Mit Sicherheit im Homeoffice

Firewall, Virenschutz und VPN – die wichtigsten Infos und Tipps, damitFirmendaten auch im Homeoffice sicher sind.

27.01.2021, 15:29

© PESHKOVA, ADOBESTOCK

Laptop und Internet – schon ist man im Homeoffice. Dabei gilt es aber, Firmendaten zu schützen.

Die Einigung von Regierung und Sozialpartnern für das Arbeiten im Homeoffice ist nun unter Dach und Fach. Doch auch abseits von arbeitsrechtlichen Aspekten gilt es, wichtige sicherheitstechnische Vorkehrungen zu treffen, damit Firmendaten nicht in falsche Hände gelangen. „Private Computer sollten auf keinen Fall ins Firmennetzwerk eingebunden werden. Stattdessen sollte man Mitarbeitern fürs Homeoffice einen Laptop zur Verfügung stellen, der vom Systemadministrator mit allen notwendigen Schutzeinrichtungen und Programmen ausgestattet wurde", empfiehlt der Obmann der Fachgruppe UBIT, Dominic Neumann. Die Kosten für die Anschaffung seien wohl geringer als der mögliche Schaden.

Wo die Risiken lauern

Die Sicherheitsrisiken im Homeoffice beginnen schon beim Zugang ins Internet. Hier schafft eine Firewall Abhilfe, die sich auf dem jeweiligen Router oder Computer einrichten lässt. Die Firewall schützt den Rechner vor Zugriffen von außen. Eine weitere wichtige Maßnahme ist der Virenschutz. „Auf neun von zehn Computern am Arbeitsplatz befindet sich Schadsoftware", so Neumann. „Antiviren-Programme sorgen dafür, dass diese weniger Schaden anrichten kann."

Der nächste Aspekt ist die Übermittlung der Daten mittels VPN (Virtual Private Network). „Dabei wird ein Tunnel aufgebaut durch den Daten verschlüsselt übertragen werden", erklärt Neumann. Auch wo die im Homeoffice bearbeiteten Daten gespeichert werden, ist ein (Un)sicherheitsfaktor – so kann man etwa auf einen firmeninternen Server zugreifen oder man speichert in einer Cloud, was in vielen Fällen sinnvoll ist. Die allseits beliebte „Dropbox" ist allerdings kein sicherer Ort. „In öffentlichen Clouds haben Firmendaten nichts verloren. Empfehlenswert ist es, eine private Cloud einzurichten, zu der nur berechtigte Personen Zugriff haben", so der Fachmann. Professionelle Lösungen gibt es etwa von Microsoft, Google, Apple oder Amazon.

Und auch bei Videokonferenzen gilt es sicherzustellen, dass niemand mithört. „Das im ersten Lockdown häufig verwendete Zoom ist in Bezug auf Sicherheit mit einem offenen Scheunentor vergleichbar“, so Neumann. Auch hier solle man auf Lösungen sicherer Anbieter zurückgreifen, etwa Microsoft Teams, Google Talks oder Apple Facetime.

Ob darüber hinausgehende Sicherheitsmaßnahmen nötig sind, hängt auch von der Tätigkeit ab. Ein Forschungsunternehmen hat andere Anforderungen an die Datensicherheit als eine Tischlerei.

Das könnte Sie auch interessieren

Sonnige Aussichten für die PV-Branche

Ob auf Dächern, Fassaden, Terrassen oder Carports: Für Photovoltaik-Lösungen gibt es laufend neue Ideen. Welches Potenzial gebäudeintegrierte PV hat. › mehr

Kräfte bündeln für den Green Deal

Mit Blick auf die Klimakrise präsentiert sich die heimische Industrie als Teil der Lösung – und unterstützt Unternehmen mit einer neuen Plattform. › mehr

Quelle:https://news.wko.at/news/steiermark/Mit-Sicherheit-im-Homeoffice.html