

Tipps für sicheres Arbeiten im Homeoffice

Immer mehr Angestellte sollen oder müssen aus aktuellem Anlass im Homeoffice arbeiten. Nachfolgend erhalten Sie einige Tipps, auf welche Aspekte hinsichtlich IT-Sicherheit geachtet werden sollte.

Hinweis:

Über das Fördermittelprogramm "go-digital" kann auch die Einrichtung von Homeoffice-Plätzen unterstützt werden. Zudem ist nun ein vorzeitiger Maßnahmenbeginn vor Erhalt des Zuwendungsbescheids in diesem Zusammenhang möglich. [Zum Programm](#)

10 Regeln für IT-Sicherheit im Homeoffice

Das Mittelstand 4.0 Kompetenzzentrum Chemnitz hat 10 goldene Regeln für mehr IT-Sicherheit im Homeoffice zusammengestellt. Hierzu zählen:

1. Definieren Sie den Einsatz von Homeoffice
2. Leiten Sie Regelungen für Ihr Unternehmen ab
3. Schaffen Sie die technischen Voraussetzungen
4. Holen Sie sich Unterstützung
5. Zugriffs- und Zugangsschutz
6. Verschlüsselte Kommunikation und Remote-Zugriff
7. Datensicherung
8. Umgang mit Unterlagen und vertraulichen Informationen
9. Haben Sie Vertrauen gegenüber Ihren Mitarbeitenden
10. Laufende Sensibilisierung für Gefahren

Die Details zu den Regeln, Hinweise zur Authentifizierung von Mitarbeitenden sowie zahlreiche weitere Leitfäden sind unter www.betrieb-machen.de/nachgelesen_it-sicherheit-im-homeoffice zu finden.

Tipps für sicheres mobiles Arbeiten hat zudem der BSI zusammengestellt (siehe Link).

Checkliste

In dieser Online-Checkliste der Allianz für Cybersicherheit sind kurzfristig realisierbare Maßnahmen für ein sicheres Arbeiten im Homeoffice zusammengestellt. Mit den darin gestellten Fragen können zudem bereits getroffene Vorkehrungen geprüft werden. Hinweise helfen bei der Umsetzung.

[zur Checkliste](#)

Allgemeingültige Sicherheitshinweise

- Das mitgebrachte Gerät vom Unternehmen oder den privaten Computer nie unbeaufsichtigt lassen.
- Keine weiteren Personen während der Homeoffice-Zeit am Gerät arbeiten lassen, um die Vertraulichkeit der Daten zu gewährleisten.
- Rechner sperren oder herunterfahren, sobald der Arbeitsplatz verlassen wird
Die Tastenkombination Windows+L sperrt Ihren Rechner schnell.

Bei privaten Computern zudem darauf achten, dass:

- das Betriebssystem aktuell ist (z.B. Windows-Updates automatisch installieren lassen)
- vor der Arbeit eine routinemäßige Kontrolle auf anstehende Updates erfolgt und
- eine Sicherheitssoftware (Antivirus, Firewall) installiert und diese aktuell ist (Updates).

Vorsicht auch im HomeOffice beim Einsatz von externen Datenträgern:

Vor der Nutzung prüfen, woher diese kommen bzw. wo/bei wem diese bisher im Einsatz waren.

Empfehlung: Möglichkeiten des Datenaustauschs online über sichere und datenschutzkonforme Anbieter nutzen.

Tipps für sicheres WLAN:

- Konfiguration (bzw. Kontrolle) des Routers, bevor dieser in Betrieb genommen wird (insbesondere bei WLAN-Nutzung). Wie die Konfiguration gelingt, kann in der Betriebsanleitung des Gerätes nachgelesen werden.
- Abschalten der Möglichkeit, den Router über eine WLAN-Verbindung zu konfigurieren - die Konfiguration sollte nach Möglichkeit nur über eine kabelgebundene Verbindung erfolgen.
- Konfiguration der Verschlüsselung mit Auswahl des sogenannten WPA2-Standards (wird in der Regel von

allen modernen Geräten, auch Tablets und Smartphones, unterstützt).

- Deaktivierung der Möglichkeit der Wartung via Fernzugriff in den Einstellungen des Routers (falls vorhanden).
- Schnellstmögliche Änderung des Administrations-Passworts des Routers (siehe Betriebsanleitung des Gerätes).
- Auswahl eines sicheren Passwort. Sichere Passwörter bestehen gerade für den WLAN-Zugang aus einer möglichst langen zufälligen Zeichenkette (32 Zeichen und mehr), gemischt aus Groß- und Kleinschreibung, Ziffern und Sonderzeichen.
- Firmware des Routers immer auf dem aktuellen Stand halten (nach Möglichkeit mit automatischen Updates).
- WLAN ausschalten, wenn es nicht gebraucht wird. Einige Router bieten die Möglichkeit, entsprechende Zeiträume zu definieren, in denen das WLAN automatisch an- beziehungsweise ausgeschaltet wird.

Generelle Empfehlung:

Ausschalten, was nicht gebraucht wird und Aktivierung der Funktionen nach Bedarf - also temporär.