Sicherheitstipps für das mobile Arbeiten

Immer mehr Mitarbeiter nutzen ihre persönlichen WLAN-Netzwerke. Daher ist es wichtiger denn je, jedes Netzwerk vor häufigen Onlinebedrohungen zu schützen. Wenn Sie nach Lösungen für den Schutz Ihrer Daten und die Aufrechterhaltung der Produktivität suchen, stehen Sie nicht alleine da:

Mehr als 65 % der Mitglieder unseres globalen Teams arbeiten flexibel, sodass wir einen umfassenden Einblick in alle Bereiche der Onlinesicherheit haben. Im Folgenden lernen Sie einige der Methoden und End-to-End-Sicherheitslösungen kennen, mit denen unsere Teams unsere persönlichen Daten und die Daten unseres Unternehmens schützen.

7 Möglichkeiten zur Verbesserung der Onlinesicherheit

1. Schulen Sie Ihre Mitarbeiter

Wenn Sie oder Ihre Mitarbeiter auf das mobile Arbeiten umstellen, sind Schulungen eine wichtige Voraussetzung dafür, dass Ihre Mitarbeiter die erforderlichen Kenntnisse haben, um ihre Arbeit sicher auszuführen.

Sorgen Sie mit entsprechenden Schulungen dafür, dass Ihr Team die gängigen Methoden kennt, mit denen sich Cyberkriminelle Zugang zu Ihren Systemen verschaffen können, wie z. B. durch Phishing-E-Mails und schwache Kennwörter. Mitarbeiter, die darin geschult sind, Anzeichen einer Sicherheitsverletzung zu erkennen, reagieren schneller, wenn eine Bedrohung auftritt. So können sie die richtigen Maßnahmen ergreifen, damit ihre Daten sicher bleiben und nicht in die Hände von Onlineangreifern gelangen.

2. Installieren Sie Virenschutzsoftware

Zusätzlich sollten Sie zum Schutz Ihres Netzwerks auf allen Geräten, die Sie für das mobile Arbeiten nutzen, Virenschutzsoftware wie z. B. McAfee installieren. Ein Programm, das Onlinebedrohungen automatisch erkennt und beseitigt, ist von unschätzbarem Wert für die Sicherung Ihrer Produktivität. Falls Sie Fragen dazu haben, welche Software für Sie am besten geeignet ist, wenden Sie sich an einen Dell Technologies Kundenberater, der Ihnen fachkundige Anleitungen zum sicheren Arbeiten Ihres Teams gibt.

3. Richten Sie Zwei-Faktor-Authentifizierung ein

Eine der einfachsten Möglichkeiten zur Verbesserung Ihrer Sicherheit ist die Aktivierung der Zwei-Faktor-Authentifizierung für Websites und Anwendungen, die dies zulassen. Diese schnelle Maßnahme hindert Hacker daran, sich bei Ihren Konten anzumelden, wenn ein Kennwort kompromittiert wurde.

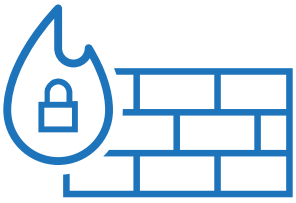
Nach der Einrichtung der Zwei-Faktor-Authentifizierung erhalten die Nutzer eine zweite Anfrage an ihr persönliches Gerät und werden zur Eingabe eines zeitkritischen Kennworts oder einer spezifischen Kennung wie z. B. eines Fingerabdrucks oder eines Netzhautscans aufgefordert, um Zugriff auf das Unternehmensnetzwerk zu erhalten. So werden für den unglücklichen Fall, dass Ihr Kennwort gestohlen wird, zusätzliche Hindernisse geschaffen, die Angreifer aufhalten, bevor sie Ihre Daten erreichen können.

DELL Technologies

4. Erstellen Sie komplexe Kennwörter

Die Gefahr durch Hacker und Onlinebedrohungen nimmt täglich zu. Es ist entscheidend, ihren Taktiken immer einen Schritt voraus zu sein. Dabei bieten komplexe Kennwörter eine der effizientesten Möglichkeiten, Angreifer abzuwehren.

Die Erstellung komplexer Kennwörter muss nicht kompliziert sein. Wählen Sie einfach ein Kennwort, das Klein- und Großbuchstaben, Satzzeichen, Ziffern und Sonderzeichen enthält. Beachten Sie folgende Best Practices für Kennwörter: Bewahren Sie Ihre Onlinekennwörter weder in physischer noch in digitaler Form auf. Verwenden Sie keine Wörter oder Ausdrücke, die persönlich mit Ihnen in Verbindung gebracht werden können, wie z. B. Spitznamen oder Geburtstage. Und nicht zu vergessen: Erstellen Sie für jede Website ein eindeutiges Kennwort. Je eindeutiger, desto besser!

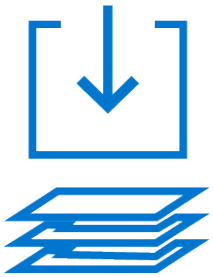


5. Nutzen Sie eine Firewall

Falls das Arbeiten im Homeoffice für Sie oder Ihr Unternehmen neu ist, bietet eine Firewall wie SonicWall leistungsstarke Intrusion Prevention, Blockierung von Malware, Inhalts-/URL-Filterung und Anwendungskontrolle. So ist Ihr Team vor Onlinebedrohungen geschützt, ganz gleich, wie groß oder klein diese sind. Eine Firewall bietet außerdem sicheren mobilen Zugriff, sodass die Mitarbeiter von überall aus sicher auf Dateien zugreifen können – direkt mit ihren persönlichen Geräten.

6. Sichern Sie Ihre Daten

Von Cyberangriffen bis hin zu einfachen menschlichen Fehlern gibt es zahlreiche Möglichkeiten für eine Kompromittierung Ihrer Daten. Die Sicherung von Dateien und Daten bietet Ihnen zusätzliche Sicherheit für den Fall, dass der Zugriff auf Ihre Dateien nicht mehr möglich ist. Die Nutzung einer Hybrid-Cloud-Lösung, die Cloud-Anwendungen mit Ihrem eigenen Server kombiniert, ermöglicht Ihnen die zuverlässige Speicherung der Onlineressourcen Ihres Unternehmens an einem sicheren Ort außerhalb der Reichweite von Hackern und Scammern.



7. Richten Sie ein VPN (virtuelles privates Netzwerk) ein

Wenn Sie Ihr Team für das mobile Arbeiten einrichten, ist die Nutzung eines virtuellen privaten Netzwerks unerlässlich, um für die Sicherheit Ihrer Unternehmensdaten zu sorgen und gleichzeitig den einzelnen Mitarbeitern den Zugriff auf E-Mails, Dateien und andere Systeme des Unternehmens zu ermöglichen.

Hierzu werden Sie über Ihren Internetdienstanbieter (ISP) mit einer Gruppe von Servern verbunden. Sobald Sie eine Verbindung zu Ihrem VPN hergestellt haben (auch als „Tunneling“ bekannt), fungieren diese Server als Ihre neue sichere „Heimatadresse“ im Internet und schränken den Zugriff von Akteuren außerhalb des Tunnels ein. Während Sie im Internet surfen, werden alle von Ihnen gesendeten und empfangenen Daten verschlüsselt, sodass Sie von zu Hause aus arbeiten können, ohne der Gefahr böswilliger Onlineaktivitäten ausgesetzt zu sein.

Wägen Sie bei der Auswahl Ihres VPN-Anbieters ab, welche Sicherheit Ihnen zu welchen Kosten geboten wird. Je nach Ihren Anforderungen und der Art der Dateien und Inhalte, auf die Sie zugreifen, benötigen Sie möglicherweise ein robusteres Sicherheitspaket. Bei Fragen zur richtigen Sicherheitsoption für Ihr Unternehmen sind wir gerne für Sie da. Wenden Sie sich an unsere Experten für eine individuelle Beratung zu sicherem Arbeiten von überall.

Sprechen Sie noch heute mit einem Berater

0800-724 49 65

DELL Technologies