IT-TIPP

essendi it
IT-Beratung und -Entwicklung

IT-Sicherheit in Coronazeiten

Wie erreicht man einen sicheren Zugriff aufs Firmennetzwerk vom Homeoffice aus?

Auch wenn aktuell die Kontaktbeschränkungen gelockert werden, hat Corona uns fest im Griff. Häufig wird vom Homeoffice aus gearbeitet. Während das Coronavirus so häufig in Schach gehalten werden kann, steht digitalen Viren und weiteren digitalen Gefahren/Angriffen manche Türe offen.

Viele Arbeitgeber ermöglichen derzeit Mitarbeitern mit Computerarbeitsplätzen, von zuhause aus zu arbeiten. So wird die Ansteckungsgefahr im Unternehmen und auf dem Weg dorthin minimiert. Die Tätigkeit vom sogenannten „Homeoffice" aus ist für viele Firmen allerdings noch Neuland. In diesem Kontext müssen umfassende technische Voraussetzungen geschaffen werden, um die Sicherheit der Firmendaten und der Zugriff auf firmeneigene Anwendungen zu gewährleisten.

Grundsätzlich gibt es mehrere Möglichkeiten, einen Heimarbeitsplatz einzurichten. Im Idealfall hat oder bekommt der Mitarbeiter ein firmeneigenes Notebook, das für die virtuelle Firmenumgebung eingerichtet ist und über einen aktuellen Virenschutz verfügt. Möchte der Mitarbeiter damit von zuhause aus arbeiten, muss er in der Regel auf das Firmennetzwerk zugreifen. Natürlich darf ein Firmennetz nicht öffentlich für jeden über das Internet zugänglich sein. Deshalb wird per Software, die auf dem Notebook (Client) installiert ist, oder speziellem Router ein privates Netzwerk hergestellt, das sogenannte VPN (Virtual Private Network).

Die Verschlüsselung der darüber übertragenen Daten erfolgt entweder über einen Pre-Shared Key (PSK), der nur den beteiligten Teilnehmern bekannt ist. Die ausgetauschten Daten können nur mit diesem speziellen PSK entschlüsselt werden. Ebenso kann ein Zertifikat eingesetzt werden, über das sich der Client am Netzwerk authentifiziert und die übertragenen Daten verschlüsselt werden.

Eine weitere Alternative ist der Zugang über den sogenannten SSL-VPN. Für diese Variante ruft der Mitarbeiter eine bestimmte Internetadresse auf, die durch ein SSL-Zertifikat geschützt ist und loggt sich mit Benutzername und Passwort ein. Durch den so entstandenen Tunnel kann er nun im Firmennetz arbeiten, ohne dass Internetkriminelle Daten abfangen oder in das interne Netz gelangen können.

Über das eingesetzte Zertifikat werden die Kommunikationspartner schon beim Einloggen authentifiziert. Die anschließende Datenübertragung wird automatisch verschlüsselt. Zudem stellt das Zertifikat die Integrität der übermittelten Daten sicher. Man kann also sichergehen, dass die Daten unverändert weitergegeben werden und unverändert ankommen. Erkennbar ist eine durch ein Zertifikat abgesicherte Internetseite am „s" in https:// oder an einem kleinen Schloss-Symbol ganz links in der Adresszeile des Browsers.

Egal, ob für die Arbeit vom Homeoffice aus private oder firmeneigene Computer genutzt werden, ist ein aktueller, verlässlicher Virenschutz unumgänglich. Befindet sich nämlich ein Virus auf dem Rechner, den man z. B. bei der privaten Nutzung über WLAN „eingefangen" hat, kann er mit den Arbeitsdaten über VPN auf das Firmennetzwerk übertragen werden. Deshalb sollten Arbeitgeber und Arbeitnehmer unbedingt festlegen, wie der für die Homeoffice-Tätigkeit genutzte Computer abgesichert sein muss und wofür er verwendet werden darf.

Wir bei essendi it entwickeln IT-Lösungen und Software für Finanzdienstleister, Handel und Industrie auf aktuellem technologischem und sicherheitstechnischem Niveau. Dabei sind wir spezialisiert auf IT-Sicherheit und Zertifikatemanagement.

essendi it
IT-Beratung und -Entwicklung

essendi it GmbH
Dolanallee 19
74523 Schwäbisch Hall
Telefon 07 91-94 30 70-12
Internet: www.essendi.de