Sicherer Fernzugriff auf Unternehmensdaten

„Virtuelle Private Netzwerke“ sorgen unterwegs für verschlüsselte Verbindungen

Der Überall-Zugriff auf Kunden- und Projektdaten per Internet macht den Arbeitsalltag für SHK-Handwerksbetriebe komfortabler. Eine beliebte und sichere Lösung ist der sogenannte Fernzugriff über ein „Virtuelles Privates Netzwerk“ (VPN).

Bild: Pixelio/Antje Delater

Wenn SHK-Handwerker unterwegs immer die aktuellsten Kunden- und Projektdaten nutzen wollen, gibt es grundsätzlich zwei Möglichkeiten: Entweder sie kopieren die jeweils aktuellsten Versionen täglich im Büro manuell auf ihre Notebooks, Smartphones und Tablets – oder sie nutzen eine Zugriffsmöglichkeit per Internet. Besonders komfortabel und sicher ist der Fernzugriff auf Daten im Büro über ein virtuelles privates Netzwerk, kurz VPN. Der größte Unterschied im Vergleich zu einem herkömmlichen, öffentlichen WLAN: Das VPN sorgt für eine verschlüsselte Verbindung, sodass keine Daten von Hackern abgefangen werden können.

ÜBERALL-ZUGRIFF AUF AKTUELLE DATEN

Technisch funktioniert das so: Über das VPN realisiert ein sogenannter „Client“ – zum Beispiel ein Smartphone oder Tablet – eine verschlüsselte Direktverbindung zu einem VPN-Server, über den die Firmendaten im Büro abrufbar sind. Der VPN-Server ist zum Beispiel ein einzelner PC im Firmennetzwerk oder ein Router, über den man Zugriff auf die Daten im gesamten Firmen-Netzwerk hat. Der Vorteil liegt auf der Hand: So arbeiten alle Kollegen im Büro und unterwegs immer nur mit den aktuellsten Datei-Versionen. Gleichzeitig entfällt das zeitaufwendige Kopieren von Daten auf verschiedene Geräte.

MINDESTGESCHWINDIGKEITEN FÜR VPNS

Um ein VPN von unterwegs aus sinnvoll zu nutzen, sollten zwei Voraussetzungen vorliegen:

- Die Internetverbindung des mobilen Geräts muss stabil sein und mindestens auf UMTS-Niveau liegen (384 kBit/s). Noch besser und schneller sind Verbindungen per HSDPA oder LTE.
- Aber auch die Internetverbindung des angebundenen VPN-Servers im Büro sollte eine gewisse Mindestgeschwindigkeit aufweisen, damit Datenzugriffe nicht zur Geduldsprobe werden. Da DSL-Anschlüsse typischerweise sehr schnelle Downloads, aber nur langsame Uploads erlauben, sollte für die Einrichtung eines VPN mindestens DSL 16000 vorhanden sein. Der Upload liegt bei

Android-Gerät per VPN mit Firmennetzwerk verbinden

Hinweis: Je nach Geräte-Hersteller und Android-Version können sich die Namen der Menüpunkte und die einzelnen Schritte leicht unterscheiden.

- Öffnen Sie die „Einstellungen“ auf Ihrem Android-Gerät.
- Wählen Sie unter „Netzwerke und Verbindungen“ bzw. „Drahtlos und Netzwerke“ den Punkt „Mehr“ bzw. „Weitere Verbindungseinstellungen“.
- Öffnen Sie den Menüeintrag „VPN“.
- Tippen Sie auf „VPN hinzufügen“ oder das „+“.
- Vervollständigen Sie das VPN-Profil mit den korrekten Daten. Diese erhalten Sie bei Bedarf vom Administrator Ihres Firmennetzwerks. Klicken Sie abschließend auf „Speichern“.
- In Zukunft können Sie sich nun bequem mit einem Klick auf den Verbindungsnamen in Ihr VPN einloggen.

solchen Anschlüssen in der Regel bei 1024 kBit/s, was für Fernzugriffe die untere Grenze darstellt.

Ferner ist zu beachten, dass bei einem aktivierten VPN auf einem mobilen Gerät wirklich alle Daten den Umweg über das Firmennetzwerk machen. So werden Downloads aus anderen Quellen oder das Surfen im Internet eventuell ausgebremst.
Sind alle Voraussetzungen erfüllt, lässt sich der Fernzugriff selbst über mehrere Wege realisieren: Betriebssysteme wie Windows, Android, MacOS oder iOS bringen bereits eigene Werkzeuge mit, um ein VPN einzurichten. Je nach vorhandener Hard- und Software ist es aber nicht immer einfach, ein eigenes VPN zu konfigurieren. Deshalb gibt es andere Lösungen, die auch technische Laien in kurzer Zeit umsetzen können.

HARD- UND SOFTWARE-LÖSUNGEN

Besonders praktisch sind Router, die VPN-Funktionen direkt unterstützen. Beispiele sind verschiedene Modelle von AVM, Lancom oder Zyxel. Hier lässt sich am Router die entsprechende Konfiguration vornehmen, welche Daten für Zugriffe über ein VPN freigegeben werden. Der Zugriff von unterwegs erfolgt dann besonders komfortabel über entsprechende Apps, die einige Routerhersteller kostenlos zum Download anbieten.
Wenn im Betrieb kein Router mit direkter VPN-Unterstützung vorhanden ist, kann man alternativ einen PC im Firmennetzwerk als sogenanntes „Gateway“ nutzen: Zur Einrichtung des VPN, auf das dann andere Notebooks oder PCs zugreifen können, gibt es einfache Software-Lösungen wie Wippien oder Ammyy Admin. Mit einigen dieser Lösungen lassen sich Rechner auch komplett fernsteuern, sofern man diese sogenannte „Fernwartungsfunktion“ nicht deaktiviert.

VPN MIT MOBILEN GERÄTEN

Wenn im eigenen Betrieb bereits ein VPN-Server eingerichtet ist, kann man mobile Geräte wie Smartphones und Tablets in wenigen Schritten direkt mit dem Firmennetzwerk verbinden (s. Kasten). Ganz ohne VPN-Server lässt sich ein Datenzugriff aber auch über Apps realisieren, die es von verschiedenen Anbietern als kostenlose oder kostenpflichtige Version gibt. Hier muss auf beiden Seiten – also zum Beispiel auf dem Tablet eines Mitarbeiters und einem Büro-PC – die entsprechende Software installiert werden. Auf diese Weise funktionieren zum Beispiel die Software-Lösungen „TeamViewer“ oder „Any Desk“. Da die Einrichtung und Anwendung bei den verschiedenen Apps unterschiedlich funktioniert, stellen die Anbieter online oder in den Apps selbst entsprechende Anleitungen bereit.

Autor: Thomas Busch

iOS-Gerät per VPN mit Firmennetzwerk verbinden

Hinweis: Je nach Modell und iOS-Version können sich die Namen der Menüpunkte und die einzelnen Schritte leicht unterscheiden.

- Öffnen Sie die „Einstellungen“ auf Ihrem iOS-Gerät.
- Scrollen Sie herunter und wählen Sie den Punkt „Allgemein“.
- Scrollen Sie wieder herunter und öffnen Sie den Menüeintrag „VPN“.
- Tippen Sie auf „VPN hinzufügen“.
- Vervollständigen Sie das VPN-Profil mit den korrekten Daten. Diese erhalten Sie bei Bedarf vom Administrator Ihres Firmennetzwerks. Klicken Sie abschließend oben rechts auf „Fertig“.
- Um das VPN künftig zu aktivieren, klicken Sie auf „Einstellungen“ und schalten Sie den Schiebeschalter rechts neben dem neuen Eintrag „VPN“ auf „an“.
- Die VPN-Verbindung ist aktiv, wenn in der Symbolleiste oben rechts ein VPN-Symbol zu sehen ist.

Wichtige Fachbegriffe kurz erklärt

DSL: Abkürzung für „Digital Subscriber Line“ (digitale Teilnehmer-Anschlussleitung). Eine digitale Übertragungstechnik, mit der ein schneller Breitband-Internetzugang über das Telefonnetz realisiert wird.
Hacker: Ein Hacker nutzt Sicherheitslücken in Computersystemen aus, um sich übers Internet unberechtigt Zugang zu fremden PCs zu verschaffen. Sein Ziel: Die Kontrolle über einen Rechner zu übernehmen oder Daten zu stehlen.
HSDPA: Die Technologie „High Speed Downlink Packet Access“ kann die Datenrate eines UMTS-Zugangs theoretisch auf bis zu 14,4 Megabit pro Sekunde beschleunigen. Mit HSDPA+ sogar auf bis zu 42,2 MBit/s.
LTE: Abkürzung für „Long Term Evolution“ (frei übersetzt: Langzeitentwicklung). Diese aktuelle Mobilfunktechnik der vierten Generation (4G) ermöglicht theoretisch Download-Geschwindigkeiten bis zu 500 Mbit/s. In der Praxis sind es meist weniger.
Router: Ein Router regelt den Übergang zwischen einem lokalen Netzwerk und dem Internet. Per WLAN können so zum Beispiel mehrere Geräte wie PCs oder Smartphones drahtlos auf das Internet zugreifen. Außerdem lassen sich verschiedene Geräte über einen Router miteinander vernetzen.
UMTS: Der Übertragungsstandard „Universal Mobile Telecommunications Systems“ kann Übertragungsraten von bis zu
384 Kbit/s erreichen.
WLAN: Abkürzung für „Wireless Local Area Network“ (drahtloses lokales Netzwerk). Bezeichnet die kabellose Verbindung über ein Funknetzwerk.

www.avm.de
www.lancom.de
www.zyxel.com
www.wippien.com
www.ammyy.com