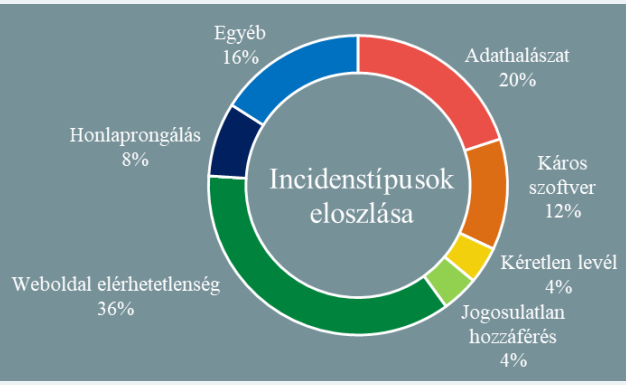
Nemzetközi IT-biztonsági sajtószemle

2021. 47. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2021.11.19. - 2021.11.25.



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

Figyelem: visszatért az EMOTET!

(bleepingcomputer.com)

Az EMOTET nem is olyan régen még a leggyakoribb számítógépes fertőzésnek (malware) számított, egészen tavaly év elejéig, amikor rendvédelmi szervek nemzetközi összefogással átvették az irányítást az EMOTET-et vezérlő szerverek felett, és két személyt letartóztatva megállították a botnetet. A Cryptolaemus jelzése szerint azonban ismeretlen fenyegetési szereplők most az EMOTET infrastruktúra újjáépítésén dolgoznak. **Bővebben...**

Több, mint 9 millió Huawei telefon lett vírusos

(thehackernews.com)

A Web Doctor hozta nemrég nyilvánosságra azt az androidos eszközöket célzó fertőzési kampányt, amelyben közel **9,3 millió eszköz** érintett. A Huawei saját alkalmazásboltjában összesen 190 játékapplikációt – köztük kimondottan orosz és kínai felhasználóknak szánt játékokat is – találtak a kutatók, amelyben azonosítani lehetett a **Cynos** nevű malware egy módosított verzióját. A fertőzött játékalkalmazások telepítését követően a program engedélyt kért a telefonhívások kezeléséhez, majd a jogosultág megszerzésével hozzáfért a telefonszámhoz, a készülék földrajzi helyzetéhez, mobilhálózati paraméterekhez és különböző rendszerinformációkhoz. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán a leggyakoribb e-mail küldési hibákról olvashat bővebben.

A nulladik napi sebezhetőségek millió dolláros piaca

(securityaffairs.co)

Az ún. nulladik napi exploitok – azaz a zero-day sebezhetőségek kihasználására szolgáló kódok, parancsok és módszerek – alapvető fegyvernek minősülnek a nemzetállami szereplők és kiberbűnözői csoportok arzenáljában. Az exploitok iránti megnövekedett kereslet egy többmilliós piacot táplál, ahol ezek a rosszindulatú kódok hihetetlenül drágák lehetnek. A Digital Shadows szakemberei egy érdekes kutatást tettek közzé "Vulnerability Intelligence: Do you know where your flaws are?" címmel (Sebezhetőségi Intelligencia: Ön tudja, hogy hol vannak a hibái?), amely rávilágított arra, hogyan működik a sebezhetőségek kihasználásán alapuló bűnözés. **Bővebben...**

Több, mint egymillió WordPress oldal adatai szivárogtak ki

(zdnet.com)

A WordPress nem csupán egy blog a sok közül, gyakorlatilag a nyílt interneten elérhető weboldalak közel fele (42%-a) ezen a platformon fut, ezért a tartalomkezelőt érintő biztonsági események kiemelt figyelmet érdemelnek. Az aktuális hír mintegy 1.2 millió felhasználó számára jelent biztonsági problémát, igaz ezúttal nem a WordPress, hanem az egyik legismertebb domain regisztrátor, a GoDaddy hibázott. **Bővebben...**

Súlyos sebezhetőségeket találtak OpenVPN alapú alkalmazásokban!

(securityweek.com)

A Claroty biztonsági kutatói figyelmeztetnek néhány súlyos kódfuttatási sebezhetőségre, amelyek az OpenVPN-re támaszkodó virtuális magánhálózati megoldásokat (VPN) érintik. A vállalat összesen négy biztonsági hibát dokumentált a **HMS Industrial Networks**, az **MB connect line**, a **PerFact** és a **Siemens** cégek egyes termékeiben, amelyek lehetővé teszik a támadók számára, hogy kódokat futtathassanak. **Bővebben...**