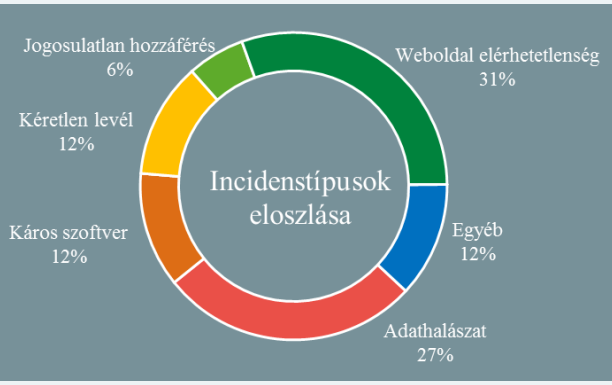
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 27. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.07.02. - 2021.07.08.



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

Kiberbiztonsági szempontból ezek a szervezetek által elkövetett leggyakoribb hibák

(cisa.gov)

Az amerikai kiberbiztonsági ügynökség (Cybersecurity and Infrastructure Security Agency – CISA) nyilvánosságra hozott két, kiberbiztonsági szempontból leggyakrabban tapasztalt rossz gyakorlatok (bad practices) közül. A legjobb gyakorlatok (best practices) mellett, a CISA összeszedi azokat a rossz gyakorlatokat is, amelyek jelentős kockázatot jelenthetnek, különösen a kritikus infrastruktúra szolgáltatókra nézve. Az egyik ilyen hiba, a már nem támogatott (end-of-life) szoftverek további alkalmazása, a másik pedig az alapértelmezett, kitudódott vagy állandó jelszavak használata. **Bővebben...**

Jól működő Android alkalmazások loptak Facebook jelszavakat

(thehackernews.com)

A Google 9 applikációt távolított el a Play Store-ból, miután felfedezték, hogy az alkalmazások ellopják a felhasználók Facebook jelszavait. Az alkalmazások funkcionalitásukat tekintve teljesen működőképesek voltak, viszont a teljes körű szolgáltatás eléréséhez, valamint az appon belüli reklámok blokkolásához arra kérték a felhasználókat, jelentkezzenek be Facebook fiókjukba. A Dr. web kutatóinak elmondása szerint egyes alkalmazások valóban tartalmaztak hirdetéseket, viszont ennek csupán az volt a célja, hogy ösztönözzék a felhasználókat a bejelentkezési művelet végrehajtására. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán a robothálózatokról (botnet) olvashat bővebb információkat.

Újra lecsapott a REvil – egy cégen keresztül további ezerötszázat bénítottak meg

(zdnet.com)

2021. július 2-án zsarolóvírus támadás érte a Kaseya vállalatot, majd a cég rendszerein keresztül több, mint 1500 kis- és középvállalkozást, a hírek szerint az eset hátterében az utóbbi idők leginkább aktív zsarolóvírus csoportja, a REvil áll. A Kaseya számos szervezet számára biztosít IT szolgáltatásokat, ügyfeleik között pedig olyan vállalkozások is megtalálhatóak, akik más cégek IT szolgáltatásait kezelik. A támadók a Kaseya egy népszerű távmenedzsment szoftverének (VSA) helyi telepítésű verziójának nulladik napi sérülékenységeit használták ki arra, hogy a zsarolóvírust juttassák a célrendszerekbe, amit frissítésnek álcáztak (Kaseya VSA Agent Hot-fix). **Bővebben...**

Biztonsági okokból erősebb gépekre van szükség a Windows 11-hez

(blogs.windows.com)

A Microsoft a közelmúltban jelentette be a jelenleg még készülő, de októberben már debütáló operációs rendszerének legújabb verzióját, a Windows 11-et. és ennek kapcsán közzétette azokat a rendszerkövetelményeket is, amelyek az operációs rendszer telepítéséhez lesznek majd szükségesek. **Bővebben...**

Chrome-ba is jön a HTTPS-Only mód, már tesztelhető is

(bleepingcomputer.com)

Bár hivatalosan még nem jelentették be az új funkciót ─ erre valószínűleg majd augusztus 31-én kerül sor ─ addig is a Chrome 93 Canary verziójában már kipróbálható a HTTPS-Only mód Mac, Windows, Linux, Chrome OS és Android rendszereken. A Google egy márciusi frissítésének köszönhetően a Chrome alapértelmezetten biztonságos HTTPS kapcsolatot alkalmaz azoknál a kereséseknél, amelyeknél a felhasználó nem adja meg a külön a használni kívánt protokollt az URL beírása során, a mostani újítás eredményeként pedig figyelmeztetni is fogja a felhasználókat arra, ha egy titkosítatlan weboldal meglátogatására készülnek. **Bővebben...**