Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Vorbereitung
- Verlorene / Gestohlene Geräte
- WLAN Zugang
- Öffentliche Computer

Sicher Unterwegs

Überblick

In diesem Newsletter beschreiben wir wie Sie sich sicher zum Internet verbinden und Dinge erledigen können, während Sie auf Reisen sind.

Gastautor

Steve Armstrong ist Technischer Direktor des CyberCPR bei Logically Secure, zertifizierter SANS Ausbilder und ehemaliger SANS Kursautor. Er ist auf Twitter als **@Nebulator** und auf Google plus unter **+SteveArmstrongSecurity** zu finden.

Vorbereitung

Während Ihr Netzwerk Zuhause und am Arbeitsplatz wahrscheinlich sicher ist, sollten Sie immer davon ausgehen, dass Netzwerke zu denen Sie sich auf Reisen verbinden nicht vertrauenswürdig sind. Sie wissen nie wer diese Netzwerke ebenfalls nutzt und welche Bedrohung diese Personen darstellen. Einige einfache Maßnahmen, die Sie vor einer Reise durchführen können, tragen schon sehr viel zum Schutz Ihrer Daten auf Reisen bei. Eine oder zwei Wochen vor Ihrer Reise:

- Überprüfen Sie welche Daten Sie auf den Geräten, die Sie mitnehmen wollen, benötigen und entfernen Sie alle nicht benötigten Daten. Das kann die Auswirkungen bei Verlust, Diebstahl oder Grenzkontrollen signifikant verringern. Wenn Sie aus beruflichen Gründen verreisen, fragen Sie Ihren Vorgesetzten, ob Ihre Organisation Ihnen spezielle Ersatzgeräte für die Dauer der Reise zur Verfügung stellt.
- Für internationale Reisen sollten Sie prüfen, welche Stromstecker im Zielland genutzt werden und bei Bedarf Adapter zum Laden Ihrer Geräte besorgen. Zudem sollten Sie die Konditionen Ihres Handyvertrags prüfen. Oft verlangen Mobilfunkanbieter sehr hohe Gebühren für die Datennutzung im Ausland, daher sollten Sie die Nutzung von mobilen Datenverbindungen während Ihrer Reise entweder deaktivieren oder den Tarif passend für Auslandsreisen umstellen.
- Installieren Sie Software auf Ihren Geräten, die es Ihnen erlaubt den Standort Ihres Geräts jederzeit zu ermitteln und gegebenenfalls eine Fernlöschung auszulösen, wenn Sie es verloren haben oder es gestohlen wurde. Viele Mobilgeräte haben diese Funktionalität bereits eingebaut, Sie müssen sie wahrscheinlich nur aktivieren (bedenken Sie aber, dass diese Funktionen Internetzugriff voraussetzen).

Ein oder zwei Tage vor der Reise:

- Aktualisieren Sie Ihre Geräte, Programme und Antivirus-Software auf die jeweils neuesten Versionen.
- Aktivieren Sie alle angebrachten Sicherheitseinstellungen auf Ihren Geräten, wie z.B. Firewalls.

Sicher Unterwegs

- Versehen Sie all Ihre Mobilgeräte mit einem starken Passwort oder Passcode. So können Sie bei Verlust des Geräts sicher sein, dass niemand die darauf enthaltenen Informationen einsehen kann.
- Verschlüsseln Sie Ihre Geräte, so dass bei Verlust oder Diebstahl niemand auf die Daten zugreifen kann. Einige Geräte wie z.B. iPhones aktivieren Verschlüsselung automatisch, sobald Sie ein Passwort oder einen Passcode auf dem Gerät einrichten.
- Erstellen Sie eine vollständige Sicherung all Ihrer Geräte. So stellen Sie sicher, dass alle Daten noch einmal an einer sicheren Stelle lagern, wenn den Geräten auf der Reise etwas widerfährt.

Um auch auf Reisen die Sicherheit Ihrer Daten zu gewährleisten, sollten Sie bereits vor der Abreise die Geräte sicher konfigurieren und unterwegs sicherstellen, dass alle Online-Aktivitäten verschlüsselt sind und Sie jederzeit den Standort Ihrer Geräte kennen.

Verlorene / Gestohlene Geräte

Sobald Sie Ihre Reise antreten, achten Sie auf die physische Sicherheit Ihrer Geräte. Lassen Sie die Geräte z.B. nie in Ihrem Auto wo Passanten sie leicht sehen können, denn Kriminelle können einfach ein Fenster einschlagen und greifen sich alles Wertvolle, dessen sie habhaft werden können. Eine gute Idee ist zudem das Mitführen eines Kabelschlosses, so dass Sie Geräte (z.B. Laptops) an Gegenständen anschließen können, wenn Sie sie irgendwo unbeobachtet lassen müssen. Während die Bedrohung durch Kriminalität nicht zu vernachlässigen ist, sollten Sie doch wissen, dass es weitaus wahrscheinlicher ist ein Gerät zu verlieren als es gestohlen zu bekommen. Laut einer 10 jährigen Studie von Verizon, verlieren Menschen 15 mal mehr Geräte als gestohlen werden. Prüfen sie daher immer, ob Sie noch alle Geräte bei sich haben, wenn Sie die Flughafenkontrolle durchlaufen, ein Taxi oder Restaurant verlassen, aus dem Hotel auschecken oder aus dem Flugzeug steigen.

WLAN Zugang

Während Reisen auf das Internet zuzugreifen bedeutet häufig, öffentliche WLAN Hotspots zu benutzen, wie sie in Hotels, der örtlichen Kaffeebar oder dem Flughafen zu finden sind. Das Problem mit öffentlichen WLAN Zugängen ist nicht nur, dass Sie nie sicher sein können wer sie eingerichtet hat, Sie wissen auch nicht, wer gerade damit verbunden ist. Sie sollten daher immer als nicht vertrauenswürdig betrachtet werden, was letztendlich der Grund für die vorbereitenden Schritte vor Ihrer Abreise ist. WLAN nutzt zudem Funkwellen für die Übertragung von Daten zwischen Ihrem Gerät und dem Zugangspunkt. Jeder, der sich in räumlicher Nähe befindet, kann diese möglicherweise abfangen und Ihre Kommunikation überwachen.

Daher müssen Sie, wenn Sie öffentliche WLANs nutzen, sicherstellen, dass all Ihre Onlineaktivitäten über verschlüsselte Verbindungen ablaufen. Wenn Sie z.B. Ihren Browser benutzen, achten Sie darauf, dass Webseiten über eine verschlüsselte

Sicher Unterwegs

Verbindung aufgerufen werden, erkennbar daran dass die Adresszeile mit 'https://' beginnt und ein Vorhängeschloss anzeigt. Einen zusätzlichen Schutz bietet die Nutzung eines VPN (Virtual Private Network) Zugangs, der all Ihre Onlineaktivitäten verschlüsselt. Dieser Zugang wird Ihnen vielleicht von Ihrem Arbeitgeber bereitgestellt oder Sie können einen VPN Zugang für Ihre private Benutzung erwerben. Sollten Sie besorgt sein keinen vertrauenswürdigen WLAN Zugang zu finden, ziehen Sie in Betracht die Tethering-Funktion Ihres Smartphones zu benutzen (Warnung: Wie bereits erwähnt kann das bei internationalen Reisen sehr kostenintensiv sein, prüfen Sie unbedingt vorher Ihren Mobilfunktarif!).

Öffentliche Computer

Nutzen Sie keine öffentlichen Computer, wie z.B. in Hotel-Lobbies, Büchereien oder Internetcafés. Sie wissen nicht was jemand vor Ihnen an einem solchen Computer getan hat. Der Computer wurde möglicherweise aus Versehen oder gar absichtlich infiziert. Wenn möglich, nutzen Sie nur Geräten die unter Ihrer Kontrolle sind und denen Sie für alle Onlineaktivitäten vertrauen. Wenn Sie einen öffentlichen Computer nutzen müssen, verwenden Sie keinen Dienst der irgendeine Art von Login benötigt.

Weiterführende Informationen

Passwörter:	http://www.securingthehuman.org/ouch/2013#may2013
Zwei-Wege Authentisierung:	http://www.securingthehuman.org/ouch/2013#august2013
Verschlüsselung:	http://www.securingthehuman.org/ouch/2014#august2014
Absicherung Ihres neuen Tablet-Computers:	http://www.securingthehuman.org/ouch/2013#december2013
Verizon DBIR 2014:	http://www.verizonenterprise.com/DBIR/2014/

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

OUCH! wurde aus dem Englischen übersetzt von Marek Kreul und René Wiedewilt. Beide arbeiten für das CERT eines deutschen IT-Dienstleisters und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis