Betriebswirtschaftliches Forschungszentrum für Fragen der mittelständischen Wirtschaft e.V. an der Universität Bayreuth

Informationssicherheit im Home-Office

Die Corona-Krise stellt jedes Unternehmen vor bisher unbekannte Herausforderungen. Die Einschränkung von persönlichen Kontakten bedeutet oft, dass sich der Ablauf des Tagesgeschäfts verändert. Heimarbeit ist dabei die häufigste Maßnahme, die Arbeitgeber treffen, um die Ansteckungsgefahr ihrer Mitarbeiter zu reduzieren. Unterdessen muss die Sicherheit interner Informationen gewahrt bleiben, unabhängig davon, ob die Mitarbeiter vor Ort oder bei sich zu Hause sind. Im Folgenden möchten wir Ihnen daher einige Praxistipps aufzeigen, um auch in Zeiten von Online-Meetings, Remote-Desktop-Verbindungen und Telefonkonferenzen auf der sicheren Seite zu sein.

1. Einrichtung eines Büros im eigenen Wohnraum

Die Arbeit von zuhause ist eine Umstellung für viele Arbeitnehmer. Um die Informationssicherheit auch im Home-Office zu gewährleisten, sollten Arbeitnehmer folgende Punkte beachten:

- Bei der Heimarbeit sollte ein gesonderter Bereich geschaffen werden, der getrennt vom restlichen Wohnraum (z.B. in einem abschließbaren Zimmer) liegt.

- Manchmal kann es notwendig sein, dass interne Dokumente nach Hause mitgenommen werden müssen. Solche Akten sind – auch vor anderen Bewohnern – zu schützen. Sie dürfen nicht offen auf dem Schreibtisch liegen gelassen werden und sollten abgeschlossen verwahrt werden. Die Entsorgung durch den Hausmüll ist nicht zu empfehlen. Sollte dies dennoch erforderlich sein, sollten die Dokumente durch einen Aktenvernichter unwiederbringlich zerstört werden. Bei besonders vertraulichen Dokumenten sollten Sie prüfen, ob die Sicherheitsstufe Ihres Aktenvernichters ausreichend ist.

- Bei der Einrichtung des Arbeitsplatzes sollte – sofern möglich – darauf geachtet werden, dass die Bildschirme nicht durch Fenster von außen eingesehen werden können.

- Wenn Telefongespräche oder Videokonferenzen geführt werden, sollte die eigene Gesprächslautstärke so angepasst werden, dass andere Bewohner den Inhalt des Gesprächs nicht mithören können. Zusätzlich sollten Kopfhörer verwendet werden, damit Gesprächsinhalte nicht abgehört werden können.

- Für die Internetverbindung kann der normale Router im Heimnetzwerk verwendet werden. Wenn andere Parteien (z. B. Mitbewohner) ebenfalls diesen Router nutzen, sollte eine VPN-Verbindung genutzt werden, um auf Unternehmensdaten zuzugreifen.

- Anstelle des Routers im Netzwerk kann auch ein Hotspot vom dienstlichen Handy verwendet werden, um eine Verbindung ins Internet zu ermöglichen. Die Verbindung zum persönlichen Hotspot muss immer mit einem ausreichend starken Passwort gesichert werden.

2. Technische Umsetzung

Die technische Umsetzung von Home-Office bietet viele Fallstricke und Möglichkeiten Sicherheitslücken zu schaffen. Im Folgenden werden einige Tipps beschrieben, wie die technischen Aspekte für die Heimarbeit umgesetzt werden können.

2.1 Umgang mit Daten

Daten sollten nicht lokal auf den Geräten gespeichert werden, um ein unbefugtes Auslesen zu erschweren. Ist eine lokale Speicherung notwendig, sollte dies in einem verschlüsselten Teil der Festplatte geschehen. Private Geräte sollten nicht dienstlich verwendet werden. Ist die Nutzung privater Geräte unumgänglich, sollten alle dienstlichen Dateien von privaten Dateien getrennt werden (z. B. durch die Verwendung eines eigenen Benutzerkontos für dienstliche Zwecke). Idealerweise speichern Sie Ihre Daten nur in sog. Netzlaufwerken, da diese durch Ihre IT-Abteilung gesichert werden. Bei ausschließlich lokal gespeicherten Daten müssen die Benutzer die Sicherung übernehmen. In diesem Fall sollten sie auf einer verschlüsselten externen Festplatte gesichert werden.

2.2 Einrichten von Remote-Verbindungen

Wenn für die Heimarbeit Daten benötigt werden, die auf internen Servern gespeichert sind, muss ein Fernzugang für Benutzer eingerichtet werden. Es empfiehlt sich die Einrichtung einer VPN-Verbindung, um zu verhindern, dass Daten auf dem Übertragungsweg mitgelesen werden. Dies ist besonders wichtig, wenn der private Router im Heimnetzwerk auch von anderen Parteien genutzt wird. Welche Art der VPN-Einrichtung und Konfiguration für Sie die beste ist, hängt von der Struktur Ihres Unternehmens ab. Möglicherweise müssen Sie zur Einrichtung mit einem Dienstleister (z. B. einem Rechenzentrum) zusammenarbeiten oder zusätzliche Produkte erwerben.

Wenn die Remote-Verbindungen auch nach Ende der Corona-Krise Teil des Unternehmens bleiben sollen, ist ein zweiter Faktor zur Authentifizierung sinnvoll, um die Sicherheit weiter zu erhöhen. Üblicherweise werden dafür Hardware-Tokens an die Mitarbeiter ausgegeben, die ein Einmal-Passwort für die Anmeldung generieren.

2.3 Patch-Management

Im Home-Office können die Sicherheitsupdates auf den Endgeräten oft nicht automatisch aufgespielt werden. Ist die Nutzung privater Geräte gestattet (z. B. eigene Laptops und Heimrouter), müssen auch diese beachtet werden. In beiden Fällen müssen Mitarbeiter angewiesen werden, Sicherheitsupdates aufzuspielen, sobald diese verfügbar sind. Sollten Mitarbeiter nicht eigenständig dazu in der Lage sein, müssen sie entweder eine Schulung oder eine Schritt-für-Schritt-Anleitung bekommen. Bei nur wenigen Angestellten kann es ausreichend sein, die Updates per Fernwartung durchzuführen.

2.4 Fernwartung

Bei Problemen mit IT-Systemen im Home-Office muss von der IT-Abteilung oftmals eine Fernwartung durchgeführt werden. Im kommerziellen Umfeld darf die weit verbreitete Software „Teamviewer“ nur in der kostenpflichtigen Variante genutzt werden. In Microsoft Umgebungen kann die vorhandene Remotedesktopverbindung verwendet werden. Falls Microsoft Teams oder Cisco WebEx genutzt werden, kann auch damit eine Fernwartung durchgeführt werden. Der Vorteil dabei ist, dass Microsoft Teams und WebEx auch auf Mac OS und Linux eine Fernwartung ermöglichen.

Wer keine Software für die Fernwartung im Einsatz hat und keine Lizenz erwerben will, kann auf ein OpenSource Tool (z. B. ThinVNC) zurückgreifen. Prüfen Sie dabei im Vorfeld immer die Datenschutzerklärung der jeweiligen Hersteller.

3. Förderprogramm „go-digital“

Bei der technischen und organisatorischen Umsetzung von Home-Office ist es oftmals vorteilhaft, mit externen Fachleuten zur Unterstützung bei der Einrichtung zusammen zu arbeiten. Das Bundesamt für Wirtschaft und Energie (BMWi) fördert mit dem Programm „go-digital“ die Beratung bei der Digitalisierung von kleinen und mittleren Unternehmen (KMU). Insbesondere in Zeiten der Corona-Krise gibt es innerhalb dieses Programms die Möglichkeit, eine Förderung zur Einrichtung von Home-Office (z. B. das Einrichten einer VPN-Verbindung) im Eilverfahren zu beantragen. Für die Beantragung der Förderung können Sie sich direkt an eines der dazu autorisierten Unternehmen wenden. Geeignete Unternehmen in Ihrer Nähe finden Sie auf der folgenden Seite:

https://www.innovation-beratung-foerderung.de/INNO/Navigation/DE/Karten/Beratersuche-go-digital/SiteGlobals/Forms/Formulare/beratersuche-go-digital-formular.html

Auch wenn theoretisch jedes Unternehmen für die Einrichtung von Home-Office in Frage kommt, sollten Sie sich dabei auf die Unternehmen innerhalb des Moduls „IT-Sicherheit“ konzentrieren.

Folgende Voraussetzungen muss Ihr Unternehmen erfüllen, um für die Förderung in Frage zu kommen:

- Unternehmenssitz in Deutschland
- Weniger als 100 Mitarbeiter
- Einkommen von weniger als 20 Mio € im vergangenen Jahr
- Förderfähig nach der de-minimis Regelung (weniger als 300.000€ Fördergelder innerhalb der letzten drei Jahre erhalten)