eGovernment COMPUTING

Sicher kommunizieren

Videokonferenzen sicher gestalten

08.03.2021 | Autor / Redakteur: Michael Sudahl / Susanne Ehneß

Der Deutsche Beamtenbund hat unlängst herausgefunden, dass auf Bundesebene 67 Prozent der Beschäftigten dauerhaft ins Homeoffice wechseln können. Auf Landesebene sind es noch mehr als die Hälfte (55 Prozent). Abgeschlagen hingegen sind Beamte und Mitarbeiter auf kommunaler Ebene. Von ihnen können nur 37 Prozent zuhause arbeiten, darunter fallen etwa Erzieherinnen oder Bauhofmitarbeiter.

<https://cdn1.vogel.de/unsafe/fit-in/1000x0/images.vogel.de/vogelonline/bdb/1805300/1805387/original.jpg>
In Deutschland gehostete Konferenzsysteme sind gefragt
(© Andrey Popov - stock.adobe.com)

Teil des Wandels ist die Nutzung von Videokonferenzen, von denen es drei Arten gibt:

- Theoretisch möglich, aber selten in der Realität anzutreffen: Kommunen und Ämter betreiben einen eigenen Dienst.
- Weiter verbreitet ist der Betrieb durch einen externen IT-Dienstleister.
- Hinzu kommt als Variante die Nutzung eines Online-Dienstes.

Bei allen ist eine DSGVO <https://egovernment-computing.de/was-ist-die-

datenschutzgrundverordnung-dsgvo-a-712294/> -konforme Nutzung möglich, wenn die Server in Deutschland stehen und nach europäischem Recht gehostet sind. Wer Daten in der Cloud, etwa bei Google, speichert, hat eine Lücke, die mit einer Bußgeldgefahr einhergeht, wie Stefan Brink es benennt. Er ist Datenschutzbeauftragter des Landes Baden-Württemberg.

Hintergrund: Gerade die größten und bekanntesten Serviceanbieter wie Google oder Microsoft sitzen in den USA und verarbeiten dort die Daten. Nach der Entscheidung des Europäischen Gerichtshofs im vergangenen Sommer und dem Wegfall des EU-US-Privacy-Shields kann das problematisch sein.

<https://cdn1.vogel.de/unsafe/fit-in/1000x0/images.vogel.de/vogelonline/bdb/1805300/1805357/original.jpg>
Felix Pflüger
(© Peoplefone)

Felix Pflüger vom Telefonnetz-Betreiber Peoplefone Deutschland berichtet, dass bei ihm vermehrt Anfragen zu Anschlüssen für in Deutschland gehostete Konferenzsysteme eingehen. Genutzt werden Anbieter wie „Big Blue Button", eine Open-Source-Web-Konferenz-Lösung, und „Jitsi Meet", eine Software, die auf eigenen Servern betrieben werden kann. Beide Varianten haben einen hohen administrativen Aufwand, den entweder die Behörde oder externer Dienstleister übernehmen. Dafür sind die Softwares kostenlos, es fallen lediglich Hosting- und Service-Kosten an. Auch hier kommt es darauf an, wo der Server steht und wer Zugriff auf die Daten hat. „Wird er in der EU betrieben und werden keine Daten mit der USA ausgetauscht, ist der Betrieb DSGVO-konform", meint Pflüger.

Ratsam ist es bei der Auswahl eines webbasierten Videokonferenztools, den zwingend notwendigen Auftragsverarbeitungsvertrag zu prüfen. Wichtig ist hier zu schauen, ob die eingesetzte Software Daten an Hersteller oder Dritte weitergibt. Zu empfehlen sind Lösungen, welche die Kommunikation verschlüsselt und als Oberfläche WebRTC nutzt –

also direkt im Browser aufgerufen werden.

Zusätzlich sollten Dokumente direkt zwischen Videoteilnehmern austauschbar sein – ohne Zwischenspeicherung auf einem externen Server. Dies ist besonders wichtig für Ämter und Notare. Unter anderen erfüllt die Software „peoplefone-Meet“ diese Ansprüche

Zu beachten ist auch: Wer Videokonferenz-Tools nutzt, um mit Kunden und Mitarbeitern zu kommunizieren, muss diese Programme in seine Datenschutzerklärung aufnehmen. Dabei sollte sichergestellt sein, dass die Datenübertragung per SSL/TLS verschlüsselt ist.

Bevor es dann mit Videokonferenzen los geht, vergibt der Einladende Sitzungsnummern, idealerweise variieren diese. Sie sollten aus mindestens acht Zeichen bestehen. Ein Passwort sorgt für zusätzliche Sicherheit, am besten über einen zweiten Kanal wie SMS übermittelt. Wer zudem Teilnehmer nicht persönlich kennt, sollte sich deren Personalausweis zeigen lassen oder Merkmale abfragen.

Während einer Sitzung lauern weitere Tücken: Um vor Mithörern zu schützen, sollten die Teilnehmer Headset tragen und auf ihr Umfeld achten. Experte Pflüger: „Den Flipchart im Hintergrund bitte wegstellen und vertrauliche Informationen besser via Chat übermitteln, statt mündlich.“

Zu empfehlen ist überdies, nie den ganzen Bildschirm zu zeigen. Stattdessen nur einzelne Applikationsfenster. Eine Filterfunktion wie eine Blacklist hilft, gewisse Fenster – wie eMail oder Messenger-Dienste – auszuschließen.

Klug ist es zudem, Rollen zu trennen. Ein Administrator legt Parameter fest und weist Moderationsrollen zu. Ein Moderator kann Videokonferenzen anberaumen, Personen einladen und ausschließen. Zudem öffnet und schließt er die Präsentationsrolle. Diese wiederum kann Medien und Dokumente für andere Teilnehmer bereitstellen und eine Diskussion steuern. Letztlich die Teilnehmer: Sie dürfen eigene Aufzeichnungs- und Wiedergabegeräte steuern. Wichtig ist auch, dass jeder Kamera und Mikrofon jederzeit deaktivieren kann.

(ID:47262753)