CSBW
CYBER
SICHERHEITS
AGENTUR
BADEN-WÜRTTEMBERG

Videokonferenzen

Durch die Arbeit im Homeoffice oder um Reisen zu vermeiden, sind Videokonferenzen inzwischen fester Bestandteil des Arbeitsalltags. Aber auch im privaten Umfeld sind Videotelefonate und Videokonferenzen, z.B. über Messenger, weit verbreitet.
Videokonferenzen bieten viele Vorteile, können jedoch auch Gefahren hinsichtlich der Sicherheit der persönlichen Daten bergen.

Tipps für den sicheren Umgang mit Videokonferenz-Tools

Empfehlungen für die Auswahl eines Videokonferenzsystems:

Bereits die Auswahl des Videokonferenzsystems ist maßgeblich für die Sicherheit Ihrer Daten. Empfehlenswert ist die Nutzung einer europäischen Software, damit gemäß den Anforderungen der europäischen Datenschutz-Grundverordnung (DSGVO) keine Übermittlung von persönlichen Daten an ein Drittland oder an eine andere Einrichtung stattfindet.[1]

Darüber hinaus empfiehlt sich die Nutzung eines Systems, das die Kommunikation Ende-zu-Ende verschlüsselt.[2] Hierdurch minimiert sich die Gefahr, dass Cyberkriminelle Daten abgreifen können.

Tipps vor Beginn einer Videokonferenz:[3]

- Schützen Sie den Zugangslink zur Videokonferenz mit einem sicheren Passwort.
- Nutzen Sie für jede Konferenz ein neues Passwort. Teilen Sie die Zugangsdaten und das Passwort nur über vertrauenswürdige Quellen mit dem eingeladenen Personenkreis, z.B. per E-Mail.
- Richten Sie einen Warteraum vor der Konferenz ein, um die Identität der Teilnehmenden überprüfen zu können.
- Deaktivieren Sie die Aufzeichnungsfunktion für die Teilnehmenden.

Videokonferenzen

Empfehlungen für eine sichere Videokonferenz:

Hintergrund

- Achten Sie darauf, was im Hintergrund zu sehen ist und entfernen Sie ggf. private oder unpassende Bilder sowie Gegenstände.
- Vermeiden Sie andere Personen im Hintergrund.
- Nutzen Sie einen Weichzeichnungsfilter oder einen virtuellen Hintergrund, wenn möglich.

Sprachassistenzsysteme

- Es besteht die Gefahr, dass Sprachassistenzsysteme sensible Informationen mithören und an unbefugte Dritte weiterleiten.
- Schalten Sie Sprachassistenzsysteme daher während Videokonferenzen aus und entfernen Sie diese aus dem Raum.

Anonyme Videokonferenzteilnehmende

- Stellen Sie sicher, dass keine unbefugten Personen in der Konferenz sind. Bitten Sie anonyme oder per Telefon zugeschaltete und Ihnen unbekannte Personen sich vorzustellen.

Screensharing = Teilen von Inhalten

- Teilen Sie nur Informationen, die für alle Teilnehmenden bestimmt sind.
- Programme und Tabs mit sensiblen Informationen vor dem Screensharing schließen und während des Sharings nicht für alle sichtbar anzeigen lassen.
- Geben Sie, wenn möglich nur einzelne Programme frei.
- Zur Eingabe von Passwörtern das Screensharing kurz unterbrechen, auch wenn ein (Offline-)Passwortmanager genutzt wird.

Quellen:

[1] https://dejure.org/gesetze/DSGVO
[2] https://www.baden-wuerttemberg.datenschutz.de/videokonferenzsysteme/#videokonferenz_als_online_dienst_rahmenbedingungen_und_empfehlungen
[3] BSI - Sicher per Videokonferenz unterrichten (bund.de)

CSBW
CYBER SICHERHEITS AGENTUR
BADEN-WÜRTTEMBERG

Weitere Factsheets und Informationen unter:
www.cybersicherheit-bw.de

CSBW Prävention
Kontakt: schulungen@cybersicherheit.bwl.de
Stand: 11.2023