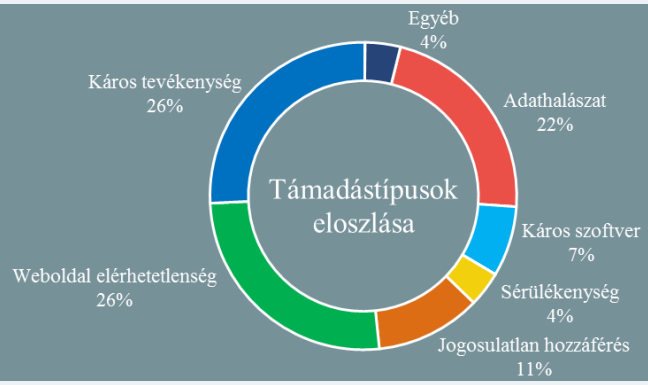
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2020. 30. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2020.07.17. - 2020.07.23.



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

ENISA felmérés az európai KKV-k kiberbiztonsági felkészültségének feltérképezéséhez

(enisa.europa.eu)

Az Európai Unió kiberbiztonsági ügynöksége (ENISA) online kérdőívet publikált a kis- és középvállalkozások kiberbiztonsági felkészültségi szintjének felméréséhez. A kérdőív arra keresi a választ, hogy a KKV-k saját megítélésük szerint milyen főbb kihívásokkal küzdenek, valamint mennyire képesek megbirkózni a leggyakoribb kiberfenyegetésekkel. A visszajelzések alapján kiadvány készül majd azon legjobb gyakorlatokról, amelyek segítségével a vállalkozások átvészelhetik a COVID-19 pandémiához hasonló krízishelyzeteket. A kérdőív innen érhető el szeptember 15-e 12:00-ig (CET).

Társkereső és közösségi oldalakról is lop személyes adatokat egy új androidos trójai

(bleepingcomputer.com)

A BlackRock nevet kapta az a veszélyes androidos banki trójai, amely hitelesítő adatokat és hitelkártya információkat is gyűjt több, mint 337 alkalmazásból. A rosszindulatú kódot még májusban fedezte fel a ThreatFabric, elemzésük szerint – a káros program forráskódja alapján – a LokiBot androidos trójai családhoz köthető. A BlackRock Google frissítésnek álcázza magát, telepítés után különböző *kisegítő lehetőségekhez* (Accessibility Service) kér jogosultságot, amelyek birtokában azután további jogosultságokat szerez, így nincs többé szüksége felhasználói inter-

IT biztonsági Tanács

Az NBSZ NKI weboldalán hasznos információkat olvashat miként állíthatja be a Magento.com oldalon a kétfaktoros azonosítást.

Zsarolóvírus támadás érte Argentína egyik legnagyobb telekommunikációs szolgáltatóját

(securityaffairs.co)

A REVil (Sodinokibi) zsarolóvírus kollektíva sikeres támadást hajtott végre a Telecom Argentina ellen, ami több, mint 18 000 munkaállomást érintett. A támadás július 18-án történt, amelynek során a támadók hozzáférést szereztek a vállalat belső hálózatához, irányításuk alá vonták az egyik domain admin fiókot, majd több ezer gépet titkosítottak. A ZDNet publikációjának elkészültekor a csoport dark webes szivárogtató oldalán még nem listázta a Telecom Argentinát, csupán a váltságdíj összegét közölték, ami nem kevesebb, mint 7,5 millió dollár értékű Monero kriptovaluta, ami nem fizetés esetén duplázódik. **Bővebben...**

Ismét kibertámadás ért izraeli vízügyi rendszereket

(securityweek.com)

Idén második alkalommal adott hírt vízügyi létesítmények elleni kibertámadásól az Izraeli Vízügyi Hatóság. A mostani incidens sok szempontból hasonló az áprilisihez, mivel ismét kisebb, helyi rendszerek álltak célkeresztben, és a SecurityWeek információi szerint mindkét támadás során ipari celluláris hálózati eszközök sérülékenységeit is kihasználták a támadók. Ezek belépési pontként szolgáltak, a támadók miután hozzáférést szereztek a célkeresztben álló hálózathoz, megpróbáltak károkozási célú módosításokat végezni az ipari vezérlőrendszerek legitim funkcióit felhasználva. **Bővebben...**

Megjelent az ENISA új stratégiája

(enisa.europa.eu)

Az Európai Unió Kiberbiztonsági Ügynöksége (ENISA) publikálta új stratégiáját (A Trusted and Cyber Secure Europe), a tavaly hatályba lépett európai kiberbiztonsági törvény (EU Cybersecurity Act – CSA) által támasztott elvárások teljesítéséhez. A dokumentum hét stratégiai célkitűzést fogalmaz meg az ENISA számára: jöjjenek létre kompetens és elkötelezett közösségek a kiberbiztonsági ágazaton belül; a kiberbiztonság váljon az EU-s irányelvek integráns részévé; stb. **Bővebben...**