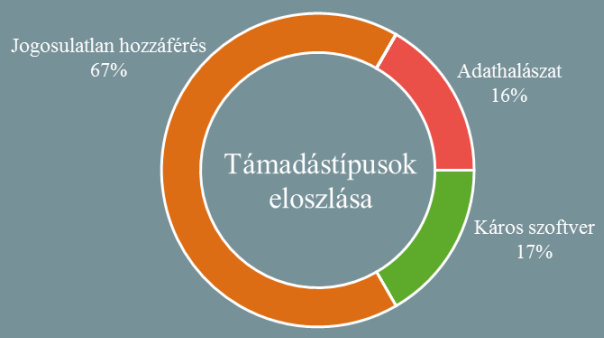
Az NKI által kezelt incidensekre vonatkozó statisztikai adatok: 2019.02.22. - 2019.02.27.


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

## Az európai választások előtt: eskü az álhírek elkerülésére

**(heise.de)**

Transzatlanti kezdeményezés született a közelgő európai parlamenti választások tisztaságának előmozdítására, mégpedig akként, hogy a jelöltek saját kötelezettség-vállalásuk révén fellépjenek egyebek mellett az álhírek, a dezinformációk és az átláthatatlan kampánypénzek alkalmazása ellen. Ezen célok elérése érdekében az érintett politikusoknak egy erre vonatkozó dokumentumot is alá kell írniuk, mindez egy nemrégiben Münchenben megrendezett biztonsági konferencián látott napvilágot. A volt amerikai alelnök, Joe Biden szerint azonban ez a kezdeményezés túlmutat a szóban forgó választásokon, mivel kihatással lehet az USA következő elnöki kampányidőszakára is, arra figyelemmel, hogy véleménye szerint Donald Trump 2016-os kampánya megsértette a kezdeményezés mind az öt tartalmi pontját, különös tekintettel a téves, kitalált és lopott információk propaganda célokra történő felhasználásának kérdésére. A már számos aláíróval rendelkező kezdeményezés azt is tartalmazza, hogy a kampányban résztvevő segítőknek olyan informatikai eszközöket kell használniuk, amelyek képesek a hekker-támadások semlegesítésére.

## A Google megfeledkezett a Nest Guard beépített mikrofonjáról?

**(www.securityaffairs.co)**

A Business Insider beszámolója szerint a Google elmulasztotta tájékoztatni ügyfeleit arról, hogy a Nest Secure otthoni riasztórendszer termékének Nest Guard modulja beépített mikrofont tartalmaz. Minderre annak kapcsán derült fény, hogy a Google február elején bejelentette a rendszer hangvezérlő funkcióval történő bővítését, azonban az eszköz 2017-es megjelenése óta egyszer sem került megemlítésre, hogy a készülékek beépített mikrofonnal vannak felszerelve. A Google elmondása szerint nem szándékosan hallgatták el a mikrofon jelenlétét, azonban elismerik, hogy hibáztak, fel kellett volna tüntetniük a specifikációban. **Bővebben...**

## Már aktívan ki is használják a WinRAR sérülékenységét

**(www.securityaffairs.co)**

A CheckPoint kutatói felfedeztek egy ún. könyvtárbejárási (azaz a támadott rendszer fájlszerkezetében emelt jogosultság megszerzését lehetővé tévő) sérülékenységet a több, mint 500 millió felhasználóval bíró WinRAR tömörítő programban, a 360 Threat Intelligence Center pedig már azonosított is egy, a sérülékenységet kihasználó támadó kampányt. Ennek során a támadók a sérülékenység következtében egy káros kódokat tartalmazó futtatható fájlt képesek elhelyezni az indítópultban, feltéve hogy a UAC (User Account Control – felhasználói fiók felügyelet) nem aktív, vagy a bejelentkezett felhasználó admin joggal bír. **Bővebben...**

## Az Edge böngésző titokban megengedi a Facebooknak, hogy automatán lejátsza a Flash tartalmakat

**(www.bleepingcomputer.com)**

Ivan Fratric, a Google Project Zero biztonsági kutatója talált rá egy fehérlistára a **C:Windowssystem32edgehtmlpluginpolicy.bin** fájlban, amely lehetővé teszi a Facebook számára a beépített click-to-play biztonsági házirend megkerülését, így felhasználói engedély nélkül automatikusan lefutnak a Flash tartalmak. A Microsoft a februári „patch kedd” során kiadott javítócsomagja óta már csupán két domain szerepel a listában (**www.facebook.com**, valamint az **apps.facebook.com**), amelyben tavaly novemberben még 58 domain volt megtalálható enkriptált formában. **Bővebben...**

## Sérülékenységet fedeztek fel a SHAREit nevű, népszerű fájlcserélő applikációban

**(thehackernews.com)**

A RedForce biztonsági kutatói két magas biztonsági besorolású sérülékenységet fedeztek fel a világszerte több, mint 1,5 milliárd felhasználóval bíró SHAREit fájlcserélő alkalmazás androidos verziójában. A hibák tetszőleges fájlokhoz történő jogosulatlan hozzáférést tettek lehetővé, és ahogy az a RedForece blogposztjából kiderült, olyan könnyedén kihasználhatóak voltak, amilyenre eddig még nem láttak példát. A sérülékenységek az androidos SHAREit applikáció 4.0.38-as verzióját, valamint az ennél korábbi kiadásokat érintik. Bár a fejlesztő cég már tavaly márciusban elvégezte a hibajavítást, erről semmilyen visszajelzést nem adott a kutatóknak, akik ezt nehezményezték is.

## IT biztonsági Tanács

A Facebook applikáció alapértelmezetten gyűjti a felhasználók helyadatait, még akkor is, amikor az alkalmazás nincs használatban. Android rendszeren mindeddig csupán arra volt lehetőség, hogy a teljes adatgyűjtést kikapcsoljuk a „Location History” beállítás alatt, azonban ez egyes facebookos szolgáltatások (pl.: „A közelben” funkció) működését ellehetetlenítette.

A Facebook most változtatott a „mindent vagy semmit” elven, és az iOS-es verzió mellett már Androidon is lehetővé tette a helyadatok gyűjtésének korlátozását, amikor az alkalmazás nem fut, azaz a helyadatok háttér szolgáltatásának ki/be kapcsolását. Minderről bővebb információt itt olvashat.

## Uniós szabvány készült a konzumer IoT eszközök biztonságossá tételéhez

**(www.securityweek.com)**

Az Európai Távközlési Szabványosítási Intézet (ETSI) február 19-én közzétette a konzumer IoT eszközök kiberbiztonsági szabványát (ETSI TS 103 645 V1.1.1), amely a remények szerint a jövőbeni IoT tanúsítási rendszer alapjául szolgál majd. A szabvány célja, hogy elejét vegye a felhasználói adatszivárgásoknak, valamint a fogyasztói IoT eszközök ─ például DDoS támadásokhoz felhasznált ─ botnet hálózatokba történő bevonásának. **Bővebben...**

## Felkészülés a választásokra: Portugália az ENISA segítségével tart kiberbiztonsági gyakorlatot

**(www.enisa.europa.eu)**

A portugál Nemzeti Kiberbiztonsági Központ (CNCS) felkérte az Európai Uniós Hálózat- és Információbiztonsági Ügynökséget (ENISA), hogy támogassa a választási folyamat kiberbiztonsági tesztelésére szolgáló gyakorlatát, amely mind az európai parlementi, mind a nemzeti választások kapcsán hozzájárul a felkészüléshez. Az ExNCS2019 névre keresztelt gyakorlat a portugál nemzeti választási bizottság (CNE) együttműködésével kerül megrendezésre, amelyben az ENISA a portugál hatóságokat segíti majd a 2010 óta szervezett Cyber Europe gyakorlatok során megszerzett tapasztalataival. **Bővebben...**

## Oroszországot vádolják az ukrán választási bizottság elleni DDoS támadással

**(www.cyberscoop.com)**

Petro Poroshenko ukrán miniszterelnök közleménye szerint Oroszország DDoS (azaz a célkeresztben lévő rendszer által nyújtott hálózati szolgáltatások ellehetetlenítésére irányuló) támadást indított az ukrán választási bizottság (Central Election Commission) ellen. A DDoS támadás több ütemben zajlott 2019.02.24-25. között, amelyet ukrán nemzetbiztonsági és bűnüldöző hatóságok, valamint külön meg nem nevezett „amerikai partnerek” segítségével sikerült elhárítani. Oleksandr Turchynov, Ukrajna Nemzeti Biztonsági és Védelmi Tanácsának (RNBOU) titkára felhívta a figyelmet arra, hogy Oroszország minden valószínűség szerint teljes arzenálját beveti majd a március 31-én esedékes elnökválasztás befolyásolására. Turchynov ezzel kapcsolatban azt is jelezte, hogy Ukrajna az Európai Unióval olyan gyakorlatokon dolgozik, amelyek során különböző kibertámadások, valamint lehetséges válaszreakciók kerülnek majd modellezésre. **Bővebben...**

## Sérülékenységeket találtak PDF olvasó alkalmazásokban

**(securityaffairs.co)**

A németországi Ruhr-Universität Bochum hallgatói csoportja számos sérülékenységet azonosított népszerű asztali és online PDF olvasókban, amelyek kihasználásával a digitális aláírással ellátott PDF dokumentumok anélkül módosíthatóak, hogy az aláírás érvénytelenné válna. A sebezhetőségben érintett ─ összesen 22 ─ PDF olvasó között szerepel az Adobe Reader, a Foxit Reader, és a LibreOffice is, az online szolgáltatások között pedig a DocuSign, az eTR Validation Service, a DSS Demonstration WebApp, az Evotrust, valamint a VEP.si. A PDF olvasó alkalmazás fejlesztő gyártók már kiadták a hibajavító frissítéseket, ellenben néhány online szolgáltatás esetében még nincs hír javításról.