OUCH! | Marzo 2017

La newsletter mensile sulla sicurezza informatica per tutti gli utenti

OUCH!

IN QUESTO NUMERO...

Usare le app in modo sicuro

Introduzione

I dispositivi mobili, tablet, smartphone e smartwatch, sono diventati una delle tecnologie più utilizzate nella nostra vita personale e professionale. Ciò che rende questi dispositivi così versatili è la grandissima quantità di app che possiamo usare. Queste app ci permettono di essere più produttivi, comunicare istantaneamente, condividere con gli altri, erogare formazione e, infine, divertirci. Purtroppo, alle possibilità che ci vengono offerte si accompagnano anche dei rischi. Ecco alcuni azioni da intraprendere per usare le app in modo sicuro e ottenere il massimo.

L'autore di questo numero

Joshua Wright è il direttore tecnico di Counter Hack nonché istruttore senior al SANS Institute. È autore del corso "SEC575: Mobile Device Security and Ethical Hacking" e del libro "Hacking Exposed: Wireless". Potere contattare Josh su Twitter: **@joswr1ght**.

Ottenere le app

Il primo passo consiste nello scaricare sempre le app da una fonte affidabile e sicura. I criminali informatici sono diventati sempre più abili nella creazione e distribuzione di applicazioni mobili infette che appaiono del tutto legittime: quando installate un'applicazione infetta, gli hacker possono prendere il controllo completo del vostro dispositivo mobile. Scaricando da fonti note e attendibili si riduce la possibilità di installare un app infetta.

È la tipologia di dispositivo mobile che regola le opzioni per il download. Per i dispositivi Apple come iPad o iPhone, scaricate applicazioni mobili solo dagli App Store Apple: il produttore esegue infatti un controllo di sicurezza di tutte le applicazioni mobili prima di renderle disponibili. Anche se Apple non può individuare tutte le app mobili infette, questo ambiente gestito contribuisce a ridurre drasticamente il rischio di installare software infetto. Inoltre, se Apple individuasse un'applicazione nel suo store che suppone infetta la farà rimuovere rapidamente. Windows Phone utilizza un approccio simile nella gestione delle applicazioni.

I dispositivi mobili Android hanno un approccio diverso. Android offre una maggiore flessibilità grazie alla possibilità di scaricare un app mobile da qualsiasi sito Internet. Tuttavia, questa flessibilità richiede una maggiore responsabilità: è infatti

Usare le app in modo sicuro

necessario porre più attenzione verso quali applicazioni mobili installate poiché non tutte vengono esaminate. Google gestisce un app store simile a quella di Apple, chiamato Google Play. Le applicazioni mobili scaricate da Google Play vengono sottoposte ad alcuni controlli di sicurezza di base, per cui si consiglia di scaricare le app per i dispositivi Android solo da questo store. Evitate il download da altri siti web poiché chiunque, ivi inclusi i criminali informatici, può facilmente creare e distribuire applicazioni maligne per poi ingannarvi allo scopo di infettare il vostro dispositivo mobile. Come ulteriore precauzione, installate un anti-virus, quando possibile

Il modo migliore per rendere sicure le app è di installarle solo da fonti conosciute, aggiornarle quando possibile e concedere solo i permessi necessari.

Indipendentemente da quale dispositivo stiate utilizzando, un ulteriore accorgimento consiste nell'evitare le applicazioni nuove, scaricate da poche persone, o che hanno ben pochi commenti positivi. Più a lungo un app è disponibile, più persone l'avranno utilizzata e la sua attendibilità sarà proporzionale ai commenti positivi. Installate solo le applicazioni necessarie. Chiedetevi se avete veramente bisogno di quell'app. Ogni applicazione potenzialmente può portare con sé non solo nuove vulnerabilità, ma anche nuovi problemi di privacy. Se un app non vi serve più, rimuovetela dal dispositivo mobile (è sempre possibile reinstallarla in un secondo momento se ne avrete ancora bisogno). Infine, non effettuate jailbreak o rooting del dispositivo: si tratta di un processo di hacking che permette l'installazione di applicazioni non approvate e la modifica delle funzionalità esistenti. Questa operazione consente di ignorare o eliminare molti dei controlli di sicurezza integrati nel vostro dispositivo mobile e anche di annullare la garanzia e il contratto di supporto.

I permessi

Dopo aver installato un app mobile da una fonte attendibile, assicuratevi che sia configurata in modo da proteggere la vostra privacy. Prima di consentire un accesso a un app, riflettete: volete concedere i permessi richiesti? L'applicazione ne ha veramente bisogno? Alcune applicazioni utilizzano, ad esempio, servizi di geo-localizzazione. Se si consente a un'app di conoscere sempre la posizione, potreste permettere al creatore di tale app il monitoraggio dei vostri movimenti, permettendo anche la vendita di queste informazioni ad altri. Se non desiderate concedere le autorizzazioni, cercate un'altra app che soddisfi le vostre esigenze. Ricordate, avete moltissime possibilità a disposizione.

Usare le app in modo sicuro

Aggiornare le app

Le applicazioni, proprio come il computer e il sistema operativo del dispositivo mobile, devono essere aggiornate. I criminali sono costantemente alla ricerca di punti deboli nelle app e sviluppano attacchi per sfruttarli. Gli sviluppatori che hanno creato la vostra applicazione, si occupano anche di rilasciare gli aggiornamenti per risolvere eventuali punti deboli e proteggere i dispositivi. Controllate spesso gli aggiornamenti. La maggior parte dei dispositivi consentono di configurare il sistema per aggiornare automaticamente le applicazioni mobili: consigliamo di configurare questa impostazione. Se ciò non dovesse essere possibile, vi suggeriamo di verificare almeno ogni due settimane la presenza di aggiornamenti. Infine, quando le applicazioni vengono aggiornate, verificate sempre eventuali nuovi permessi che potrebbero essere richiesti.

Per saperne di più

Iscriviti ad OUCH!, la newsletter mensile dedicata alla security awareness, consulta i suoi archivi online, e scopri le soluzioni di SANS sulla security awareness visitando il sito
securingthehuman.sans.org/ouch/archives

Versione in Italiano

La versione in italiano è curata da Advanction S.A., un'azienda impegnata nella Sicurezza, nel Risk Management Operativo e nella Security Awareness. Seguila su www.advanction.com e su Twitter(@advanction).

Risorse

Il Social Engineering:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201701_it.pdf
Sostituire un dispositivo mobile:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201612_it.pdf
Tablet e sicurezza:	https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_it.pdf
Gli archivi di Ouch!:	https://securingthehuman.sans.org/ouch/archives

Direzione editoriale: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley