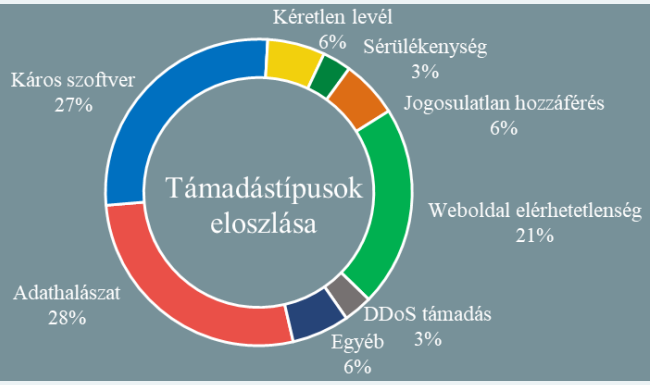
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 18. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.03.24. - 2020.03.30.



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

Zsarolóvírus támadások 2.0: ezekkel az intézkedésekkel csökkenthető a kockázat a Microsoft szerint

(bleepingcomputer.com)

A Microsoft fenyegetés elemző csapata arra figyelmeztet, hogy egyes kritikus szolgáltatások, mint például az egészségügy, fokozott veszélynek vannak kitéve a "human-operated ransomware", azaz a kiberbűnözői csoportok által célzottan irányított támadásokkal szemben. (A terminológiát a Microsoft vezette be, ami alatt — szemben a Wannacry-típusú, automatikusan terjedő vírusokkal — a célzottan, leginkább vállalkozások ellen alkalmazott, adatlopást és szenzitív adatok nyilvánosságra hozásával történő zsarolást is magában foglaló zsarolóvírus támadásokat értik.) **Bővebben...**

Vigyázat: sextortion zsarolóvírus terjed Androidon

(thenextweb.com)

"Black Rose Lucy"-nak hívják azt az új androidos zsarolóvírust, ami azzal igyekszik ráijeszteni áldozataira, hogy amennyiben nem teljesítik az 500 dolláros váltságdíj kifizetését — a támadók nem Bitcoin átutalást várnak, hanem bankkártyás utalást és a bankkártya adatok megadását —, a készüléken talált felnőtt tartalmakat eljuttatja a Szövetségi Nyomozó Iroda (FBI) kiberbűnözési részlegének. A zsarolóvírust a Check Point biztonsági kutatói fedezték fel, akik arra figyelmeztetik a felhasználókat, hogy a vírus különféle közösségi média olalakon terjed egy video streaming optimalizáló alkalmazásnak álcázva magát. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat az Egyesült Királyság által közzétett online oktatási platformról.

DNS biztonság: elindult az ingyenes deSEC szolgáltatás

(heise.de)

A berlini non-profit deSEC szervezet éles üzembe állította a DNSSEC szabványon alapuló DNS menedzsment szolgáltatását, amelynek célközönsége a kis- és középvállalkozások, valamint az egyéni felhasználók, akik mostantól például TLS tanúsítványokat, GPG kulcsokat vagy SSH lenyomatokat tehetnek közzé a deSEC-en kezelt domainjeik segítségével. A deSEC szolgáltatás létrejöttét a Let's Encrypt ihlette, célkitűzésük pedig a DNS biztonsági megoldásainak terjesztése. Míg a Let's Encrypt a HTTP böngészés kliens és szerver közötti kapcsolatát teszi biztonságosabbá ingyenes TLS tanúsítványokkal, addig a deSEC a DNS zónák DNSSEC-el történő aláírását teszi lehetővé, hogy védjen a domain nevekhez hozzárendelt IP címek manipulálásával szemben. **Bővebben...**

Sérülékeny Sophos tűzfalakat céloz egy új trójai

(bleepingcomputer.com)

Az Asnarök egy újonnan felfedezett trójai program, amellyel hackerek egyes Sophos tűzfalak nulladik napi sérülékenységét igyekeznek kihasználni, hogy hitelesítő adatokat szerezzenek. Az Asnarököt az elemzések szerint arra tervezték, hogy a tűzfalból olyan adatokat nyerjen ki, mint például licence kulcsok, szériaszámok, a létrehozott felhasználói fiókok adatai — köztük a titkosított jelszavak, e-mail címek — illetve a VPN kapcsolatok tekintetében kiemelt jogosultságokkal bíró felhasználók azonosítói. **Bővebben...**

Vízügyi SCADA rendszerek elleni kibertámadásokat hárított el Izrael

(securityweek.com)

Az izraeli kormányzat figyelmeztetést adott ki az ország vízügyi szervezetei számára, miután több vízügyi rendszer ellen is kibertámadást hajtottak végre. A támadásik célpontjában többek között szennyvíz tisztító létesítmények központi irányító (SCADA – Supervisory control and data acquisition) rendszerei álltak. **Bővebben...**