protea networks

"Bleiben Sie während dem Oktoberfest bitte im Homeoffice"

So lautet die Anweisung der HR Abteilung einer guten Freundin von mir. Sie arbeitet in einer Agentur und seit Beginn der Pandemie arbeitet dort praktisch die gesamte Belegschaft zu 70% von Zuhause aus. Und wo remote work früher noch als absolute Ausnahme galt, gehört es mittlerweile zur "neuen Normalität". Ein Wendepunkt für Arbeitnehmer, Recruiting, weltweite Beschäftigung und die soziale Mobilität. Remote Work revolutioniert das Arbeitsumfeld, stellt aber auch ein erhebliches Sicherheitsrisiko für die bestehenden IT-Infrastrukturen dar, das berücksichtigt werden muss.

Auch der Arbeitsplatz daheim muss ein Secure Workplace sein.

Obwohl mobiles Arbeiten immer häufiger vorkommt, sind IT-Sicherheitsmaßnahmen oft immer noch nur auf den Perimeter bezogen, d. h. sie konzentrieren sich auf die Vorgänge innerhalb des Büros und des Unternehmensnetzwerks. Doch genau das muss sich ändern - denn wenn Mitarbeiter von außerhalb des Firmengeländes auf Unternehmensdaten und -systeme zugreifen, steigt das Potenzial für Sicherheitsrisiken. Im Folgenden finden Sie Beispiele für Sicherheitsprobleme bei der Fernarbeit:

Ungesicherte Wi-Fi-Netzwerke: die Verwendung unzureichend gesicherter öffentlicher oder privater Wi-Fi-Netzwerke für den Zugriff auf Unternehmensdaten und -systeme könnte das Unternehmensnetzwerk einem unbefugten Zugriff aussetzen.

Geringe Visibilität: wenn Mitarbeiter von zu Hause aus arbeiten, verliert das IT-Personal den Überblick über die von ihnen genutzten Endgeräte und das möglicherweise gefährliche Benutzerverhalten.

Der Faktor Mensch: die menschliche Natur stellt eine der größten Sicherheitsbedrohungen dar. Mitarbeiter, die sich nicht über Sicherheitsprobleme, wie z. B. Phishing, im Klaren sind, können anfällig für Cyberangriffe sein. Mitarbeiter, die abgelenkt sind, können unabsichtlich ihre Anmeldedaten an einem öffentlichen Ort preisgeben.

Verwendung des eigenen Computers oder Tablets: die Verwendung von privaten Geräten wie Laptops oder Mobiltelefonen für die Arbeit wird immer häufiger, was zu einer Verbreitung von Geräten führt, die möglicherweise nicht den Sicherheitsanforderungen des Unternehmens entsprechen.

Mangelnde Sicherheitskenntnisse und -schulungen für Mitarbeiter im Homeoffice: Mitarbeiter, die nicht in bewährten Sicherheitspraktiken geschult wurden, verwenden mit größerer Wahrscheinlichkeit z. B. schwache Passwörter und setzen ihr Unternehmen anderen Gefahren aus.

Die richtige Sicherheit am remote Arbeitsplatz kann ein komplexes Thema sein. Wenn Sie einen zuverlässigen Partner für die Sicherheit Ihrer Mitarbeiter benötigen, wenden Sie sich an **m.seele@proteanetworks.de**. Wir betreuen Sie ganzheitlich, beraten unabhängig und lösen individuell – nur so können wir Ihr Sicherheitsniveau nachhaltig garantieren. Auf jeden Fall gehören aber folgende Maßnahmen zu den "Basics", um Gefahren im Homeoffice zu begrenzen und einzudämmen: eine umfassende Sicherheitsrichtlinie, die Implementierung starker Sicherheitsprotokolle und -technologien für den Fernzugriff, wie z. B. die Multi-Faktor-Authentifizierung (MFA) und die Verwendung virtueller privater Netzwerke (VPNs), die Schulung der Mitarbeiter zur Erkennung von Risiken und die Stärkung der allgemeinen Sicherheitsrichtlinien (z. B. starke, häufig geänderte Passwörter).

Wir empfehlen jedem Unternehmen, das Thema Sicherheit im Homeoffice anzugehen. Schließlich wollen wir ja alle, dass das Einzige was O'zapft wird, das Wiesnbier kommenden Samstag ist.

Michael Seele
Geschäftsführer und Leitung der Technik, Protea Networks GmbH