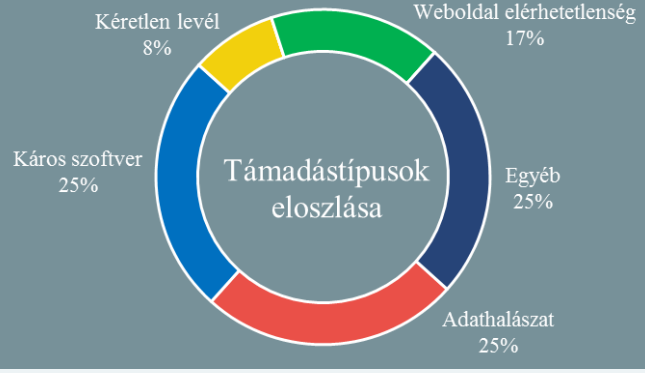
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.11.15. - 2019.11.21.



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

A Microsoft tagadja, hogy platformját zsarolóvírus terjesztésére használják a kiberbűnözők

(zdnet.com)

A Microsoft tagadja, hogy a Microsoft Teams névre hallgató kommunikációs és kollaborációs platformját kiberbűnözői csoportok zsarolóvírus terjesztésre használnák. A híresztelések pontos forrása ismeretlen, mindössze annyit tudni, hogy azok kora novemberben kaptak szárnyra, amikor több spanyol cég DoppelPaymer zsarolóvírussal fertőződött meg. Simon Pope, a Microsoft Security Response Center (MSRC) incidenskezelési vezetője azt a híresztelést is cáfolta, miszerint a hónapok óta ismert, BlueKeep nevű RDP sérülékenység is közrejátszott volna a káros kód terjedésében. Vizsgálatuk szerint a támadók ehelyett a megtámadott cégek távoli munkatársainak hitelesítő adatait szerezték meg és használták a vállalatok hálózatain történő terjesztésre. A nyilatkozat szokatlan lépés a tech óriástól, nem jellemző ugyanis, hogy ilyen nyilvánvalóan hamis online hírekre reagálnának. **Bővebben...**

Így tudna az USA és az EU szabad internetet hozni Iránba

(dw.com)

Az Amerikai Egyesült Államok németországi nagykövete, Richard Grenell tweetje szerint az USA és az Európai Unió képes lenne visszakapcsolni a netet Iránban, miután az uralkodó rezsim azt elérhetetlenné tette a magas üzemanyagárak miatti tüntetések idején. A World Wide Web az Internet egyik legfontosabb szolgáltatása, amelynek megfelelő működéséhez folyamatos kapcsolat szükséges, így egy nemzetállam az internet szolgáltatókon keresztül gyakorlatilag lehetetlenné teheti a webes kommunikációt. Ebben az esetben alternatívát jelenthetnek az ún. CrossPoint (XP) szerverek segítségével alkotott hálózatok. Ezek gyakorlatilag egyszerű személyi számítógépek, amelyek hagyományos telefon vonalakat használnak az adatcserére. **Bővebben...**

Ipari vezérlőrendszerekre támad egy iráni hacking csoport

(wired.com)

Iráni hackerek követték el a legpusztítóbb kibertámadásokat az elmúlt évtizedben, elsősorban a Közel-Keletre, valamint az Egyesült Államokra koncentrálva. Jelenleg úgy tűnik, hogy Irán legaktívabb hacker csoportja, az APT33 (más néven Holmium, Refined Kitten, vagy Elfin) taktikát váltott és standard IT hálózatok helyett most már energetikai és gyártó- valamint olajipari rendszerek vezérlői ellen indít támadásokat. Minderről a Microsoft fenyegetés elemző csoportja számolt be a CyberwarCon konferencián. A hackerek motivációja a kiválasztott célpontok alapján nem egyértelmű, egyes spekulációk szerint elsősorban csak meg akarták vetni a lábukat későbbi fizikai károkat is okozó támadásokat előkészítve. **Bővebben...**

Vigyázat: A karácsonyi szezon közeledtével egyre több a megtévesztő domain

(securityweek.com)

A Venafi az ünnepi szezon közeledtével vizsgálatot végzett potenciálisan megtévesztő domain nevek után kutatva, ennek során pedig több, mint 100 000 olyan domaint azonosított, amelyek valamilyen ismert kereskedői platform domain nevére hasonlítanak és emellett érvényes TLS tanúsítvánnyal is rendelkeznek. A cég szerint ez több, mint a duplája a tavaly tapasztaltnak, ami még akkor is hatalmas szám, ha tekintetbe vesszük, hogy a fellelt domainek egy része vélhetően legitim célokat szolgál. Egy másik érdekesség, amire a jelentés rámutat, hogy a valós tanúsítvány kibocsátások száma jóval alacsonyabb, ezekből ugyanis csupán negyed annyi került kiadásra. **Bővebben...**

146 biztonsági hibát fedeztek fel előre telepített androidos alkalmazásokban

(thenextweb.com)

A Kryptowire kutatói összesen 146 biztonsági hibát fedeztek fel 29 androidos gyártó előre telepített alkalmazásában. Az Egyesült Államok Belbiztonsági Minisztériuma (DHS) által finanszírozott vizsgálat során a kutatók több nagyobb OEM (original equipment manufacturers), például az Asus, a Samsung és a Xiaomi alkalmazásaiban tártak fel biztonsági réseket. A Google tavaly vezette be Build Test Suite (BTS) nevű rendszerét, amelynek segítségével az OEM-ek által nyújtott alkalmazások és frissítések még azelőtt tesztelésre kerülnek, hogy a felhasználók számára elérhetővé válnának. Amennyiben az ellenőrzések során egy adott alkalmazásban biztonsági rést találnak, azt a gyártókkal közösen javítja ki a Google, ennek ellenére mégis előfordulnak olyan esetek, amikor a biztonsági hibák átcsúsznak az ellenőrzéseken. Súlyosbító körülmény, hogy míg egy letöltött alkalmazás eltávolítható az eszközről (miután annak nyilvánosságra kerülnek a sérülékenységei), addig az OEM-ek által előre telepített alkalmazások esetében erre nincs lehetőség.

IT biztonsági Tanács

Az iOS 13.2-es verziója számos új funkciót hoz, köztük hasznos adatvédelmi beállítási lehetőségeket.

Az utóbbi időben nagy felháborodást keltett, hogy az Apple készülékek hangvezérlésű asszisztens programja, a Siri hogyan kezeli az ügyfelek adatait, ezért az Apple úgy döntött lehetőséget ad a felhasználóknak arra, hogy töröl-hessék a program által rögzített hang-utasításokat.

Az NBSZ NKI erre vonatkozó javaslatai itt olvashatók.

ENISA ajánlás „Security by Design” elv implementálására IoT eszközök esetében

(enisa.europa.eu)

Az okos eszközök száma folyamatosan nő, a Gartner szerint 2021-re számuk eléri a 25 milliárdot. Az elmúlt évek során tapasztalt IoT támadások, mint a Stuxnet, vagy a Mirai, fokozódó aggodalmat keltenek ezen eszközök biztonságával kapcsolatban. A biztonságos fejlesztésre vonatkozó segédletek, mint például a most tárgyalt ENISA ajánlás (Good Practices for Security of IoT) a kiberbiztonsági ügynökség szerint alapvető jelentőséggel bírnak az IoT biztonság megteremtésében. A szóban forgó kiadvány részletesen kitér a biztonsági követelmények meghatározására, a tervezésre, a fejlesztésre, sőt az IoT rendszerek és szolgáltatások megsemmisítésére is. A biztonsági előírások és jó gyakorlatok a teljes IoT ökoszisztémára vonatkoznak, beleértve az eszközöket, kommunikációs hálózatokat, a felhőszolgáltatásokat, stb. **Bővebben...**

A uBlock Origin firefoxos verziója mostantól képes blokkolni a first-party nyomkövető szkripteket

(bleepingcomputer.com)

Mivel a böngészők egy ideje elkezdték blokkolni a third-party nyomkövetőket, egyes weboldalak elkezdtek saját (first-party) nyomkövető szkripteket alkalmazni. Ezt adott esetben úgy teszik, hogy a weboldal DNS rekordjai között a CNAME rekordban adják meg a nyomkövető szolgáltatásokat nyújtó külső oldalt, amit eddig a blokkoló programok nem vizsgáltak. Szerencsére a Firefox esetében elérhető egy API, ami lehetővé teszi a böngésző kiegészítők számára DNS elkérdezések végrehajtását, így a uBlock Origin 1.24.1b0 verziójától kezdődően már védelmet nyújt a fenti eljárással szemben. **Bővebben...**

A Shade ransomware jelenleg a legaktívabban terjesztett káros kód

(bleepingcomputer.com)

A Group-IB szerint 2019 első felében a Shade (vagy más néven Troldesh) ransomware volt az e-mailen keresztül terjesztett káros kódok közül a leggyakoribb. A szingapúri biztonsági cég szerint lényegesen megemelkedett a zsarolóvírusok alkalmazása a káros kampányok során 2018-hoz képest, amikor még a backdoorok és banki trójai programok számítottak vezető fenyegetésnek. A Shade ransomware nem új malware, azonban fejlesztői folyamatosan új képességekkel ruházzák fel, ezért a kiberbűnözők továbbra is előszeretettel veszik bérbe, amit a Malwarebytes és az Avast is megerősít. Fontos megjegyezni, hogy ─ habár ez csak a régebbi verziókra vonatkozik ─ a No More Ransom projekt a Kaspersky segítségével elérhetővé tett egy dekriptorokat, amelyekkel a titkosított állományok visszafejthetők.

Twitter végre telefonszám megadása nélkül lehetővé teszi a kétfaktoros azonosítást

(techcrunch.com)

Már régóta ismert probléma, hogy az SMS alapú kétfaktoros azonosítás nem a legbiztonságosabb módja a felhasználók hitelesítésének, ugyanis az SMS-ek eltérítésével a kódok könnyen arra nem jogosultak birtokába juthatnak. A Twitter régóta kötelezi felhasználóit az SMS alapú 2FA használatára, amit a felhasználóknak módjukban áll ugyan lecserélni más hitelesítési opciókra, mint a Google Authenticator, vagy a Yubikey, de ehhez előbb meg kell adniuk a telefonszámot. A közösségi platform biztonsági csapatának bejelentése szerint azonban a Twitter mostantól lehetővé teszi a kétlépcsős azonosítást telefonszám megadása nélkül is. **Bővebben...**