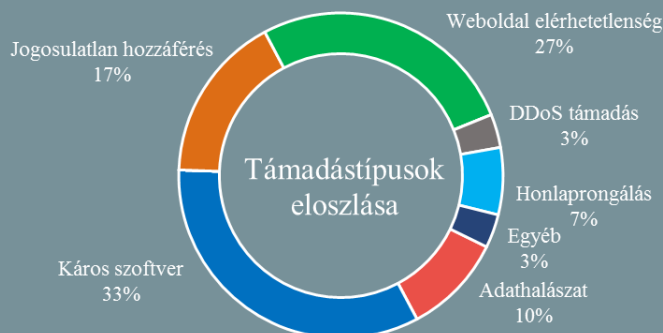


Az NKI által kezelt incidensekre vonatkozó statisztikai adatok:
2020.01.17. - 2020.01.23.



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

Citi bank ügyfeleket célzó adathalászkampány

([bleepingcomputer.com](#))

Egy Citi bank ügyfeleket célzó szofisztikált adathalászkampányt [azonosított](#) a MalwareHunterTeam. A kampány fő veszélyessége egyrészt abban rejlik, hogy a csaló weboldal igazán megtévesztő: arculati elemeiben hűen utánozza a Citi bank valós weboldalát, emellett TLS tanúsítványt, illetve az eredetire hasonlító domain nevet (update-citi[.]com) használ. Azonban ha mindez nem volna elegendő, az adathalász oldal a BleepingComputer szerint képes lehet a kétfaktoros hitelesítést is kijátszani. Az áldozat által megadott felhasználói adatok birtokában ugyanis a háttérben a Citi bank szerverétől kikényszeríti az egyszer használatos jelszó (OTP – one time password) kiküldését az ügyfélnek. **Bővebben...**

Az Opera védi az androidos rablóhitelek alkalmazásait

([cnet.com](#))

Az Opera visszautasította a Hindenburg Research jelentésében elhangzott vádakat, miszerint a böngészőgyártó egyes rövid lejáratú hitelek nyújtására szolgáló alkalmazásai megsértik a Google Play Store irányelveit. A kifogásolt appok jellemzően harmadik világbeli országokban érhetők el, az OKash és OPesa például Kenyában, a CashBean Indiában, az OPay pedig Nigériában. A jelentés szerint az alkalmazásokon keresztül nagyon rövid lejáratú – 15 napos – kölcsönöket kínálnak, amelynek alátámasztására az Opera pénzügyi vezetőjét is idézik, aki korábban azt nyilatkozta, hogy a vállalat által adott hitelek átlagosan két hét időtartamra szólnak. **Bővebben...**

A NATO hibrid hadviselési egységet létesített Montenegróban

([securityaffairs.co](#))

NATO Katonai Bizottságának (NATO MC) elnöke bejelentette, hogy a szövetség létrehozta az első hibrid hadviselési egységét Montenegróban, amelyre többek között az ellenséges orosz tevékenység miatt volt szükség. Szakértők attól tartanak, hogy Oroszország a 2020 októberi montenegrói parlamenti választások befolyásolására tör majd. Nem alaptalan a félelem, hiszen a balkáni ország 2016-os választásakor masszív támadás ért egyes állami intézményeket, ami egy évvel később, a NATO csatlakozás évében is megismétlődött. **Bővebben...**

Elkészült az adatvédelmi keretrendszer 1.0-s verziója

([securityaffairs.co](#))

A Nemzetközi Szabványügyi és Technológiai Intézet (NIST) közzétette [Adatvédelmi keretrendszerének első verzióját](#), amely – összhangban az adatvédelmi törvényekkel – segíti a szervezeteket az adatvédelmi kockázatok megfelelő kezelésében, kiemelt figyelmet fordítva az optimális adatkezelési gyakorlatokra, illetve a személyes adatok és az ügyfelek magánéletének védelmére. A keret három fő részből tevődik össze: az első, amely a kommunikációt és az adatvédelmi célkitűzéseket foglalja magában, a második, amely a tevékenységek, értékek és felmerülő kockázatok priorizálását teszi lehetővé, míg az utolsó rész a kockázat kezeléséhez szükséges erőforrások optimalizálásához nyújthat segítséget. **Bővebben...**

Internet Explorer használók veszélyben

([securityweek.com](#))

A Microsoft megkerülő megoldásokat [tett elérhetővé](#) egy ismertté vált, Internet Explorert érintő zero-day sérülékenységhez (CVE-2020-0674), amelynek kihasználásával távolról kód futtatható a célrendszeren. Egy web-alapú támadás kivitelezhető oly módon, hogy a támadó egy speciálisan szerkesztett weboldalt készít, majd az áldozatot rábírja ennek betöltésére. Amennyiben a felhasználó adminisztrátori fiókkal volt bejelentkezve, a támadó egy sikeres kihasználás során teljesen ellenőrzése alá vonhatja a megcélzott rendszert. **Bővebben...**

IT biztonsági Tanács



Az NBSZ NKI [weboldalán](#) hasznos információkat olvashat arra vonatkozóan, mely szempontokat érdemes figyelembe venni, egy adott kommunikációs szolgáltatás biztonságának értékeléséhez.