Havi biztonság tudatossági hírlevél számítógép felhasználók számára

OUCH!

Ebben a kiadásban...

Mobil alkalmazások biztonságos használata

Áttekintés

Az olyan mobil eszközök, mint az okostelefonok és tabletek 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 azonnali kapcsolattartást és megosztást, képezhetjük magunkat, vagy éppen segítenek a kikapcsolódásban. Azonban az alkalmazások erejével együtt jönnek a kockázatok is. Az alábbi tanácsok betartásával biztonságosabbá tehetjük a mobil eszközünkre telepített alkalmazásokat.

A szerzőről

Joshua Wright a Counter Hack technikai igazgatója és vezető oktató a SANS Intézetnél. Ő a szerzője a SEC575 kurzusnak a Mobil Eszköz Biztonságról és Etikus Hackelésről, illetve a Vezetéknélküli Hálózatók Feltöréséről. Josh elérhető a Twitter-en **@joswr1ght** cím alatt.

Alkalmazások beszerzése

Első lépés, hogy kizárólag biztonságos, megbízható forrásból töltsünk le bármilyen alkalmazást. 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. 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 előnye az, hogy az Apple minden alkalmazást ellenőriz biztonsági szempontból mielőtt elérhetővé teszi. Bár az app store sem képes elfogni az összes 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

Mobil alkalmazások biztonságos használata

észben kell tartanunk, hogy az alkalmazás, amit letöltünk és telepítünk nem kerül ellenőrzésre. A Google is működtet az Apple-éhez hasonló app store-t, ezt úgy nevezik, hogy Google Play. Az innen letöltött alkalmazások átesnek néhány egyszerű ellenőrzésen. Javasolt csak innen letölteni bármilyen alkalmazást az Androidos 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 mobil alkalmazások biztonságos használatának a kulcsa, hogy csak biztonságos forrásból telepítsünk szoftvert, folyamatosan frissítsünk, és mindig ellenőrizzük az engedélyezett jogosultságokat.

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. Tegyük fel magunknak a kérdést: vajon tényleg szükségem van erre az alkalmazásra? Tartsuk észben, hogy az újabb alkalmazások nem csak újabb sérülékenységeket hoznak magukkal, hanem új adatvédelmi problémákat is. Ha már nem használunk egy alkalmazást, inkább távolítsuk el a mobil eszközről (ha később mégis szükség lenne rá, akkor újra letölthetjük). Végül, soha ne törjük fel szoftveresen a mobil eszközt, aminek során nem jóváhagyott alkalmazásokat telepíthetünk vagy meglévő, gyári beállításokat állítunk át. Ezzel nemcsak megkerüljük vagy kitöröljük a gyárilag beállított biztonsági kontrollokat, hanem elveszítjük a készülékre vonatkozó garanciát és támogatást is.

Jogosultságok

Miután megbízható forrásból telepítettünk egy új alkalmazást, gondoskodnunk kell arról, hogy a megfelelő beállítások segítségével megvédjük a saját adatainkat. 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. Ne feledjük, nagy a kínálat, adott a választás lehetősége.

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 securingthehuman.sans.org/ouch/archives 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:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201701_hu.pdf
Mielőtt megválunk a régi mobiltól:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201612_hu.pdf
Az új tablet biztonsága:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_hu.pdf
OUCH! archívum és fordítások:	https://securingthehuman.sans.org/ouch/archives
SEC575: Mobil biztonsági kurzus:	http://www.sans.org/sec575

Szerkesztette: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Fordította: Birkás Bence

