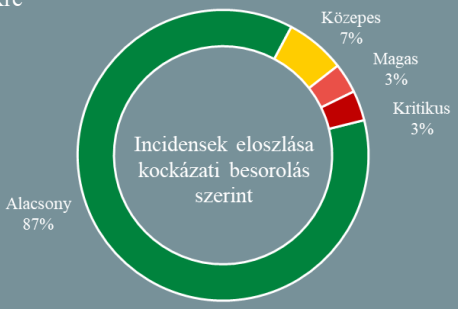
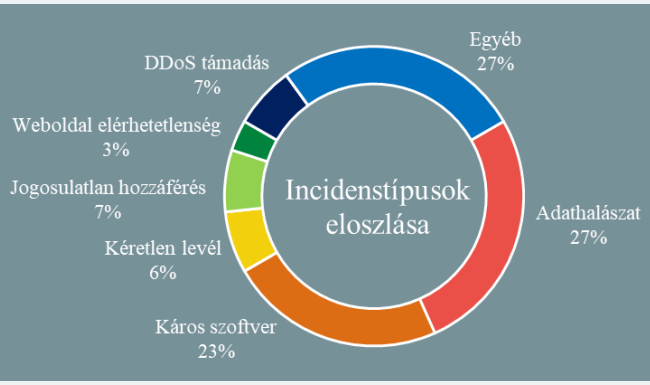
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 45. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.11.05. - 2021.11.11.





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

Ransomware támadás sújtotta a Media Marktot, 240 millió dollár a váltságdíj

(bleepingcomputer.com)

Zsarolóvírus támadás miatt vasárnap estétől hétfő reggelig álltak a Media Markt holland és német üzletágának egyes IT rendszerei, hogy megakadályozzák a zsarolóvírus továbbterjedését. Bár az online értékesítés zavartalanul működött, a helyi áruházakban több probléma is adódott, például nem lehetett bankkártyával fizetni, az eladások során pedig nem tudták kinyomtatni a vásárlást igazoló nyugtákat, illetve a termékek visszavétele sem működött, mivel a korábbi vásárlások nem voltak visszakereshetőek. **Bővebben...**

Androidos kémprogram szedi áldozatait Dél-Koreában

(securityaffairs.co)

A Zimperium zLabs kutatói fedeztek fel egy eddig kifejezetten dél-koreai felhasználókat célzó támadási kampányt, amelynek során az áldozatok eszközei egy új, kifinomult kémprogrammal fertőződnek meg, amely *PhoneSpy* névre hallgat. A PhoneSpy legitim alkalmazásoknak álcázza magát, például jóga, vagy TV-és videónéző appnak. A PhoneSpy több kémfunkcióval is bír, többek között a kamera elérésével képes fényképeket, videó felvételeket és hangot is rögzíteni, eléri a GPS helymeghatározási adatokat és a készüléken tárolt képeket, fájlokat is, valamint a fertőzött eszközökön távoli irányítást is lehetővé tesz a támadóknak, amivel manipulálhatják a hívásokat és SMS-eket. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán a Windows 11 biztonsági beállításairól olvashat bővebb információkat.

A CISA listázza azon sérülékenységeket, amelyeket az állami szervezeteknek javítaniuk szükséges

(securityweek.com)

Az Amerikai Egyesült Államok Kiberbiztonsági és Infrastruktúra-biztonsági Ügynöksége (CISA) nemrég nyilvánosságra hozott egy listát, amely aktuálisan körülbelül 300 olyan sebezhetőséget tartalmaz, amelyekről ismert, hogy aktívan kihasználják őket, és kötelező érvényű utasítást (BOD) adott ki, amelyben utasítja az amerikai kormányzati szervezeteket, hogy javítsák ki ezeket a biztonsági hiányosságokat. A listában olyan cégóriások termékei is megtalálhatóak, mint például az Apple, Google, Mozilla, WordPress és a Microsoft ─ a teljes lista elérhető itt. **Bővebben...**

Kritikus hiba érinti a Gitlabot, sokan mégsem frissítik

(thehackernews.com)

Kiberbiztonsági kutatók figyelmeztetnek, hogy a GitLab webes felületén egy kritikus sebezhetőséget találtak. Az említett biztonsági rést a CVE-2021-22205 azonosítón tartják számon, amely tetszőleges kód távoli futtatását teszi lehetővé. A sebezhetőséget, amely a 11.9-től kezdődően minden verziót érintett, a GitLab 2021. április 14-én, a 13.8.8, 13.9.6 és 13.10.3 verziókban javította. **Bővebben...**

Kritikus szektorokat vettek célba a kiberbűnözők, ezt a sérülékenységet használják ki

(securityaffairs.co)

A Palo Alto szakértői egy folyamatban lévő hackerkampányra figyelmeztetnek, amely a CVE-2021-40539 kihasználásával már több kritikus ágazatokból származó szervezetet veszélyeztetett, többek között a technológiai, védelmi, egészségügyi, energetikai és oktatási szektorokban. A sebezhetőség a Zoho ManageEngine ADSelfService Plus REST API URL-jeiben található, amely egy önkiszolgáló jelszókezelő és egyszeri bejelentkezési megoldás, kihasználása pedig távoli kódfuttatáshoz (RCE) vezethet. **Bővebben...**