OUCH! | Januari 2015

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

Mobiele Apps Veilig Gebruiken

Overzicht

Mobiele toestellen zoals tablets en smartphones zijn één van de belangrijkste technologieën die we zowel in ons persoonlijk als professioneel leven gebruiken. Mobiele toestellen zijn veelzijdig doordat we uit miljoenen apps kunnen kiezen. Deze apps zorgen ervoor dat we productiever zijn, of meteen met anderen kunnen communiceren, delen, trainen of onderwijzen, of gewoon meer plezier hebben. Maar de mobiele apps introduceren ook risico's. Hier zijn enkele stappen die je kan nemen om jouw mobiele apps veilig te gebruiken.

Gastredacteur

Chris Crowley is een onafhankelijk consultant en een gecertifieerde SANS-instructeur en cursusauteur. Hij is actief op Twitter als **@CCrowMontance** en op Google Plus als **+ChrisCrowley**.

Mobiele Apps Verkrijgen

De eerste stap is je ervan te verzekeren dat je ze altijd downloadt van een veilige en vertrouwde bron. Besef goed dat iedereen zomaar een mobiele app kan ontwikkelen, net daarom dien je voorzichtig te zijn waar je ze haalt. Cybercriminelen hebben reeds hun vaardigheden gebruikt om geïnfecteerde mobiele apps te ontwikkelen en te verdelen, die er legitiem uitzien. Indien je één van deze geïnfecteerde apps installeert, kunnen de criminelen controle nemen over jouw mobiel toestel en e-mails lezen, jouw gesprekken volgen en jouw contactpersonen stelen. Door enkel van veilige en vertrouwde bronnen te downloaden, verklein je de kans om een geïnfecteerde app te installeren. Het merk van het mobiel toestel bepaalt welke opties je hebt om je hiertegen te verdedigen.

Voor Apple toestellen zoals een iPad of een iPhone, kan je enkel mobiele apps downloaden van een beheerde omgeving, zoals de Apple app store. Het voordeel van dit is dat Apple een beveiligingscontrole doet van zowel de mobiele apps en als van hun auteurs. Hoewel Apple niet alle slechteriken of geïnfecteerde apps kan strikken, zorgt de beheerde omgeving ervoor dat er minder kans is om een geïnfecteerde app te installeren. Bijkomend, indien Apple een app vindt in zijn store waarvan vermoedt wordt dat deze is geïnfecteerd, dan zal het snel de app verwijderen. Windows Phone gebruikt een soortgelijke aanpak om apps te beheren.

Android mobiele toestellen zijn anders. Android geeft je meer flexibiliteit doordat je mobiele apps kunt downloaden van overal op het Internet. Hoewel deze flexibiliteit met meer verantwoordelijkheden komt. Je moet beter oppassen welke mobiele apps je downloadt en installeert, aangezien niet alle apps worden gereviewed. Google beheert zelf een mobiele

Mobiele Apps Veilig Gebruiken

app store, gelijkaardig aan die van Apple, genaamd Google Play. De mobiele apps die je downloadt van Google Play, worden op enkele aspecten gecontroleerd. Net daarom raden we aan om enkel mobiele apps van Google Play te installeren. Vermijd het downloaden van Android apps via andere websites omdat iedereen, inclusief cybercriminelen, eenvoudig schadelijke mobiele apps kunnen ontwikkelen en verdelen. Om jou vervolgens te misleiden en jouw mobiel toestel te infecteren. Overweeg dus om een antivirus te installeren op jouw mobiele toestel als extra beveiliging.

De sleutel om jouw mobiele apps te beveiligen is door enkel apps van vertrouwde bronnen te installeren. Zorg ervoor dat jouw apps up-to-date zijn en verifieer of ze de juiste permissies hebben.

Om je risico's nog meer te beperken, kan je best splinternieuwe apps mijden of apps die door weinig mensen zijn gedownload of apps die maar weinig positieve feedback hebben. Des te langer een app beschikbaar is of hoe meer positieve feedback het heeft, des te hoger is de kans dat je de app kan vertrouwen. Installeer bovendien enkel apps die je nodig hebt en effectief gebruikt. Stel je zelf de vraag, heb ik de app werkelijk nodig? Niet enkel kan iedere app potentieel nieuwe zwakheden introduceren, maar ook privacy issues. Indien je een app niet langer gebruikt, verwijder het dan van jouw mobiel toestel (je kan het altijd later toevoegen als je het terug nodig hebt).

Ten slotte kan je in de verleiding komen om jouw mobiel toestel te jailbreaken of te rooten. Hiermee ga je het toestel hacken en zal je niet toegelaten apps installeren of bepaalde ingebouwde functionaliteit veranderen. We raden af om jailbreaking of rooting te doen, aangezien dit security controles niet alleen omzeilt maar ook uitschakelt, die in jouw mobiele toestel zijn voorzien. Vaak vervalt hierdoor ook de garantie en ondersteuning van het toestel.

Permissies

Eens je een mobiele app installeert van een vertrouwde bron, dan is de volgende stap je ervan te verzekeren dat de app veilig geconfigureerd is om jouw privacy te beschermen. Tijdens het installeren of configureren van mobiele apps, zal je vaak permissies moeten toekennen. Denk altijd na vooraleer je toegang geeft, heeft de mobiele app wel daadwerkelijk een nood aan al die permissies? Bijvoorbeeld, sommige apps gebruiken geo-locatie diensten. Indien je toestaat dat een app altijd jouw locatie bijhoudt, dan sta je toe dat de maker jouw bewegingen kan volgen, misschien dat deze informatie wordt verkocht aan andere partijen. Indien je de app geen permissie wil geven, kijk dan rond voor een andere app die wel aan deze vereisten voldoet. Besef dat er genoeg alternatieven beschikbaar zijn. Apple toestellen laten toe dat sommige permissies worden veranderd in het Instellingen menu of tijdens het uitvoeren van de app, zoals de toegang tot de geo-locatie informatie. Windows en Android toestellen zijn verschillend, ze hanteren een alles of niets aanpak. Indien je niet alle permissies toelaat, kan je de app zelfs niet installeren.

Mobiele Apps Veilig Gebruiken

Apps Updaten

Mobiele apps vereisen, net als het besturingssysteem op jouw computer en mobiel toestel, updates om de laatste versie te hebben. Criminelen zijn continu op zoek naar zwakke plekken in apps. Om manieren te ontwikkelen om deze zwakke plekken uit te buiten. Ontwikkelaars die jouw app hebben ontwikkeld, brengen updates uit om deze zwakke plekken te dichten om jouw toestellen te beveiligen. Hoe meer je controleert op updates en ze installeert, hoe beter. De meeste platformen laten toe om jouw systeem automatisch te laten updaten. We raden deze instelling aan. Indien dit niet mogelijk is, dan raden we aan om minstens om de twee weken te controleren op updates. Wanneer je automatisch updates doet, verifieer dan ook welke nieuwe permissies ze vereisen.

Meer Weten?

Ga naar http://www.securingthehuman.org om je te abonneren op de maandelijkse OUCH! Security awareness nieuwsbrief, toegang te krijgen tot het OUCH! archief en kom meer te weten over SANS security awareness oplossingen.

Over Cegeka Groep

Cegeka Groep is een onafhankelijke ICT-dienstverlener opgericht in 1992. Cegeka heeft zijn hoofdkantoor in België en heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Tsjechië en Slovakije. Het bedrijf levert diensten aan klanten in heel Europa: enterprise cloud- en securitydiensten, applicatiediensten, agile coaching en outsourcingdiensten. Cegeka stelt 3.200 mensen tewerk en haalde in 2013 een omzet van 330 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen (Engels)

Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
Disposing Your Mobile Device:	http://www.securingthehuman.org/ouch/2014#june2014
Securing Your New Tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Common Security Terms:	http://www.securingthehuman.org/resources/security-terms
SEC575: Mobile Device Security Course:	http://www.sans.org/sec575

Redactie: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis
Vertaald door: Sven Jacobs, Tom Palmaers

securingthehuman.org/blog /securethehuman @securethehuman securingthehuman.org/gplus