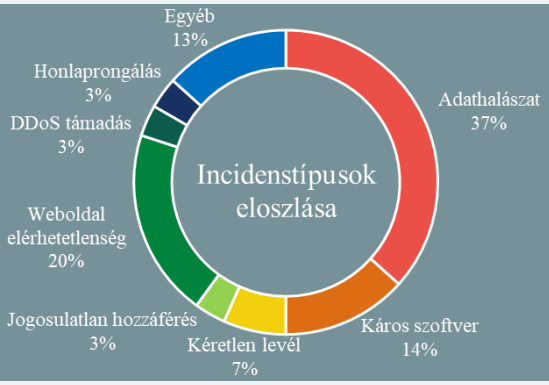
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2022. 18. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2022.04.29. - 2022.05.05.



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

Biztonsági csomagellenőrző eszközt adott ki az OpenSSF, lássuk mire lehet használni

(thehackernews.com)

A nyílt forráskódú programkönyvtárak rosszindulatú használata komoly biztonsági kitettséget jelent, és az elmúlt időszakban nem is egy olyan esetre derült fény, amikor fejlesztőket káros kódot tartalmazó csomagokkal támadtak. Az Open Source Security Foundation (OpenSSF) nemrég bejelentett új eszköze erre a problémára szeretne megoldást nyújtani, a Package Analysis ugyanis képes dinamikus elemzést végezni – a szoftverek nyílt forráskódját tároló – népszerű repository-kba feltöltött szoftvercsomagokon. **Bővebben...**

Androidosok figyelem: fontos biztonsági frissítés érkezik!

(heise.de)

Kritikus sérülékenységetfoltoz be az Android májusi biztonsági javítása. A frissítések az **Android 10, 11, 12** és **12L** verziókhoz érhetőek el. A CVE-2021-35090 számmal fémjelzett, kritikus biztonsági rés a Qualcomm zárt forráskódú összetevőjében található. A Google figyelmeztetése szerint a további biztonsági rések nemcsak a rendszert, hanem a keretrendszert és a kernelt, a MediaTek és a Qualcomm összetevőit is érintik. A legtöbb esetben a támadók magasabb felhasználói jogokat szerezhetnek. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán megtudhatjuk, hogyan törölhetünk még több személyes adatot a Google keresőjéből.

Egyre inkább a kiberbűnözők célkeresztjébe kerül a Linux

(securityweek.com)

A Linux hosszú ideig az egyik legkevésbé támadott platform volt az informatikában, azonban ez úgy tűnik változóban van. Az utóbbi időben egyre több rosszindulatú szoftverrel találkozunk, amelyeket kifejezetten Linux rendszerek megtámadására terveztek. Ezek a rendszerek egyre népszerűbb célpontjai a támadóknak, mivel számos hálózat háttérrendszerét, IoT eszközök és más kritikus fontosságú alkalmazások alapjait szolgálhatják. Napjainkban a Linux operációs rendszerek és a rajtuk futó különböző alkalmazások elleni támadások majdnem olyan gyakoriak, mint a Windows rendszerek ellen irányulók. **Bővebben...**

Jelentős szigorításokat vezet be India a biztonsági események kezelésével kapcsolatban

(thehackernews.com)

Az indiai nemzeti hálózati vészhelyzeteket elhárító csoport, CERT-In több ponton is szigorított a felügyelete alá eső szervezetek incidenskezelési kötelezettségein. A legfontosabb változás, hogy a bejelentésköteles szervezeteknek ─ ide tartoznak például az IKT szolgáltatók, adatközpontok és a kormányzati szervek ─ hat órán belül be kell jelenteniük a kiberbiztonsági incidenseket. **Bővebben...**

Újabb adathalász kampánnyal vették célba a Twitter hitelesített felhasználóit

(bleepingcomputer.com)

Az elmúlt hetekben a BleepingComputer számos riportere kapott olyan adathalász e-mailt, ami látszólag a Twitter Verifiedtól – a Twitter fiók-hitelesítőtől – érkezett, és amelyben a fiók felfüggesztésével ijesztegetik a felhasználót. Ez a támadási típus meglepően sokszor vezet sikerre. A Twitter a fióknév melletti kék pipát tartalmazó jalvénnyel (badge) jelöli a hitelesített felhasználói fiókokat, ami azt jelzi, hogy az adott felhasználó személyazonosságát a platform ellenőrizte, megbízhatónak találta, illetve a fiók aktív. **Bővebben...**