OUCH! | Februari 2017

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers.

OUCH!

IN DEZE EDITIE...

Veilig blijven onderweg

Overzicht

We willen ervoor zorgen dat je het meeste haalt uit jouw toestellen, ook wanneer je onderweg bent. In deze nieuwsbrief gaan we in op hoe je best jouw toestellen verbindt met het Internet en gebruikt wanneer je onderweg bent.

Gast redacteur

Mark Williams is Enterprise Security Architect bij BlueCross Blueshield in Tenessee. Hij is ook een SANS-instructeur en voorzitter van de ISSA Chattanooga chapter. Hij heeft heel veel gereisd en begrijpt de uitdagingen als geen ander als je jouw toestellen met je meeneemt.

Vooraf

Jouw netwerk thuis of op het werk mag dan wel veilig zijn, dat betekent niet dat het netwerk op de baan ook zomaar te vertrouwen is. Je weet niet wie er nog allemaal verbonden is en wat ze uitspoken. Hier zijn een aantal eenvoudige stappen die je een heel eind op weg helpen om jezelf en jouw data te beveiligen tijdens het reizen.

- De veiligste informatie is de informatie die je niet bij je hebt. Identificeer welke informatie je niet nodig hebt op jouw toestellen en verwijder de overbodige informatie. Hierdoor verminder je de impact wanneer jouw toestellen verloren of gestolen raken of in beslag worden genomen door de douane of veiligheidspersoneel. Indien je reist voor het werk, vraag dan aan jouw leidinggevende of jouw werkgever andere toestellen voorziet dan diegene waarmee je normaal mee werkt.
- Vergrendel jouw mobiele toestellen en/of laptop met een sterk wachtwoord of PIN-code. Op die manier zal men geen toegang hebben tot het toestel als het verloren of gestolen is.
- Installeer of schakel software in op jouw toestel, zodat je vanop afstand de locatie kan zien en zelfs een remote wipe kan uitvoeren, indien het toestel gestolen of verloren is.
- Update jouw toestellen, apps en antivirussoftware zodat je over de laatste versies beschikt. Veel aanvallen focussen op systemen met verouderde software.
- Voer een volledige back-up uit van ieder toestel. Hierdoor zal je altijd een kopie hebben op een veilige locatie indien er iets gebeurt.

Veilig blijven onderweg

- Voor internationele reizen, ga na welk tariefplan je hebt voor jouw telefoon bij jouw provider. Vaak hanteren providers hoge tarieven voor internationaal dataverbruik, mogelijk wil je hierdoor mobiele data uitschakelen of een lokale prepaid SIM-kaart aanschaffen voor de reis.

Om tijdens het reizen veilig te blijven, beveilig je toestellen alvorens je vertrekt, houd ze fysiek veilig en versleutel iedere onlineactiviteit.

Verloren/Gestolen Toestellen

Als je aan de reis begint, zorg dan voor een goede fysieke beveiliging van jouw toestellen. Laat jouw toestellen niet in de wagen op een zichtbare plaats achter. Criminelen deinzen niet terug om een autoraam te vernielen en alle waardevolle spullen mee te nemen die ze zien. Criminaliteit is een groot risico, volgens een recente studie van Verizon loopt men 100 keer meer kans om een toestel te verliezen dan dat deze wordt gestolen. Controleer daarom telkens of je jouw toestellen nog hebt, zoals wanneer je door de security gaat in een vliegveld, uit een taxi stapt of een restaurant verlaat, uitcheckt in het hotel of vooraleer 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 die in hotels, koffieshops of in het vliegveld. Er zijn twee problemen met publieke Wi-Fi netwerken, je weet nooit wie deze heeft opgezet en wie er verbonden is. Net daarom dien je voorzichtig te zijn, het is net hierom dat je maatregelen hebt ondernomen om jouw toestellen te beveiligen. Wi-Fi gebruikt radiogolven, dit betekent dat iedereen die vlakbij jou zit deze signalen kan opvangen en kan meeluisteren met wat je doet. Om deze reden dien je als je publieke Wi-Fi netwerken gebruikt ervoor te zorgen dat jouw verbinding versleuteld is. Bijvoorbeeld wanneer je surft met jouw browser, bezoek dan enkel websites die versleuteld zijn. Je kan dit zien door te letten op ‘HTTPS://” in de URL en/of een gesloten hangsloticoontje in de adresbalk. Het best gebruik je een VPN (Virtual Private Network) waarmee je al jouw onlineactiviteiten versleuteld. Deze kan door het werk worden voorzien of je kan een persoonlijke VPN aanschaffen. Kan je niet meteen een publiek Wi-Fi netwerk vertrouwen, overweeg dan tethering via jouw smartphone. Waarschuwing: zoals ook eerder vermeld, mobiel dataverbruik kan kostelijk zijn wanneer je internationeel reist, kijk daarom eerst het tariefplan na.

Veilig blijven onderweg

Openbare Computers

Gebruik geen openbare computers, zoals deze in een hotellobby of in cybercafés, om in te loggen tot accounts of om vertrouwelijke gegevens te raadplegen. Je weet niet wie er allemaal de computer heeft gebruikt. Mogelijk is de openbare computer per ongeluk of met opzet besmet. Gebruik daarom enkel toestellen die je vertrouwt en beheert. Openbare computers zijn enkel goed om het weerbericht of het nieuws te raadplegen. Inloggen op accounts zoals jouw Google account kan mogelijk een uitnodiging zijn aan hackers die meekijken.

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 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)

Passphrases:	https://securingthehuman.sans.org/ouch/2015#april2015
Backups:	https://securingthehuman.sans.org/ouch/2015#august2015
Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Encryption:	https://securingthehuman.sans.org/ouch/2016#june2016
OUCH Archives / Translation:	https://securingthehuman.sans.org/ouch/archives

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