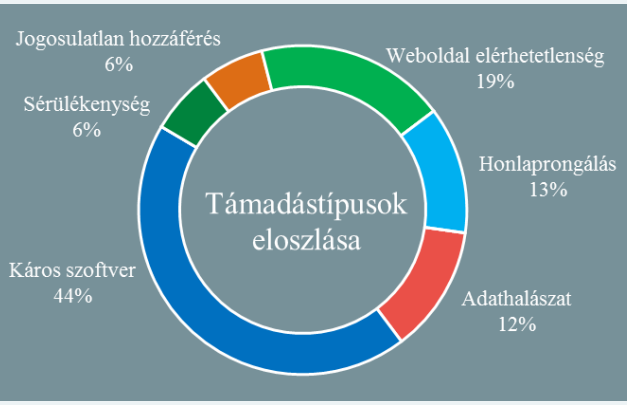
NEMZETI KIBERVÉDELMI INTÉZET

Nemzetközi IT-biztonsági sajtószemle

2019. 46. hét

Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.11.08. - 2019.11.14.



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

A Microsoft minden amerikai ügyfelére alkalmazni szeretné a CCPA-t

(zdnet.com)

A 2020. január 1-től életbe lépő California Consumer Privacy Act (CCPA) az egyik legszigorúbb adatvédelmi törvénynek ígérkezik világszerte, ugyanis teljes transzparenciát ír elő a vállalatok számára az általuk gyűjtött és kezelt ügyféladatok tekintetében. Bejelentése óta a kaliforniai cégek és különböző lobbista csoportok részéről folyamatos támadás éri a jogszabálytervezetet, elsősorban a halasztást kérvényezve, valamint arra kérve a Kongresszust, hogy álljon elő egy teljes Egyesült Államokra kiterjedő szövetségi törvénnyel, eddig sikertelenül. **Bővebben...**

Az Apple védelmi megoldást nyújt a meghekkelt iPhone eszközök ellen

(cyberscoop.com)

Az App Store új programjának ígérete szerint segíteni fogja az iPhone felhasználókat annak felismerésében, hogy eszközeik támadás áldozatává váltak. A Trail of Bits tanácsadó vállalat csütörtökön jelentette be iVerify elnevezésű eszközét, amely működése során az iPhone készülékek megszokottól eltérő viselkedését figyeli, például ha egy alkalmazás a felhasználó engedélye és előzetes beleegyezése nélkül továbbít adatokat. **Bővebben...**

IT biztonsági Tanács

A valós krízishelyzetek bekövetkezése előtt érdemes szervezetünk működési és védelmi folyamatait szimulációs gyakorlatok formájában ellenőrizni. A valósághű szituációk szimulált környezetben történő kezeléséről bővebb információkat az NBSZ NKI weboldalán itt olvashat.

Vállalati szervereket támad egy új ransomware

(zdnet.com)

Kifejezetten nagycéges kiszolgálókra irányul egy új ransomware kampány – derül ki az Intezer és az IBM X-Force, a PureLocker zsarolóvírusról készült közös elemzéséből. Az elemzők szerint a káros kódot készítői minden bizonnyal RaaS (Ransomware-as-a-Service) konstrukcióban bocsátják áruba, azonban nem bárki számára, ugyanis ehhez komoly összeget kérnek. A malware cserébe egy jelentős tulajdonsággal bír, ugyanis PureBasic nyelven íródott, ami megnehezíti a védelmi szoftverek számára a kód detektálását. Exkluzivitására utal továbbá az is, hogy a malware a hírhedt ‘more_eggs’ backdoor-ból is tartalmaz kódrészleteket, amely az internetes feketepiacon veterán kereskedőkhöz köthető. **Bővebben...**

Egyre népszerűbbek a politikai személyeket felhasználó zsaroló kampányok

(bleepingcomputer.com)

A Cisco Talos Group egy közelmúltbeli malspam kampányra lett figyelmes, amely egy Trump.exe elnevezésű káros programmal fertőz. Az elmúlt néhány év rosszindulatú kampányait vizsgálva a Talos megállapította, hogy a támadók előszeretettel választják témául az elmúlt évek nemzetközi politikai életének jelentős személyeit. Donald Trump amerikai elnök arcképével több káros program is előkerült a vizsgálat során, köztük zsarolóvírusok, a „Donald Trump Screen of Death” képernyőzár (screen locker), valamint a védelmi szoftverek megkerülését megvalósító „Trump Crypter”. **Bővebben...**

Kiberháborús gyakorlat tartott Tajvan és az Amerikai Egyesült Államok

(ehackingnews.com)

Egy hétig tartott az USA és Tajvan közös kiberháborús gyakorlata. Az eseményt a tajvani hatóságok együttesen szervezték az American Institute in Taiwan (AIT) szervezettel, amely az amerikai érdekeltségeket képviseli a szigeten. **Bővebben...**