Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

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

Sicher auf Reisen

Überblick

Wir wollen Sie in die Lage versetzen, zu jeder Gelegenheit den größten Nutzen aus der Ihnen verfügbaren Technologie zu ziehen, auch wenn Sie reisen. In diesem Newsletter sprechen wir über die sichere Nutzung des Internets und Ihrer Geräte wenn Sie unterwegs sind.

Gastautor
Mark Williams ist Enterprise Security Architect bei BlueCross Blueshield Tennessee. Er ist zudem SANS instructor und Vorsitzender des Ortsverbands ISSA Chattanooga. Er ist viel gereist und versteht die Herausforderungen denen man begegnet wenn man seine Technik-Spielzeuge auf Reisen mitnimmt.

Vorbereitung

Während Ihr Netzwerk zuhause oder im Büro sicher sein mag, sollten Sie auf Reisen immer annehmen, dass Sie keinem Netzwerk mit dem Sie sich verbinden vertrauen können. Sie wissen nie wer sonst noch mit dem Netz verbunden ist und was er oder sie tut. Hier sind einige einfache Schritte die Sie befolgen sollten um sich und Ihre Daten auf Reisen zu schützen.

- Die sicherste Information ist die, die Sie nicht (dabei) haben. Überlegen Sie sich, welche Daten Sie auf keinem der Geräte benötigen, die Sie mitnehmen wollen, und entfernen Sie diese Daten von den Geräten. Dadurch werden die Gefahren bei Verlust oder Diebstahl des Geräts oder Durchsuchungen durch Grenzbehörden massiv verringert. Wenn Ihre Reise beruflich bedingt ist, fragen Sie Ihren Vorgesetzten, ob Ihre Organisation Geräte bereitstellt, die speziell für die Nutzung auf Reisen vorgesehen sind.
- Sichern Sie Ihre Mobilgeräte und/oder Ihren Laptop mit einem starken Passwort oder Code. So kann niemand auf die enthaltenen Daten zugreifen, wenn das Gerät verloren geht oder gestohlen wird. Zusätzlich sollten Sie eine Festplattenverschlüsselung installieren oder aktivieren. Auf den meisten Mobilgeräten wird das automatisch aktiviert, wenn Sie den Passwortschutz einrichten.
- Installieren oder aktivieren Sie Software, mit der Sie den Aufenthaltsort Ihres Geräts sehen und es bei Bedarf fernlöschen können.
- Aktualisieren Sie Ihre Geräte, Anwendungen und die Antivirusprogramme vor der Abreise, so dass sie auf dem neuesten Stand sind. Viele Angriffe zielen auf Systeme mit veralteter Software.
- Erstellen Sie eine Sicherungskopie aller Daten auf sämtlichen Geräten. Somit haben Sie die Daten zusätzlich sicher zuhause verwahrt, wenn den Geräten unterwegs etwas widerfährt.

Sicher auf Reisen

- Prüfen Sie für internationale Reisen, welchen Mobilfunktarif Sie haben und wie dessen Kosten im Zielland zusammengesetzt sind. Oft fallen für Datenverbrauch im Ausland unverhältnismäßig hohe Kosten an, weshalb Sie für internationale Reisen in Betracht ziehen sollten die Datennutzung zu deaktivieren oder vor Ort eine Prepaid-SIM-Karte zu erwerben.

Um auch auf Reisen sicher zu sein, sollten Sie Ihre Geräte vor möglichen Bedrohungen schützen, sie physisch absichern und all Ihre lokalen Daten und Onlineaktivitäten verschlüsseln.

Verlorene / Gestohlene Geräte

Sobald Sie Ihre Reise beginnen sollten Sie auf die physische Sicherheit Ihrer Geräte achten. Lassen Sie z.B. Ihre Geräte nie in einem PKW zurück, wo jeder Passant sie leicht sehen kann - Kriminelle werfen dann vielleicht einfach eine Seitenscheibe ein und nehmen sich alles Wertvolle, dessen sie habhaft werden können. Während Kriminalität definitiv ein Risiko ist, besteht gemäß einer kürzlich von Verizon veröffentlichten Studie ein hundertfach höheres Risiko, Geräte einfach zu verlieren als sie gestohlen zu bekommen. Prüfen Sie daher immer, ob Sie Ihre Geräte bei sich haben, wenn Sie z.B. die Sicherheitskontrolle am Flughafen oder ein Restaurant verlassen, oder wenn Sie aus einem Taxi steigen. Auch beim Auschecken aus dem Hotel oder dem Verlassen eines Flugzeugs geht gerne mal ein Gerät verloren - schauen Sie in Flugzeugen immer in die Tasche der Rückenlehne vor Ihnen!

WLAN Zugang

Zugriff auf das Internet während man reist bedeutet oft, sich mit öffentlichen WLAN Zugangspunkten zu verbinden, z.B. diejenigen in Hotels, örtlichen Cafés oder am Flughafen. Mit solchen öffentlichen WLAN Zugängen gibt es zwei Probleme: Sie wissen nie mit Sicherheit, wer sie betreibt, und wer noch mit ihnen verbunden ist. Sie sollten daher als nicht vertrauenswürdig angesehen werden - und das ist genau der Grund warum Sie all die Schritte zur Absicherung Ihrer Geräte vor Ihrer Abreise durchgeführt haben. Hinzu kommt, dass WLAN Funkwellen nutzt, was bedeutet, dass jeder in Reichweite des WLANs Ihre Kommunikation potentiell abfangen und mitschneiden kann. Sie sollten daher, wenn Sie unbedingt ein öffentliches WLAN nutzen müssen, sicherstellen, dass Ihre sämtliche Online-Kommunikation verschlüsselt ist. Wenn Sie mit Ihrem Browser eine Webseite aufrufen, achten Sie darauf dass diese Verbindung verschlüsselt erfolgt. Sie erkennen das daran, dass die Adresse mit den Zeichen 'HTTPS://' beginnt und/oder ein geschlossenes Schloss daneben angezeigt wird. Vielleicht haben Sie zudem die Möglichkeit, ein VPN (Virtual Private Network) zur Verschlüsselung Ihrer kompletten Netzwerkkommunikation zu verwenden. Ein VPN stellt Ihnen vielleicht Ihr Arbeitgeber bereit, oder Sie können auch für Ihre

Sicher auf Reisen

private Nutzung einen VPN Zugang erwerben. Wenn Sie befürchten, dass Sie keinem verfügbaren WLAN ausreichend trauen können, besteht eine weitere Möglichkeit in der Tethering-Funktion Ihres Smartphones. ACHTUNG: wie vorher schon erwähnt kann das sehr hohe Kosten nach sich ziehen, wenn Sie international reisen. Prüfen Sie die Kosten vorab mit Ihrem Mobilfunkanbieter.

Öffentliche Computer

Nutzen Sie nie öffentliche Computer, wie die in Hotel-Lobbys, Internetcafés oder Büchereien, um sich an einem Ihrer Benutzerkonten anzumelden oder auf sensible Daten zuzugreifen. Sie haben keinerlei Ahnung, wofür der Computer zuvor genutzt wurde, und ob er absichtlich oder unabsichtlich mit Schadsoftware infiziert wurde. Nutzen Sie, wann immer möglich, nur vertrauenswürdige Geräte über die Sie die Kontrolle haben. Öffentliche Computer sind bestenfalls gut, um darüber öffentlich verfügbare Informationen wie die Wettervorhersage oder Nachrichten abzurufen. Sich darüber an einem Ihrer Benutzerkonten anzumelden kann eine Einladung für Hacker sein, die Sie dabei vielleicht unbemerkt beobachten.

Weiterführende Informationen

Starke Passwörter:	https://securingthehuman.sans.org/ouch/2015#april2015
Backup & Wiederherstellung:	https://securingthehuman.sans.org/ouch/2015#august2015
Malware:	https://securingthehuman.sans.org/ouch/2016#march2016
Verschlüsselung:	https://securingthehuman.sans.org/ouch/2016#june2016
OUCH Archive / Übersetzungen:	https://securingthehuman.sans.org/ouch/archives

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 securingthehuman.sans.org/ouch/archives.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns 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, Cheryl Conley