Sieben Tipps für Cybersicherheit im Urlaub

Sommerferienzeit: Das kann heißen, zwei Wochen Camping, aber auch sechs Wochen Übersee, inklusive Arbeiten von unterwegs. Damit Daten und Geräte in fremden WLAN-Netzen geschützt bleiben, hat Sophos sieben kleine Vorsorgetipps zusammengestellt. Für einen unbeschwerten und sicheren Sommer.

Das Arbeiten im Home-Office hat die Arbeitnehmer im Hinblick auf Cybersicherheit daheim und unterwegs gut geschult. Dennoch ist das Arbeiten im eigenen Haus immer noch ein kleinerer Schutzraum für die IT als beim Arbeitsplatz vor Ort. Zugleich bietet das Netzwerk zuhause aber auch weitaus mehr Schutz als auf Reisen. Für einen sorglosen Urlaub in Sachen Cybersicherheit hat Sophos deshalb ein paar der wichtigsten Punkte zusammengefasst:

1.) Sollte ich ein Backup vor meiner Abreise machen?
Ja. Selbst wenn Sie sehr gewissenhaft über alle Geräte wachen, ein Handy oder Laptop kann immer mal herunterfallen, im Pool landen oder eine Cocktail-Dusche nehmen. Worst Case: es kann auch gestohlen werden, was im Urlaub gar nicht so unüblich ist. Also folgen Sie bitte dem Grundsatz: Das einzige Backup, das man bereut, ist das, das man nicht gemacht hat. Eine zuverlässige Sicherung vor der Abreise bedeutet auch, mal die Daten auszumisten und damit die Datenmenge zu reduzieren, die man bei einem Grenzübertritt möglicherweise angeben oder offenlegen muss (siehe unten weitere Tipps dazu).

2.) Sollte ich meine Geräte verschlüsseln?
Ja. Die meisten modernen Handys und Tablets sind ab Werk bereits vor-verschlüsselt, aber die Verschlüsselung hängt davon ab, dass man einen richtigen Sperrcode hat, der Zugang zu der verwendeten Verschlüsselung und den entsprechenden Schlüsseln ermöglicht. Suchen Sie sich einen langen Sperrcode aus. Wir empfehlen zehn Ziffern oder mehr – nein, nicht 12345 12345. Üben Sie ihn wie eine Telefonnummer. Zur Not lässt der Code sich auch verklausuliert notieren – falls man in der Schrecksekunde einen absolut nachvollziehbaren Black-Out hat. Sollte ein Laptop mit in den Urlaub kommen, ist auch hier ein sicheres Passwort und eine Festplattenverschlüsselung dringen anzuraten.

3.) Sollte ich mir Sorgen machen, wenn ich ins Ausland fahre?
Sorgen? Nein. Aber Vorsorgen wäre gut. Viele Länder mit Grenzkontrollen behalten sich als Einreisebedingung vor, dass Nutzer die mitgeführten Geräte entsperren und die Beamten einen Blick darauf gewähren lassen. Einige wenige Länder können sogar verlangen, eine so genannte forensische Kopie zu erstellen. Das bedeutet, sie kopieren jeden Sektor des Geräts, auch die Sektoren der Festplatte, die Daten enthalten, die zuvor gelöscht wurden. Dieser Vorgang kann eine ganze Weile dauern, so dass aus einem 10-minütigen Grenzübertritt mit etwas Pech eine mehrstündige Verzögerung werden kann. Manche Länder fordern nicht nur Postadresse und Telefonnummer, sondern auch E-Mail- und Social-Media-Adresse ein. Natürlich lassen sich diese Informationen verweigern, aber möglicherweise erlaubt die Urlaubsdestination dann auch keine Einreise. Es macht daher Sinn, sich vor der Urlaubsbuchung mit den technischen Einreisebestimmungen des entsprechenden Landes vertraut zu machen.

4.) Sollte ich öffentliches Wi-Fi auf meiner Reise nutzen?
Wenn Sie möchten. Die Gefahren bei der Nutzung öffentlicher Wi-Fi-Angebote sind sehr überschaubar und lassen sich gut eindämmen: Bleiben Sie bei den Anwendungen mit guter Verschlüsselung und surfen Sie auf Webseiten mit **s**icheren URLs also beginnend mit http**s**://. Wenn Sie aber in dem Land, in dem Sie sich aufhalten, auf Dienste zugreifen, für die Sie ein

spezielles digitales Zertifikat installieren müssen, bedeutet dies, dass Ihr Surfverhalten mit ziemlicher Sicherheit ausgespäht werden kann, während Sie sich dort aufhalten und sogar dann noch, wenn Sie wieder zu Hause sind. Wer kein öffentliches WLAN nutzen möchte, sollte sich eine lokale SIM-Karte mit einem Prepaid-Datentarif für die Dauer des Aufenthalts kaufen. Bitte bedenken, dass die meisten Länder von ihren Telefonanbietern verlangen, dass sie über so genannte legale Abhörmöglichkeiten verfügen. Ein mobiler Datentarif ist also nicht anonym, nur weil Sie eine SIM-Karte in einem Laden gekauft haben.

5.) Sollte ich Kiosk-PCs in Flughäfen oder Hotels nutzen?
Nein. Wir raten dringend davon ab, es sei denn, es lässt sich wirklich nicht vermeiden. Schränken Sie hier aber Anmeldungen und Preisgabe von Daten so weit wie möglich ein. Wenn Sie zum Beispiel an einem Hotelkiosk-PC eine Bordkarte ausdrucken müssen, bevor Sie zum Flughafen fahren, sollten Sie nicht gleichzeitig Ihr Facebook- oder gar das Onlinebanking-Konto überprüfen. Es gibt auf diesen Geräten schlichtweg zu viele unbekannte Komponenten und Nutzer.

6.) Wie sieht es mit Spycams in Hotelzimmern oder Airbnbs aus?
Pauschal lässt sich diese Frage nicht beantworten, aber Kameraspione in Gästequartieren sind eine ernste Sache und diese zu entdecken, ist aufgrund ihrer winzigen Größe oftmals Glückssache. Wer sich dennoch auf die Suche machen will: Schauen Sie zunächst bei offensichtlichen Verstecken nach. Uhren, die seltsam positioniert sind, doppelte Rauchmelder, elektronische Geräte and Stellen, wo sie nicht gebraucht werden, Anzeichen für digitale Geräte, die in Lüftungsschächte gequetscht wurden, und so weiter. Bei Fund, fotografieren (nicht herausoperieren, um keine Gegenforderung des Täters zu provozieren) und den Vorfall der örtlichen Polizei und Hauptgeschäftsstelle des Hotels oder Vermieters melden. Um das Risiko zu verringern, bei der Eingabe von Passwörtern oder Sperrcodes aufgezeichnet zu werden, kann die Tastatur bei der Eingabe kritischer Daten abgeschirmt werden. Das ist generell für die Nutzung sensibler Dienste mit Passworteingaben unterwegs empfehlenswert.

7.) Was ist, wenn ich meinen Arbeitslaptop mitnehmen möchte?
Diese Frage muss als erstes mit dem Arbeitgeber geklärt werden. Erlaubt er es, gibt er möglicherweise auch Ratschläge oder Anweisungen für die Benutzung in dem entsprechenden Land. Manche Arbeitgeber haben sogar dezidierte Nutzungsbedingungen für Arbeitsgeräte im Ausland.

Zum Schluss:
Die Sicherheit Ihrer Geräte sollte Ihnen nicht die Urlaubsvorfreude verderben. Bereiten Sie sich mit Hilfe der obigen Hinweise vor und nehmen Sie nur so viele Geräte mit, wie Sie wirklich benötigen. Und bei der Datenangabe gilt: haben Sie Zweifel, geben Sie eben nichts an und verschieben es auf die Zeit, wenn Sie wieder zuhause sind.

Sophos wünscht einen unbeschwerten und sicheren Sommer.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de