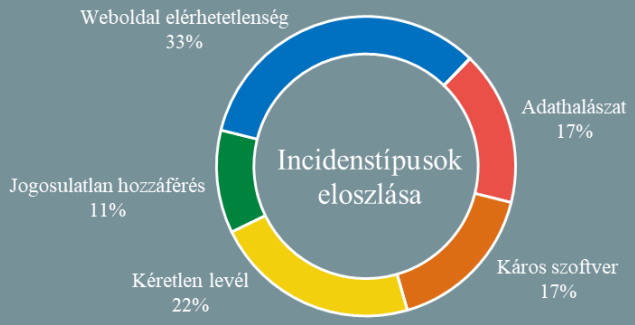
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2021. 46. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.11.12. - 2021.11.18.



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

EU digitális körkép – lassú növekedés és informatikai szakemberhiány a jellemző

(heise.de)

Megjelent a 2021-es Digitális Gazdasági és Társadalmi Index (DESI), amely az Európai Unió évente megjelenő, az országok digitális fejlettségét mérő mutatószámrendszere. Eszerint az elmúlt évben valamennyi tagállam előrelépést tett a humán tőke, a széles sávú kapcsolatok elérhetősége, a digitális technológia vállalati integrációja, valamint a digitális közszolgáltatások terén. Az EU-ban átlagosan az a lakosság mintegy 56%-a rendelkezik legalább alapfokú digitális készségekkel, az információs és kommunikációs technológiák (IKT) területén foglalkoztatott szakemberek száma pedig 8,4 millióra növekedett. **Bővebben...**

Ismét lecsap a GravityRAT Androidon

(bleepingcomputer.com)

Ezúttal „*SoSafe Chat*” végpontok közötti titkosítást ígérő android-alkalmazásnak álcázzák a GravityRAT néven ismert távoli elérésű trójai programot, amellyel jellemzően magas tisztségben álló indiai felhasználókat céloznak. A rosszindulatú program még 2020-ban egy bizonyos „*Travel Mate Pro*” nevű alkalmazással terjedt, azonban mivel a pandémia visszaszorította az utazási lehetőségeket a támadók új köntösbe bújtatták a káros programot. Valószínűleg rosszindulatú hirdetésekkel, közösségi édia-bejegyzésekkel és azonnali üzenetekkel terjesztették a kártevőt, amely során feltehetően nagy szerepet játszott a sosafe[.]co[.]in weboldal is. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán a biztonságos Black Friday-ről olvashat bővebben.

Feltörték az FBI e-mail szerverét egy lejáratókampány miatt

(thehackernews.com)

Az Egyesült Államok Szövetségi Nyomozóirodája (FBI) szombaton megerősítette, hogy feltörték a szervezet egyik e-mail szerverét és ismeretlen elkövetők hamis figyelmeztető e-maileket küldtek ki az FBI nevében. Az „*Urgent: Threat actor in systems”* tárgyú hamis e-maileket az *eims@ic.fbi[.]gov* címről küldték ki és azt állították, hogy Vinny Troia biztonsági kutató felel a támadásért, aki ráadásul kapcsolatban áll a TheDarkOverlord nevű hackerszervezettel – szerepelt az e-mailben. Marcus Hutchins, a Kryptos Logic kutatója szerint a támadás Vinny Troia diszkreditálására irányult, miután a biztonsági kutató információkat tárt fel a TheDarkOverlord hacker kollektíváról könyvében. **Bővebben...**

Adathalászat a TikTokon – célpontban az influenszerek

(bleepingcomputer.com)

Egy új adathalász kampány van kibontakozóban a TikTok közösségi videómegosztó platformon, amely elsősorban az influenszereket, azok menedzsereit, a márkatanácsadókat és a produkciós stúdiókat célozza. Az Abnormal Security kutatói két hullámban érzékelték a támadásokat, először október 2-án, majd november 1-én, és valószínűsíthető, hogy hamarosan újabb hullámra lehet számítani. **Bővebben...**

WordPress adminok figyelem: ne dőljünk be a hamis zsarolásnak!

(bleepingcomputer.com)

Ez idáig közel 300 WordPress weboldal érintett abban a múlt hét végén kezdődött támadási hullámban, amely során a támadók zsarolóüzenetet jelenítettek meg a feltört weboldalakon. A támadók egy visszaszámlálót is elhelyeztek az oldalon, ezzel is sürgetve a webhelyek adminisztrátorait a váltságdíjként kért 0,1 bitcoin mielőbbi kifizetésére. Az egyik áldozat által felbérelt Sucuri kiberbiztinsági cég azonban hamar rámutatott, hogy a weboldalak **valójában nem kerültek titkosításra**. **Bővebben...**