SANS SECURITY AWARENESS

Der monatliche Security Awareness Newsletter für Sie

Virtual Private Networks (VPN)

Übersicht

Möglicherweise müssen Sie ein öffentliches WLAN für den Internetzugang verwenden, wenn Sie unterwegs sind, z.B. wenn Sie in einem lokalen Restaurant oder Café sind oder wenn Sie sich in einem Hotel oder Flughafen befinden. Aber wie sicher sind diese öffentlichen Netzwerke und wer beobachtet oder zeichnet auf, was Sie online tun? Vielleicht vertrauen Sie nicht einmal dem Anbieter Ihres Internetzugangs und wollen sicher sein, dass er nicht überwachen kann, was Sie online tun. Schützen Sie Ihre Online-Aktivitäten und Ihre Privatsphäre mit einem sogenannten VPN (Virtual Private Network). Ein VPN ist eine Technologie, die einen privaten, verschlüsselten Tunnel für Ihre Online-Aktivitäten erstellt, was es für jeden viel schwieriger macht, Ihre Onlineaktivitäten zu beobachten oder zu überwachen. Darüber hinaus hilft ein VPN, Ihren Standort zu verschleiern, somit ist es für Websites, die Sie besuchen, viel schwieriger festzustellen, wo Sie sich befinden.

Wie funktioniert es?

Ein VPN funktioniert, indem es einen privaten, verschlüsselten Tunnel zu einem von Ihnen gewählten VPN-Anbieter erstellt. Alle Ihre Online-Aktivitäten durchlaufen diesen Tunnel und verlassen dann das Netzwerk Ihres VPN-Anbieters an ihrem Bestimmungsort. Wenn Sie beispielsweise in München ansässig sind und sich mit einem VPN-Server in Tampa, Florida, verbinden, wird jede Website die Sie besuchen denken, dass Sie sich von Tampa aus verbinden. Ein VPN ist einfach zu bedienen. Der erste Schritt besteht darin, einen vertrauensvollen VPN-Provider zu finden und dann ein Konto bei diesem zu erstellen (dies ist in der Regel kostenpflichtig). Sobald Sie ein Konto haben, laden Sie die VPN-Software herunter, installieren und konfigurieren diese. Nach der Installation und Konfiguration stellen Sie wie gewohnt eine Verbindung zum Internet her. Die VPN-Software erstellt im Hintergrund Ihren verschlüsselten Tunnel und beginnt mit dem Schutz Ihrer Privatsphäre, ohne dass Sie es überhaupt merken.

Auswahl eines VPN-Providers

Ihre Online-Aktivitäten sind nur so sicher und privat wie Ihr VPN-Anbieter. Achten Sie darauf, einen Anbieter auszuwählen, dem Sie vertrauen können. Hier sind die wichtigsten Punkte bei der Auswahl eines VPN-Dienstleisters.

⚠ **Protokollierung: Suchen Sie sich einen Dienst aus, der keine Daten sammelt und Ihre Privatsphäre achtet. Wenn Ihr VPN-Dienstanbieter keine Daten sammelt, ist es für jeden viel schwieriger zurückzuverfolgen, was Sie online getan haben.**

Wo ist der Sitz des VPN Anbieters: Verschiedene VPN Anbieter sind in unterschiedlichen Ländern beheimatet. Stellen Sie sicher, dass Sie einen VPN-Anbieter auswählen, der seinen Sitz in einem Land mit strengen Datenschutzgesetzen hat. VPN-Anbieter in Ländern mit sehr wenigen oder schwachen Datenschutzgesetzen können gezwungen sein, Informationen, die sie über Sie sammeln, weiterzugeben.

Server: Suchen Sie nach einem VPN-Dienst, der Server in den Ländern oder Städten hat, die Sie benötigen. Einige VPN-Anbieter verfügen über tausende von Servern und Standorten auf der ganzen Welt. Müssen Sie Ihre Verbindungen so aussehen lassen, als kämen sie aus einem bestimmten Land, und kann Ihr VPN-Provider dies leisten?

Kompatibilität: Suchen Sie nach Diensten, die auf verschiedenen Computern und mobilen Geräten funktionieren. Sie verwenden beispielsweise einen Windows-Laptop, ein Tablet und ein iPhone. Sie werden einen VPN-Dienst benötigen, der auf all diesen Geräten funktioniert.

Vermeiden Sie kostenlose Dienste: Seien Sie sehr vorsichtig bei "kostenlosen" VPN-Diensten, wie verdienen diese Geld und bleiben im Geschäft? Kostenlose Dienste sammeln und verkaufen womöglich Ihre Daten.

Ein VPN ist eine fantastische Möglichkeit, zum Schutz Ihrer Online-Privatsphäre beizutragen. Ein VPN schützt jedoch nicht Ihren Computer, Ihre Geräte oder Ihre Online-Konten. Selbst wenn Sie also ein VPN verwenden, sollten Sie immer die grundlegenden Sicherheitsschritte befolgen und sicherstellen, dass Ihre Geräte aktualisiert werden, Sie eine Bildschirmsperre und immer sichere, eindeutige Passwörter für alle Ihre Konten verwenden.

Gastredakteur

Phil Johnsey *(@peakreflections) ist ein IT-Profi aus Palm Beach County mit Erfahrung in den Bereichen Sicherheit, Forensik und Auditierung. Er ist SANS zertifiziert in digitaler Forensik, Security Essentials und Mitglied des OUCH Community Review Board. Seine Leidenschaft ist es, Sicherheit für andere einfach zu machen.*

Weiterführende Informationen

Personalisierte Angriffe:	https://www.sans.org/u/Sd8
Sicherung Ihrer mobilen Geräte:	https://www.sans.org/u/Sdd
Malware stoppen:	https://www.sans.org/u/Sdi