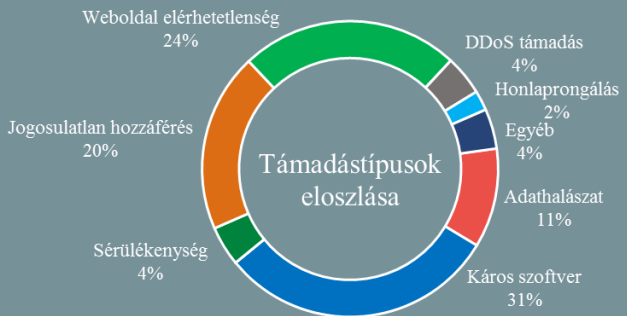
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 13. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.03.20. - 2020.03.26.



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

HR-esek vigyázat: az önéletrajz is rejthet káros kódot

(databreachtoday.co.uk)

A Prevailion új tanulmányában arra figyelmeztet, hogy a TA505-ként jegyzett kiberbűnözői csoport új kampányában önéletrajzoknak álcázott káros fájlokkal támad humán erőforrás (HR) részlegeket. *(A TA505 fenyegetési csoport több éve működik, és olyan jól ismert káros kódok terjesztése köthető hozzájuk, mint a Dridex banki trójai vagy a Locky és Jaff zsarolóvírusok. A káros kódok terjesztését eddig a nemrég lekapcsolt Necurs robothálózat segítségével végezték.)* **Bővebben...**

Lengyelország: mobil alkalmazással ellenőrzik a házi karantén betartását

(businessinsider.com)

A lengyel kormányzat múlt hét pénteken közreadott egy alkalmazást, amit a külföldről hazaérkezőknek a kötelező két hetes karantén alatt használniuk kell ahhoz, hogy igazolják: nem hagyták el a lakóhelyüket. Az érintettek választhatnak: vagy letöltik az alkalmazást, vagy számíthatnak rá, hogy véletlenszerű időközönként a rendőrség személyesen ellenőrzi őket. Akik az — Androidra és iOS-re is elérhető — alkalmazás („Home quarantine") mellett döntenek, időközönként szelfit kell készíteniük magukról, amit el kell küldeniük az applikáción keresztül. Amennyiben ezt elmulasztják megtenni 20 percen belül, a rendőrség automatikusan értesítésre kerül. **Bővebben...**

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat a videókonferencia (VTC — Video Teleconferencing) szolgáltatás biztonságos használatáról.

A telefonok nyomon követését javasolja egy ausztrál járványügyi kutató

(theregister.co.uk)

Marylouise McLaws, az ausztrál Közegészségügyi és Közösségi Orvostudományi Iskola professzora, aki – többek közt a WHO fertőzések megelőzésével foglalkozó egységének is tagja – szerint a fertőzött betegek tartózkodási helyének nyomon követése kulcsfontosságú szerepet játszott a járvány hatásainak mérséklésében. Ez több országban is megfigyelhető volt: így például Szingapúr, Tajvan és Dél-Korea esetében is. Szingapúrban, azon betegek számára, akiknek házi karanténban kellett maradniuk, a hatóságok előírták, hogy telefonjukon kapcsolják be a helymeghatározást, és időközönként kattintsanak rá egy SMS-ben érkező linkre, ami továbbította aktuális helyzeti adataikat. **Bővebben...**

Zyxel NAS-ok veszélyben: új köntösben csap le a Mirai botnet

(thehackernews.com)

Zyxel hálózati adattárolókat (NAS) és tűzfalakat céloz a Mirai botnet új variánsa, a „Mukashi". *(Az elsősorban IoT eszközökre veszélyes Mirai botnetnek 2016-os felfedezése óta újabb és újabb verziói látnak napvilágot, ami részben annak köszönhető, hogy kódja szabadon hozzáférhető bárki számára.)* A malware egy Zyxel eszközöket érintő kritikus sérülékenység (CVE-2020-9054) kihasználásával vonja irányítása alá a célkeresztben álló eszközöket, amelyeket ezután robothálózatba kapcsol. **Bővebben...**

Egyre több zsarolóvírust alkalmazó csoport készít adatszivárogtató weboldalt

(bleepingcomputer.com)

Újabb ransomware terjesztő kollektívák kezdték el nyilvánosságra hozni a nem fizető áldozatok privát adatait. Az első ilyen „hír oldal" a Maze zsarolóvírushoz köthető, később a Sodinokibi/REvil, Nemty, és a DoppelPaymer is felzárkóztak. A BleepingComputer most arra hívja fel a figyelmet, hogy az elmúlt két napban további három ransomware család követte a példájukat, a Nefilim, a CLOP és a viszonylag új Sekhmet. A trendet jól példázza, hogy a zsarolóvírus támadásokat miért is kell adatszivárgási incidensnek tekinteni.