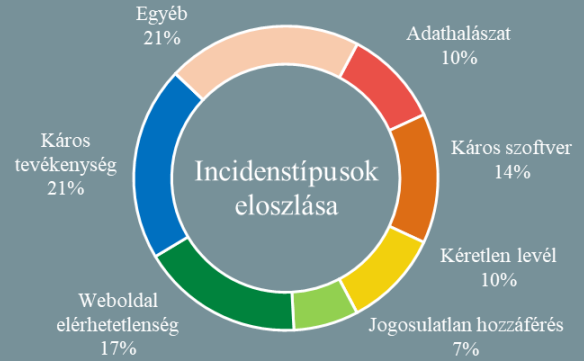


Az NKI által kezelt incidensekre
vonatkozó statisztikai adatok:
2022.05.06. - 2022.05.12.



Kövessen minket [weboldalunkon](#), ahol friss IT-biztonsági hírek kerülnek publikálásra!

A NIST frissítette az ellátási láncok biztosítására szolgáló útmutatóját ([securityaffairs.co](#))

Az amerikai Nemzeti Szabványügyi és Technológiai Intézet (NIST) frissítette az ellátási láncok védelmének megerősítéséhez korábban kiadott „Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations” című útmutatóját. A kiadvány célja, hogy segítséget nyújtson a vállalkozások számára a kockázatkezelési folyamatok és a védelmet erősítő kontrollok azonosításához, értékeléséhez, kiválasztásához és bevezetéséhez a teljes ellátási lánc tekintetében. **Bővebben...**

A legnagyobb tech cégek elkötelezték magukat a jelszómentes jövő mellett ([zdnet.com](#))

Lehet, hogy a jelszavakat hamarabb hagyhatjuk magunk mögött, mint gondolnánk. A Google, az Apple és a Microsoft legalábbis nagyot léptek előre ebben az irányban, ugyanis döntöttek arról, hogy platformjaikat (Android és Chrome; iOS, macOS és Safari; Windows és Edge) a jövő év során kompatibilissá teszik a FIDO jelszómentes szabványokkal. Mindez azt jelenti a gyakorlatban, hogy nemsokára ezeken a felületeken egyáltalán nem lesz szükség jelszavakra, ehelyett a telefonunkon tárolt FIDO jelszókulcs szolgál majd nem csupán a telefon feloldására, hanem automatikusan be is fogunk tudni jelentkezni a fiókjainkba. **Bővebben...**

Costa Ricán nemzeti vészhelyzetet rendeltek el Conti zsarolóvírus támadások miatt ([bleepingcomputer.com](#))

Elnöki beiktatása napján, 2022. május 8-án rendelt el Rodrigo Chaves elnök nemzeti vészhelyzeti szükségállapotot Costa Ricán, miután több kormányzati intézményt is Conti zsarolóvírus támadás ért. "A Costa Ricát ért, kiberbűnözők és kiberterroristák által indított támadások miatt a teljes Costa-ricai közszférára vonatkozóan nemzeti szükségállapotot rendelünk el, lehetővé téve társadalmunk számára, hogy bűncselekményként reagáljon ezekre a támadásokra" – mondta az elnök, Natalia Díaz elnökségi miniszter és Carlos Alvarado tudományos, innovációs, technológiai és távközlési miniszter társaságában. **Bővebben...**

HP firmware hibák került javításra, több mint 200 PC és notebook modell érintett ([bleepingcomputer.com](#))

A HP BIOS (UEFI firmware) frissítést adott ki két magas kockázati besorolású sérülékenységre (CVE-2021-3808, CVE-2021-3809) javításához, amelyek az érintett termékek esetében kernel szintű kódfuttatást tehetnek lehetővé. A sérülékenységekben érintett BIOS verziók között találhatóak üzleti kategóriás laptopok (például: Zbook Studio, ZHAN Pro, EliteBook, ProBook, Elite Dragonfly) és asztali gépek (EliteDesk, ProDesk), sőt kiskereskedelmi PoS (Point of sale) számítógépek is, mint például az Engage. A teljes lista megtalálható a HP biztonsági közleményében. **Bővebben...**

Kritikus távoli kódfuttatási hibát találtak az F5 BIG-IP eszközeiben, exploit is ismert ([bleepingcomputer.com](#))

Biztonsági kutatók figyelmeztették az F5 BIG-IP adminokat, hogy azonnal telepítsék a legújabb biztonsági frissítéseket, miután exploitok váltak elérhetővé a nemrég nyilvánosságra hozott kritikus RCE (CVE-2022-1388) sebezhetőséghez. A hiba a BIG-IP iControl REST hitelesítési komponensét érinti, és lehetővé teszi a hitelesítés megkerülését, és az emelt jogosultságokkal történő parancsvégrehajtást. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI [weboldalán](#) megtudhatjuk, hogyan tudjuk könnyen nyomon követni a Windows registry változásokat.