OUCH! | 2015. január

Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadványban...

Mobil alkalmazások biztonságos használata

Áttekintés

Az olyan mobil eszközök, mint az okostelefonok és tablet-ek mostanra az egyik legfontosabb technológiákká váltak, amelyeket mind a privát életünkben, mind a munkahelyünkön egyaránt használunk. A rengeteg hozzáférhető alkalmazás teszi igazán sokoldalúvá a mobil eszközünket. Segítenek növelni a munkánk hatékonyságát, lehetővé teszik a másokkal történő folyamatos kapcsolattartást, akikkel meg is tudjuk osztani a saját adatainkat, képezhetjük magunkat, vagy éppen segítenek a kikapcsolódásban. Az alábbi tanácsok betartásával biztonságosabbá tehetjük a mobil eszközünkre telepített alkalmazásokat.

A szerzőről

Chris Crowley független tanácsadó, a SANS minősített oktatója és kurzusainak szerzője. Írásai megtalálhatók a Twitter-en (**@CCrowMontance**) és a Google plus-on (**+ChrisCrowley**).

Alkalmazások beszerzése

Első lépés, hogy kizárólag csak biztonságos, megbízható forrásból töltsünk le bármilyen alkalmazást! Mindig tartsuk észben, hogy bárki készíthet mobil alkalmazást, ezért legyünk mindig körültekintőek, honnan töltünk le bármit is! A kiberbűnözők egyik kedvelt módszere az, hogy káros szoftverrel fertőzött, de valódinak tűnő alkalmazásokat készítenek és terjesztenek. Ha a felhasználó telepít egy ilyen alkalmazást, akkor a támadók át tudják venni az irányítást az eszköz felett, így el tudják olvasni az email-eket, belehallgathatnak a beszélgetésekbe, valamint meg tudják szerezni a mobil eszközön tárolt kontaktinformációkat. Azzal, hogy csak megbízható forrásból töltünk le bármilyen alkalmazást, csökkenteni tudjuk annak kockázatát, hogy megfertőződjünk ilyen káros szoftverrel. A mobil készülék gyártója meghatározza, hogy milyen lehetőségeink vannak alkalmazások letöltésére.

Az iPhone vagy iPad készülékekre csak az Apple által működtetett app store-ból lehet telepíteni alkalmazásokat. Ennek az az előnye, hogy az Apple mind az alkalmazást, mind az alkalmazás készítőjét le tudja ellenőrizni biztonsági szempontból. Bár az app store sem képes elfogni az összes rosszfiút vagy káros szoftverrel fertőzött alkalmazást, nagymértékben csökkenti a veszély mértékét. Ezen kívül, ha az Apple úgy véli, hogy valamelyik szoftver fertőzött, azonnal letiltják a további elérést. A Windows Phone hasonló módszereket használ a saját app store-jával kapcsolatban.

Az Android készülékek ebből a szempontból mások. Sokkal nagyobb szabadságot biztosítanak, így bárhonnan le tudunk tölteni egy alkalmazást. Azonban a nagyobb szabadság nagyobb felelősséggel is jár. Jobban oda kell figyelnünk, és észben kell tartanunk, hogy az alkalmazás, amit letöltünk és telepítünk, az, aminek látszik. A Google is működtet az Apple-éhez hasonló app store-t, ezt úgy nevezik, hogy Google Play. Az innen letöltött alkalmazások átesnek néhány

© The SANS Institute 2015

Mobil alkalmazások biztonságos használata

egyszerű ellenőrzésen. Javasolt csak innen letölteni bármilyen alkalmazást a mobil készülékünkre. Lehetőség szerint kerüljünk bármilyen alkalmazást, amit más weboldalakról lehet letölteni, mivel könnyen lehet, hogy azokat kiberbűnözők készítették, amellyel meg tudják fertőzni az áldozat készülékét. A biztonság felé tett további lépés gyanánt telepítsünk egy antivírus szoftver is.

A kockázatok elkerülése érdekében ne töltsünk le vadonatúj alkalmazásokat, amelyeket csak néhányan próbáltak ki, vagy csak nagyon kevés pozitív visszajelzéssel rendelkeznek. Minél régebb óta elérhető egy alkalmazás, vagy minél több pozitív visszajelzés van róla, annál valószínűbb, hogy megbízható alkalmazásról van szó. Továbbá csak olyan alkalmazást telepítsünk, amire tényleg szükségünk van, és használni is fogjuk. Sőt, tegyük fel magunknak a kérdést: tényleg szükségem van erre az alkalmazásra? Tartsuk észben, hogy az újabb alkalmazások nem csak újabb sérülékenységeket hoznak magukkal, hanem akár új adatvédelmi problémákat is. Ha már nem használunk egyet, akkor távolítsuk el a mobil eszközről (ha később mégis szükség lenne rá, akkor újra letölthetjük).

A mobil alkalmazások biztonságos használatának a kulcsa az, hogy csak biztonságos forrásból telepítünk szoftvert, amit folyamatosan frissítünk a legújabb verzióra, és mindig ellenőrizzük az engedélyezett jogosultságokat.

Előfordulhat, hogy valaki javasolja az ún. jailbreak vagy root-olás eljárást. Ez az a folyamat, amikor a felhasználó „feltöri” a saját telefonját azért, hogy nem engedélyezett alkalmazásokat telepítsen rá, vagy, hogy megváltoztasson egyes beépített funkciókat. Erősen ellenjavallt ezen eljárás alkalmazása, mivel nem csak megkerüli vagy megszünteti a mobil eszközbe épített biztonsági eljárásokat, hanem a garancia elvesztésével is jár.

Jogosultságok

Miután megbízható forrásból telepítettünk egy új alkalmazást, gondoskodnunk kell arról, hogy a megfelelő beállítások segítségével megvédjük a saját adatainkat. A mobil alkalmazások telepítése és konfigurálása gyakran együtt jár azzal, hogy engedélyezünk bizonyos dolgokat az új alkalmazás számára. Mindig gondoljuk végig, hogy mielőtt engedélyezünk bármilyen hozzáférést az alkalmazás számára, annak tényleg szüksége van-e rá. Például néhány alkalmazás használ geolokációs szolgáltatásokat. Ha engedélyezzük ezt, akkor lehet, hogy a program készítője nyomon tudja követni a mozgásunkat, és ezeket az információkat eladhatja egy harmadik félnek. Ha nem akarunk engedélyezni bizonyos dolgokat egy alkalmazás számára, akkor inkább nézzünk körül, hátha van olyan, amely kielégíti az igényeinket. Jegyezzük meg, számtalan választási lehetőségünk van! Az Apple eszközöknél van lehetőség arra, hogy bizonyos jogosultságokat a ’Beállításokban’ vagy akár futás közben változtassunk (például hozzáférést engedélyezhetünk a geolokációs szolgáltatáshoz). A Windows és Android készülékek másként működnek, mivel azok a mindent vagy semmit elvet követik. Ha nem engedélyezzük az összes jogosultságot az alkalmazás számára, akkor nem tudjuk telepíteni azt.

© The SANS Institute 2015

Mobil alkalmazások biztonságos használata

Alkalmazások frissítése

A mobil alkalmazásokat – hasonlóan az asztali gépek és mobil eszközök operációs rendszereihez – időnként szükséges frissíteni. A kiberbűnözők folyamatosan keresik – és meg is találják – az alkalmazásokban megbújó biztonsági réseket, illetve mindig újabb és újabb exploitokat, káros szoftvereket készítenek ezek kiaknázására. Az alkalmazások készítői folyamatosan javítják a szoftvereiket, és újabb verziókat készítenek, hogy ezzel védjék a felhasználókat. Minél gyakrabban ellenőrizzük az újabb verziók meglétét, annál jobb. A legtöbb rendszer lehetőséget ad arra, hogy automatikusan frissüljenek az alkalmazások. Javasolt ennek a beállítása. Ha erre nincs lehetőség, akkor javasolt legalább kéthetente ellenőrizni, hogy van-e újabb verzió a telepített szoftverekből. Azonban ne felejtsük ellenőrizni, hogy az újabb verzió kér-e esetleg újabb jogosultságokat!

További Információ

Iratkozzon fel a havi rendszerességű OUCH! biztonságtudatossági hírlevélre, férjen hozzá az OUCH! archívumhoz, tudjon meg többet a SANS biztonságtudatossági megoldásairól a http://www.securingthehuman.org weboldalon keresztül.

Magyar Kiadás

Kormányzati, távközlési és informatikai szolgáltatóként, Magyarország egyik stratégiai fontosságú gazdasági társasága a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Társaságunk kiemelt feladata a kormányzati infrastruktúra működtetése, az e-közigazgatási megoldások támogatása, valamint kormányzati szintű informatikai szolgáltatások nyújtása. További információ a http://www.nisz.hu oldalon olvasható.

Hivatkozások

Pszichológiai manipuláció (social engineering): http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201411_hu.pdf

Mielőtt megválunk a régi mobiltól: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201406_hu.pdf

Így lesz biztonságosabb az új tablet-ed: http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201312_hu.pdf

Általános biztonsági megfontolások: http://www.securingthehuman.org/resources/security-terms

SEC575: Mobil biztonsági kurzus: http://www.sans.org/sec575

OUCH! a SANS Securing The Human program által közzétett hírlevél, amelyre Creative Commons BY-NC-ND 4.0 licensz feltételei vonatkoznak. A hírlevél szabadon terjeszthető vagy felhasználható tudatosító programban, addig amíg az nem kerül módosításra. A fordításért vagy további információért kérjük írjon az ouch@securingthehuman.org címre.

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Fordította: Birkás Bence, Árvai Gábor