OUCH! | Februari 2015

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

Veilig blijven onderweg

Overzicht

In deze nieuwsbrief gaan we in op hoe je veilig met het Internet kan verbinden en hoe je jouw zaken gedaan krijgt tijdens het reizen.

Gastredacteur

Steve Armstrong is de Technische Directeur van CyberCPR bij Logically Secure, een gecertifieerd SANS-instructeur en een voormalig cursusauteur bij SANS. Hij is actief op Twitter als **@Nebulator** en op Google Plus: **+SteveArmstrongSecurity**.

Vooraf

Hoewel jouw netwerk thuis of op het werk mogelijk veilig zijn, moet je ervan uit gaan dat het netwerk op de baan eerder onveilig is. Je weet niet wie er nog allemaal op is en welke dreigingen ze met zich meebrengen. Enkele eenvoudige voorbereidende stappen kunnen je al een heel eind op weg brengen om je data te beveiligen tijdens het reizen. Voorzie één of twee weken op voorhand het volgende:

- Identificeer welke data je niet nodig hebt op de toestellen die je meepakt en verwijder alle overbodige informatie. Hierdoor verminder je de impact drastisch als jouw toestellen verloren raken, gestolen worden of in beslag worden genomen door douane of veiligheidspersoneel. Indien je reist voor het werk, vraag dan aan jouw leidinggevende of jouw organisatie andere toestellen voorziet dan diegenen waarmee je normaal mee werkt.
- Voor internationale reizen, ga na welke stekkertypen er in het land worden gebruikt, mogelijk dien je een adapter te voorzien om jouw toestellen op te laden. Controleer bovendien welk tariefplan je hebt bij jouw mobiele provider. Vaak hanteren mobiele providers hoge tarieven voor internationaal dataverbruik, mogelijk wil je hierdoor jouw dataverbruik uitschakelen tijdens internationaal reizen of jouw tariefplan aanpassen in functie van jouw reis.
- Installeer software waarmee je jouw toestel van op afstand kunt terugvinden en wissen, indien het verloren of gestolen raakt. Veel mobiele toestellen hebben deze functies reeds ingebouwd, hierdoor hoef je het enkel in te schakelen (houd rekening met dat je Internet toegang nodig hebt om te werken).

Een of twee dagen voor de reis:

- Update jouw toestellen, toepassingen en antivirussoftware zodat je over de laatste versies beschikt.
- Schakel alle relevante security functies in zoals firewalls op jouw toestellen.
- Voorzie al jouw mobiele toestellen met een sterk wachtwoord of passcode. Als jouw toestel dan verloren of gestolen

Veilig blijven onderweg

is, dan kan men de informatie erop niet raadplegen.

- Encrypteer al jouw toestellen, zodat de data niet kan worden geraadpleegd indien ze verloren of gestolen raakt. Sommige toestellen zoals iPhones doen dit automatisch als je een wachtwoord of passcode instelt.
- Maak een volledige back-up van al jouw toestellen. Hierdoor zal je altijd een kopie hebben op een veilige locatie indien er iets gebeurt.

Om veilig te blijven tijdens het reizen, is het belangrijk dat je jouw toestellen vooraf beveiligt en dat je ze fysiek beveiligt en weet waar ze altijd zijn. En versleutel al jouw online activiteiten.

Verloren / Gestolen toestellen

Als je aan de reis begint, zorg dan voor een goede fysieke beveiliging van jouw toestellen. Bijvoorbeeld laat jouw toestellen niet in de wagen op een zichtbare plaats achter. Criminelen deinzen niet terug om het autoraam te vernielen en alle waardevolle spullen mee te nemen die ze zien. Je kan een kabelslot voorzien om jouw toestellen vast te maken, zoals jouw laptop, als je ze alleen laat. Criminaliteit is een reëel risico, maar mensen raken eerder hun toestel kwijt dan dat het gestolen wordt. Volgens een onderzoek van Verizon, loopt men 15 keer meer kans om een toestel kwijt te raken dan dat deze wordt gestolen. Daarom controleer telkens of jouw toestellen er nog zijn, zoals wanneer je door de security gaat in een vliegveld, uit een taxi stapt of een restaurant verlaat, uit het hotel checkt of alvorens je uit een vliegtuig stapt.

Wi-Fi Toegang

Op het Internet surfen tijdens het reizen, betekent dat je vaak gebruik zal maken van publieke Wi-Fi netwerken, zoals diegene die je vindt op hotel, in een koffieshop of op het vliegveld. Het probleem met zulke Wi-Fi netwerken is dat je nooit weet wie deze heeft opgezet en wie ermee verbonden is. Net daarom beschouw je deze best als onbetrouwbaar, het is net hierom dat je al deze maatregelen hebt ondernomen om jouw toestellen te beveiligen. Bovendien gebruikt Wi-Fi radiosignalen die jouw toestel verstuurt naar het Wireless Access Point. Dit houdt in dat iedereen die dicht bij jou is deze signalen kan onderscheppen en bekijken.

Dit is de reden waarom je geen publieke Wi-Fi gebruikt, verzeker je ervan dat al jouw online activiteit versleuteld is via encryptie. Bijvoorbeeld wanneer je online surft via jouw browser, let er dan op dat alle websites een versleutelde verbinding hebben (kijk naar de https:// in de URL en het icoon van een gesloten slotje). Daarbij kan je best een VPN (Virtual Private Network) account gebruiken waardoor al jouw online activiteiten versleuteld worden. Dit kan voorzien zijn door jouw werk of

Veilig blijven onderweg

je kan VPN mogelijkheden kopen voor jouw privé activiteiten. Indien je bezorgd bent dat er geen Wi-Fi netwerken zijn die je kan vertrouwen, overweeg dan om tethering te activeren op jouw smartphone. (Opgepast: zoals we eerder hebben vermeld, kan dit prijzig zijn tijdens het internationaal reizen, kijk de tarieven na bij jouw mobiele provider).

Publieke middelen

Gebruik geen publieke computers, zoals deze in hotel lobbies, bibliotheken of cybercafés. Je weet niet wie de computer eerder heeft gebruikt en of ze mogelijk de computer hebben geïnfecteerd per ongeluk of doelbewust. Indien mogelijk, gebruik enkel toestellen die jij beheert en vertrouwt voor online activiteiten. Indien je een publieke computer moet gebruiken, gebruik dan geen diensten waarvoor je hoeft in te loggen of een wachtwoord moet typen.

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)

Passwords:	http://www.securingthehuman.org/ouch/2013#may2013
Two step verification:	http://www.securingthehuman.org/ouch/2013#august2013
Encryption:	http://www.securingthehuman.org/ouch/2014#august2014
Securing Your New Tablet:	http://www.securingthehuman.org/ouch/2013#december2013
Verizon DBIR 2014:	http://www.verizonenterprise.com/DBIR/2014/

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