In der dienstlichen Kommunikation spielen Telefon- und Videokonferenzen eine immer größere Rolle. Es geht schnell, es ist live – und teilweise gefährlich neu.

Heute wird viel mit dem Telefon gearbeitet, am Schreibtisch, mobil oder in der Telefonkonferenz. Die Bediensteten müssen dabei routiniert unterschiedliche Vorsichtsmaßnahmen beachten, weil keine Form der Telefonie wirklich sicher ist.

Eine besondere Rolle spielt seit kürzerer Zeit die Videokonferenz. Ihre Vorzüge machen sie für interessierte Dritte und Cyber-Angriffe besonders attraktiv: Anders als am Telefon werden auf der Videokonferenz Informationen live in Ton und Bild übertragen.

Die Bediensteten müssen deshalb neue Sicherheitsrisiken berücksichtigen und neue Regeln kennenlernen und beachten.

Risiken beim Telefonieren und auf der Videokonferenz

Bei der Telefonie besteht die Gefahr, dass Unbefugte mithören und Dateien stehlen, Angreifer Schadprogramme ins Behördennetz einschleusen oder dass das Endgerät beschädigt, verloren oder gestohlen wird. Bei Videokonferenzen kann Verwaltungshandeln in Echtzeit ausspioniert werden, das übertragene Bildmaterial kann zusätzlich sensible Informationen verraten. Die Neuartigkeit der Videokonferenztechnik und die Vielzahl ihrer Funktionen führen leicht zu Fehlern beim Nutzer.

Drohende Folgen:

- Verlust und Weitergabe sensibler Informationen an Dritte
- Ausfall der digitalen Infrastruktur
- Ansehensverlust der Landesverwaltung
- Großer finanzieller Schaden

www.thueringen.de

digitale Services
verwaltung.thueringen.de

SICHER ZUSAMMENARBEITEN · SICHER MITWIRKEN

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

Bilder:
Rogge GmbH, Bildmontagen unter Verwendung von Motiven aus AdobeStock, ©taniasv (Titel), © LIGHTFIELD STUDIOS (innen unten), ©ty (innen oben)
Text und Layout:
Rogge GmbH, Weimar

Freistaat Thüringen

Verwaltungshandeln live in Bild und Ton

Sicher telefonieren und Videokonferenzen durchführen

Informationssicherheit

Hinweise für sicheres Telefonieren im Dienst:

Vertrauliche Gespräche nur in gesicherter Umgebung
Achten Sie darauf zum Beispiel bei Telefonaten in Büros mit mehreren Arbeitsplätzen oder im öffentlichen Raum.

Telefonkonferenzen abschirmen
Stellen Sie sicher, dass keine unberechtigten Dritten mithören können. Telefonkonferenzen dürfen nur in sicheren Arbeitsumgebungen abgehalten werden. Dazu zählen unter Umständen das eigene Büro, gesonderte Besprechungsräume oder – im mobilen Einsatz – ein ungestörtes Umfeld ohne Mithörende.

Nichts Vertrauliches an Externe weitergeben
Grundsätzlich sollten Sie keine schützenswerten Informationen am Telefon oder Handy mitteilen, besonders nicht Dritten gegenüber. Vergewissern Sie sich, dass Ihr Gesprächspartner berechtigt ist, die Informationen zu erhalten, stellen Sie gegebenenfalls Kontrollfragen.

Vorsicht vor Social-Engineering-Angriffen
Auch beim Telefonieren besteht die Gefahr, Opfer von Social-Engineering-Attacken zu werden. Unterlassen Sie deshalb, Angaben zu machen über Passwörter, Zugangsdaten, sensible Daten aus dem Behördenumfeld, Organisationsstrukturen, Mailadressen oder Bedienstete.

Regelmäßig Sicherheitsupdates aktualisieren
Halten Sie die Sicherheitsprogramme Ihres dienstlich genutzten Mobiltelefons immer auf dem neuesten Stand.

Verlust und Diebstahl von Endgeräten unverzüglich melden
Wenden Sie sich sofort an den Vorgesetzten und den zuständigen Administrator.

Woran Sie bei Videokonferenzen denken sollten:

Gesonderte Konferenzsysteme verwenden
Nutzen Sie für eine Videokonferenz möglichst ein vom Dienstherrn zur Verfügung gestelltes System.

Separates Zimmer bereitstellen
Sie verhindern damit, dass Informationen aus Gesprächen oder Telefonaten aus dem Hintergrund auf der Videokonferenz zu hören sind.

Auf den Bildhintergrund achten
Stellen Sie auch sicher, dass im übertragenen Bild des Konferenzraums keine Informationen zu sehen sind. Entfernen Sie Whiteboards, Bildschirme, Flipcharts u. Ä. Verwenden Sie gegebenenfalls ein virtuelles Hintergrundbild.

Immer die Kontrolle behalten
Informieren Sie sich über die Bedienung des Systems. Deaktivieren Sie die Optionen, die eine Möglichkeit bieten, die Kontrolle über das System vorübergehend aus der Ferne zu übernehmen.

Keine Verschlusssachen!
In einer Video- bzw. Telefonkonferenz oder in einer Screensharing-Sitzung dürfen auf keinen Fall VS- oder VS-NfD-Dokumente oder -Themen besprochen oder geteilt werden.

Videokonferenzen durch sichere Kennworte schützen
Das Passwort dürfen ausschließlich die vorgesehenen Teilnehmer erhalten.

Teilnehmer überprüfen
Vergewissern Sie sich, wer sich tatsächlich in die Konferenz eingewählt hat oder an der Konferenz teilnimmt. Sind Ihnen alle Teilnehmer bekannt und angemeldet?

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

Ansprechpartner/
IT-Sicherheitsbeauftragte(r):

Name:

Dienststelle:

Telefon:

E-Mail: