökségek

(thehackernews.com)

Amerikai kormányügynökségek (CISA, FBI, DoD) közös tájékoztatóban hívják fel a figyelmet egy – feltételezések szerint kínai állami hackerek által – 2008 óta alkalmazott vírusra. A Taidoor malware az utóbbi évek során folyamatos fejlesztésen esett keresztül, azonban a fő támadási vektor alapvetően nem változott: a támadók megtévesztő e-mailek fertőzött csatolmányaként juttatják célba a malware-t. 2012-ben a tajvani kormányzat ellen fertőzött PDF csatolmányaként terjesztették, egy évvel később a támadók egy közbülső lépcsőként egy downloadert iktattak be a fertőzési folyamatba, tavaly pedig fertőzött Microsoft Word dokumentumokat használtak japán szervezetek ellen. **Bővebben...**

Adatszivárgás történt a Zellónál, kötelező a jelszócsere

(bleepingcomputer.com)

Adatszivárgás történt a Zellónál, amely egy 140 milliós ügyfélbázissal rendelkező digitális walkie-talkie alkalmazás. A cég 2020. július 8-án fedezte fel a jogosulatlan hozzáférést, amelynek során ismeretlenek hozzáférhettek Zello ügyfelek e-mail címeihez és hashelt jelszavaihoz. A cég közleménye szerint habár felhasználónevek nem érintettek ─ ügyfeleik pedig ritkán használják e-mail címüket felhasználónévként ─ elővigyázatosságból minden felhasználónál jelszócserét kényszerítenek ki. **Bővebben...**

Valószínűleg kifizette a rendszereit titkosító zsarolóvírus utáni váltságdíjat a Garmin

(bleepingcomputer.com)

2020. július 23-án zsarolóvírus támadás miatt vált elérhetetlenné a Garmin több szolgáltatása. Mintegy négy napos üzemkiesést követően a vállalat hirtelen bejelentette, hogy a szolgáltatások ismét elérhetőek, ám a szűkszavú nyilatkozatban a helyreállításról nem közöltek bővebb információkat. **Bővebben...**