Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

- Overzicht
- Mobiele Apps Verkrijgen
- Permissies
- Apps Updaten

Mobiele Apps Veilig Gebruiken

Overzicht

Mobiele toestellen zoals tablets, smartphones en horloges zijn een van de belangrijkste technologieën in ons persoonlijk en professioneel leven. Mobiele toestellen zijn veelzijdig doordat we uit miljoenen apps kunnen kiezen. Met deze apps kunnen we productiever zijn, meteen met anderen communiceren, delen, trainen of zaken uitleggen of gewoon meer plezier beleven. Maar de mobiele apps gaan gepaard met risico's. Hier zijn enkele stappen die je kan nemen om jouw apps veilig te gebruiken.

Gast redacteur

Joshua Wright is technisch directeur bij Counter Hack en een ervaren instructeur bij het SANS-instituut. Hij is auteur van SEC 575: Mobile Device Security & Ethical Hacking en Hacking Exposed: Wireless. Je kan hem via Twitter bereiken via **@joswr1ght**.

Mobiele Apps Verkrijgen

De eerste stap is je ervan te verzekeren dat je mobiele apps downloadt van een vertrouwde en veilige bron. Cybercriminelen maken en verdelen tegenwoordig mobiele apps die er legitiem uitzien. Indien je deze valse apps installeert kunnen de criminelen de controle overnemen van jouw toestel. Door enkel apps te downloaden bij officiële, vertrouwde en bekende bronnen verminder je de kans dat je een besmette app installeert. Wat je mogelijk niet beseft is dat het merk van jouw mobiel toestel jouw mogelijkheden tot het downloaden van apps bepaalt.

Apple toestellen zoals de iPad of iPhone, kunnen enkel apps downloaden van de Apple App Store. Het voordeel hier is dat Apple een veiligheidscheck uitvoert van alle mobiele apps alvorens ze worden gepubliceerd. Apple kan niet iedere besmette app spotten, maar deze beheerde omgeving verlaagt de kans op een besmette app aanzienlijk. Als Apple een app vindt waarvan men vermoedt dat het besmet is, wordt deze snel verwijderd uit de app store. Windows Phone hanteert een gelijkaardige aanpak bij het beheer van apps.

Android toestellen zijn anders. Android biedt meer flexibiliteit en maakt het mogelijk om een app te downloaden van elke locatie op het Internet. Deze flexibiliteit vraagt een grotere verantwoordelijkheid. Je moet voorzichtiger zijn met welke

© SANS Institute 2017

Mobiele Apps Veilig Gebruiken

mobiele apps je downloadt en installeert, omdat ze niet allemaal zijn nagekeken. Google heeft wel een beheerde mobiele app store zoals Apple, Google Play. De mobiele apps die je downloadt van Google Play hebben een aantal security tests doorstaan. Daarom raden we aan om enkel apps te downloaden van Google Play voor jouw Android toestellen. Download geen mobiele apps van andere websites, omdat cybercriminelen deze gebruiken om valse en schadelijke mobiele apps te verdelen, die jouw toestel kunnen besmetten. Als extra bescherming installeer je best een antivirus oplossing op jouw toestel indien mogelijk.

Om mobiele apps veilig te gebruiken, installeer je best apps van vertrouwde bronnen, installeer je updates als deze beschikbaar zijn en ken je enkel noodzakelijke app permissies toe.

Ongeacht het merk van toestel dat je gebruikt, kan je ook een extra stap nemen door apps te vermijden die splinternieuw zijn, door weinig mensen zijn gedownload, of weinig positieve feedback heeft. Hoe langer een app bestaat, hoe meer mensen het hebben gebruikt en hoe meer positieve feedback het heeft, hoe groter de kans dat de app veilig is. Stel jezelf de vraag, heb ik deze app echt nodig? Iedere app brengt niet alleen nieuwe kwetsbaarheden met zich mee maar ook mogelijke privacy issues. Wanneer je stopt met een app te gebruiken, verwijder het dan van jouw mobiel toestel (je kan het later altijd terug toevoegen wanneer je het nodig hebt). Ten slotte, jailbreak of root jouw mobiel toestel niet. Hierdoor hack je het toestel en door onvertrouwde apps te installeren wijzig of verwijder je bepaalde ingebouwde securityinstellingen en riskeer je dat de garantie en ondersteuning aan het toestel vervalt.

Permissies

Nadat je een mobiele app hebt geïnstalleerd van een vertrouwde bron, moet je ervoor zorgen dat het veilig is ingesteld om jouw privacy te beschermen. Denk goed na vooraleer je bepaalde app permissies toestaat, geef je de app zomaar permissie of heeft de app deze werkelijk nodig? Bijvoorbeeld bepaalde apps gebruiken geolocatie services. Als je toelaat dat een app altijd jouw locatie weet, dan sta je toe dat de ontwikkelaar jouw bewegingen kan volgen of zelfs de auteur toelaat om deze gegevens aan anderen te verkopen. Wil je de permissies niet toelaten, weiger dan het permissieverzoek of ga op zoek naar een andere app die voldoet aan jouw vereisten. Besef goed dat je hier veel keuze in hebt.

Mobiele Apps Veilig Gebruiken

Apps Updaten

Mobiele apps, moeten net als jouw computer en het besturingssysteem worden aangepast om up-to-date te blijven. Criminelen zoeken constant naar kwetsbaarheden in apps, hiervoor ontwikkelen ze exploits om deze kwetsbaarheden te misbruiken. De ontwikkelaars van jouw app voorzien en maken updates om deze kwetsbaarheden te repareren en zo jouw toestellen te beschermen. Hoe vaker je controleert op updates en deze installeert des te beter. De meeste toestellen laten toe om apps automatisch te laten updaten. We raden aan om deze instelling te gebruiken. Indien dit niet mogelijk is, raden we aan om minstens om de twee weken te controleren op app updates. Als jouw apps zijn geupdated, dien je nog na te gaan of de vereiste permissies correct zijn.

Meer Weten?

Ga naar securingthehuman.sans.org/ouch/archives 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 is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft 3.600 medewerkers. In 2015 realiseerde Cegeka Groep een omzet van 368 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen (Engels)

Veilig Internetten – Apps:	https://veiliginternetten.nl/themes/mobiel/apps-mobiel/
Social Engineering:	https://securingthehuman.sans.org/ouch/2017#january2017
Disposing Your Mobile Device:	https://securingthehuman.sans.org/ouch/2016#december2016
Securing Your New Tablet:	https://securingthehuman.sans.org/ouch/2016#january2016
OUCH Archives & Translations:	https://securingthehuman.sans.org/ouch/archives
Mobile Device Security Course:	https://sans.org/sec575

OUCH! Is een publicatie van SANS Securing The Human en wordt verdeeld onder de Creative Commons BY-NC-ND 4.0 license. Deze nieuwsbrief mag verder verdeeld worden en gebruikt worden in uw eigen security awareness programma, zolang u de inhoud niet wijzigt. Stuur een bericht naar ouch@securingthehuman.org voor meer informatie en voor vertalingen.

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

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