Mobiles Arbeiten ist für viele Routine. Niemand sollte allzu routiniert damit umgehen, denn die Sicherheitsrisiken und die möglichen Konsequenzen daraus können erheblich sein

Bevor ein mobiler Arbeitsplatz eingerichtet werden kann, muss entschieden werden, ob die Tätigkeit und die vorgesehene Arbeitsumgebung für mobiles Arbeiten geeignet sind. Dies ist nicht der Fall, wenn

→ die zu bearbeitenden Daten vertraulich sind und somit nicht außerhalb der geschützten Büroumgebung bearbeitet werden dürfen.

→ die Umgebung es nicht erlaubt, ohne Einsichtnahme Dritter zu arbeiten, zum Beispiel in einem Großraumwagen der Bahn.

Bei mobiler Arbeit sind folgende Risiken zu betrachten:

- **Dritte können mitlesen:** Beim Arbeiten außerhalb des Büros besteht die Gefahr der Kenntnisnahme durch Unbefugte.
- **Verlust oder Diebstahl von Hardware:** Es steigt das Risiko, dass das Endgerät und damit Daten verloren gehen oder gestohlen werden.
- **Unbefugte im Behördennetz:** Wenn Zugangsdaten ausgespäht werden, besteht die Gefahr, dass Unberechtigte Zugang zum internen Behördennetz bekommen.
- **Angriffe auf das mobile Endgerät:** Auch diese Gefahr wird größer, wenn Sie in unsicheren Arbeitsumgebungen mobil arbeiten.
- **Nicht aktualisierter Virenschutz:** Ohne aktuellen Stand der Virenschutzsoftware und ohne aktuelle Sicherheitsupdates droht Schadsoftware-Befall.

www.thueringen.de

digitale Services
verwaltung.thueringen.de

Herausgeber:
Thüringer Finanzministerium
Informationssicherheitsbeauftragter des Freistaats
Ludwig Erhard-Ring 7
99099 Erfurt

Bilder:
Rogge GmbH, Bildmontagen unter Verwendung von Motiven aus AdobeStock, ©Federico Rostagno (Titel), ©Idprod (innen oben), ©Jacob Lund (innen unten)
Text und Layout:
Rogge GmbH, Weimar

Freistaat Thüringen

Mobiles Arbeiten

Worauf Sie achten müssen, wenn Sie unterwegs arbeiten

Informationssicherheit

Mitarbeiter, die mobil arbeiten, sind in besonderer Weise für die Sicherheit der ihnen anvertrauten Daten verantwortlich. Sie sind verpflichtet, die verwendeten Geräte und Daten sicher zu verwahren und Dritten keinen Zugriff auf diese Geräte zu ermöglichen.

Arbeiten Sie nur in sicheren Umgebungen

Tun Sie es nicht an unsicheren Orten wie Restaurants, Flugzeugen oder öffentlichen Plätzen.

Die vereinbarten Sicherheitsvorgaben strikt einhalten

Als Mitarbeiter sind Sie eigenverantwortlich zur Umsetzung der hohen Sicherheitsanforderungen für mobiles Arbeiten verpflichtet.

Unberechtigte Dritte von dienstlichen Daten fernhalten

Dies gilt nicht nur in Bahn, Flugzeug oder auf öffentlichen Plätzen, sondern auch im sogenannten sicheren häuslichen Bereich. Ihre Familienmitglieder zählen zu den unberechtigten Dritten, die keine Kenntnis von sensiblen Daten erlangen dürfen.

Ausschließlich dienstlich vorgegebene Speicherorte nutzen

Speichern Sie dienstlichen Daten nie auf privaten Datenträgern.

Verboten: Kein Datenaustausch mit privaten Postfächern oder Clouds!

Für den dienstlichen Datenaustausch dürfen Sie ausschließlich die dienstlich vorgesehenen Online-Speicher-Lösungen nutzen. Das Weiterleiten von dienstlichen Mails an private Mailadressen ist verboten.

Keine automatisierte Speicherung von Anmeldedaten auf Dienst-Geräten

Um Missbrauch bei Verlust mobiler Geräte vorzubeugen, sind die Anmeldedaten bei jedem Start neu einzugeben. Die Administratoren der Dienststelle müssen dies bei Erstinstallation der mobilen Geräte so einstellen.

Mobiles IT-Gerät vor Verlust und Diebstahl sichern

Wie im normalen Bürobetrieb sind beim mobilen Arbeiten die Geräte beim Verlassen des Arbeitsortes zu sperren. Wenn sie nicht verwendet werden, müssen sie sicher und verschlossen aufbewahrt werden.

Dasselbe gilt für Datenträger

Sichern Sie auch alle weiteren mitgeführten Speichermedien sowie Unterlagen in Papier vor Verlust und Diebstahl.

Im Ernstfall sofort Alarm schlagen

Bei Diebstahl oder Verlust von IT-Geräten oder dienstlichen Datenspeichern müssen unverzüglich der zuständige IT-Sicherheitsbeauftragte und der Vorgesetzte informiert werden. Das gilt auch bei möglichen Kompromittierungen von Zugangsdaten und beim Verlust von Papierakten.
Bei Diebstahl ist Anzeige bei der Polizei zu erstatten.

Kampagne SECURITY AWARENESS
Eine Handreichung des
Thüringer Finanzministeriums
für die Arbeit mit digitalen Medien

Ansprechpartner/
IT-Sicherheitsbeauftragte(r):

Name:	
Dienststelle:	
Telefon:	
E-Mail:	