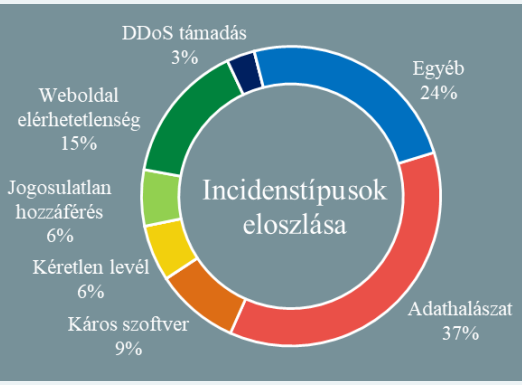
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 44. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.10.29. - 2021.11.04.



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

Már egy kattintással is jelenthetők a spam üzenetek Signalon

(bleepingcomputer.com)

Tavaly augusztusában a Signal lehetővé tette, hogy a felhasználók kapcsolatba léphessenek olyan felhasználókkal is, akik nem szerepelnek a névjegyzéklistájukban, és persze le is tilthatták az ilyen jellegű kéréseket. A most eszközölt módosítások során a Signal egyszerűbbé tette ennek folyamatát, ugyanis már az üzenetkérési panelen kiválasztható a „Spam bejelentése és blokkolása” opció. Mikor valaki erre a lehetőségre kattint, az eszköz elküldi a bejelentett üzenet feladójának telefonszámát és üzenetazonosítóját a Signal szervereinek. **Bővebben...**

Óriási Android frissítési csomag a Google-től

(securityaffairs.co)

A Google 2021. novemberi biztonsági frissítése az Android keretrendszer, illetve a rendszerelemek 18 sérülékenységét és még további 18 kernel szintű és gyártói komponensekben található sebezhetőséget javít. Az egyik ilyen befoltozott biztonsági rés például a CVE-2021-1048-as számon bejegyzett, kernelben található UAF (user-after-free) sérülékenység, amely kihasználásával kiterjeszthető a jogosultság a célzott rendszerben. A Google nem közölt technikai részleteket a sebezhetőségről, ámbár tisztában van annak korlátozott és célzott kihasználhatóságával kapcsolatban. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat arról, hogy mi a teendő, ha elveszítjük vagy ellopják okostelefonunkat.

A Trojan Source támadási módszer lehetővé teszi a hibák elrejtését a forráskódban

(securityaffairs.co)

A kutatók egy új támadási módszert dolgoztak ki “Trojan Source” néven, amely lehetővé teszi a sebezhetőségek elrejtését egy szoftver forráskódjában. A technika kihasználható láthatatlan kártevők bejuttatására, anélkül hogy a forráskód szemantikáját befolyásolná, miközben megváltoztatja annak logikáját. Ez a támadás a szövegkódolási szabványok (Unicode) tulajdonságait használja ki, hogy olyan forráskódot állítson elő, amelynek tokenjei logikailag más sorrendben vannak kódolva, mint ahogyan megjelennek. **Bővebben...**

A Microsoft teljeskörű kiberbiztonsági felügyeletet biztosítana az otthoni felhasználóknak

(bleepingcomputer.com)

Az elmúlt években a Microsoft inkább a vállalati biztonságra helyezte a hangsúlyt, azonban úgy tűnik ez a közeljövőben változni fog. A cég ugyanis azon dolgozik, hogy a felhasználók egyetlen dashboardról felügyelhessék az otthoni hálózatra csatlakoztatott különböző digitális eszközeik biztonsági állapotát. A Microsoft Store-ban múlt héten megjelent Microsoft Defender Prewiev nevű alkalmazás jelenleg csak Microsoft platformok felügyeletére szolgál, azonban a Bleeping Computer szerint a tech óriás Android, iOS és macOS rendszerekkel is kompatibilissá szeretné tenni. **Bővebben...**

A digitális identitások kezelése a szervezetek számára egyre nagyobb problémát jelent

(itsecurityguru.org)

A digitális identitások számában ugrásszerű megemelkedés tapasztalható, amelynek mendezselése a szervezetek számára komoly kihívást jelent — derül ki a One Identity felméréséből. (A digitális idenitás egy komplex fogalom, ami alatt alapvetően olyan adatkészleteket értünk, amely valakit — vagy valamit — azonosíthatóvá tesz (Fehér, 2014).) **Bővebben...**