Digitale Sicherheit im Homeoffice

Seit Ausbruch der Corona-Pandemie arbeiten Millionen Beschäftigte aus dem Homeoffice. Eine der vielen Herausforderungen, mit denen sich Unternehmen durch die veränderten Arbeitsbedingungen befassen müssen, ist die Gewährleistung von IT-Sicherheit am Arbeitsplatz zu Hause. Besonders wenn die Remote-Mitarbeitenden auf eigene Heimnetzwerke und Geräte angewiesen sind, tauchen unzählige Risiken auf.

Phishing-Mails sind eine beliebte Methode von Angreifern, um an sensible Daten der Mitarbeitenden zu gelangen.

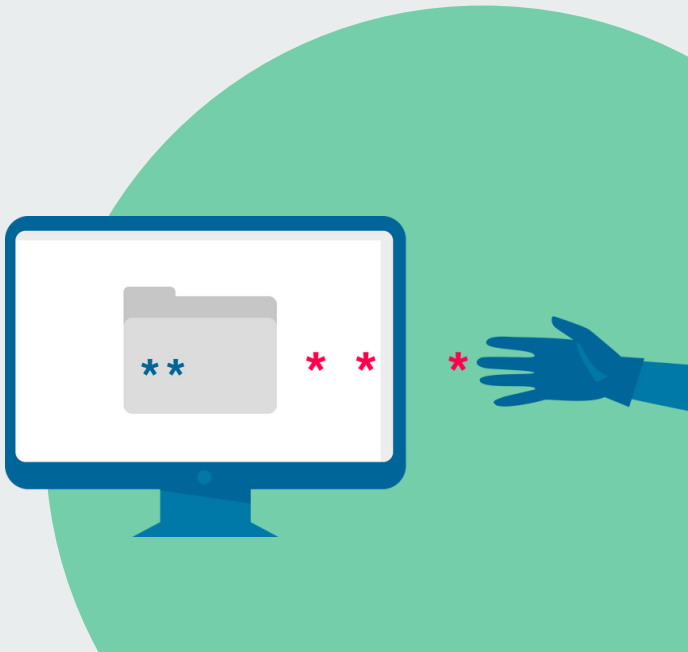
Informieren und sensibilisieren Sie regelmäßig zu den Gefahren im Homeoffice. Mitarbeitende zählen zwar zur größten Sicherheitslücke, gleichermaßen aber auch zum besten Abwehrschirm gegen potenzielle Angriffe.

Durch die Nutzung von privaten Geräten für berufliche Zwecke können unerkannte Viren in Ihr Unternehmensnetzwerk gelangen. Private Geräte sind wesentlich anfälliger für Schadsoftware als Firmengeräte.

Erstellen und definieren Sie Homeoffice-Richtlinien für die berufliche und private Nutzung digitaler Geräte. Kommunizieren Sie diese klar an Mitarbeitende.

Nicht verwaltete Mobilgeräte bieten potenziellen Angreifern einen zusätzlichen Weg, um auf Ihr Unternehmensnetzwerk zuzugreifen.

Mit einer zentralen Mobile-Device-Management (MDM)-Lösung kann die Sicherheit auf jedem einzelnen Gerät im Netzwerk gewährleistet werden. Es können Protokolle erstellt werden, um Maßnahmen im Falle einer Bedrohung zu ergreifen. Darüber hinaus können hochsensible Daten ferngesteuert und Benutzerauthentisierungen ermöglicht werden.



TISiM
Einfach. Sicher. Machen.

Durch die Nutzung von öffentlichen WLAN-Zugängen sind Angreifer in der Lage Ihre Daten auszuspähen und zu manipulieren.

Verwenden Sie für unterwegs und zuhause ein Virtual Private Network (VPN), das sämtliche Daten via Internet grundsätzlich in verschlüsselter Form überträgt. Stellen Sie grundsätzlich sicher, dass Ihre Geräte sich nicht automatisch in fremde, offene WLAN-Netzwerke verbinden.

Benutzername und Passwort sind zu schwach und vereinfachen es Angreifern durch die erste wichtige Verteidigungslinie in das Unternehmensnetzwerk zu gelangen.

Eine Mehr-Faktor-Authentisierung (MFA) hat eine wichtige Funktion bei jeglichen Zugangspunkten im Internet. Sie steigert die Sicherheit, indem sie mindestens zwei unterschiedliche Nachweise bei der Anmeldung eines Accounts fordert, z.B. ein Passwort und ein zusätzlicher Fingerabdruck, oder ein Passwort und eine zusätzliche Bestätigung über das Mobiltelefon.

Schwachstellen in Software und Betriebssystemen stellen Sicherheitslücken dar, die von Hackern ausgenutzt werden können, um bösartige Viren auf Ihr System zu übertragen.

Zeitnahe und regelmäßige Software-Updates sind unentbehrlich, um eine nachhaltige Immunität Ihrer Systeme zu gewährleisten. Eine Gefährdung wird somit abgewehrt, bevor sie überhaupt Schaden anrichten kann.

Nutzen Sie die automatischen Update Funktionen in den Einstellungen Ihrer Software-Programme und Applikationen auf Ihrem Computer und Smartphone.

Ermitteln Sie jetzt ihren IT-Sicherheitsbedarf mit dem kostenfreien Sec-O-Mat der Transferstelle IT-Sicherheit im Mittelstand.
www.sec-o-mat.de

Gefördert durch:
Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages