ZfK Zeitung für kommunale Wirtschaft

IT

ZfK+ Videoformate mit und ohne Nebenwirkungen

Kommunikation via Video ist in der Verwaltung angekommen. Doch wer externe Software nutzt, spielt mit dem Datenschutz.

13.06.2023

Bei Videokonferenzen gibt es einige Punkte, die man auch im Rahmen von Datenschutz beachten sollte.

Bild: © rh2010/AdobeStock

Bild: © privat

Von:
Michael Sudahl,
Journalist

Sogar Erzieherinnen im städtischen Kindergarten und Pflegedienstleiter kommunaler Krankenhäuser verbringen einen Teil ihrer Arbeitszeit in Videokonferenzen. Auf Landesebene nutzen solche Werkzeuge mehr als die Hälfte der Beschäftigten. Spitzenreiter sind Beamte und Mitarbeiter des Bundes. Zwei Drittel der hier arbeitenden können dauerhaft an den heimischen Schreibtisch wechseln und dort via Video konferieren. Das hat der Deutsche Beamtenbund unlängst ermittelt.

Vereinbarung fehlt

Etliche Behörden holen sich für Bildschirmmeetings externe IT-Firmen ins Haus oder nutzen Online-Dienste. Bei beiden ist eine DSGVO-konforme Nutzung nur möglich, wenn die Server in Deutschland stehen und nach europäischem Recht gehostet sind. Wer Daten hingegen in der Cloud speichert, etwa bei Google oder Amazon, hat eine Lücke, die ein Bußgeldrisiko in sich birgt, wie Stefan Brink weiß.

Der Datenschutzbeauftragter des Landes Baden-Württemberg erklärt, dass Anbieter wie Microsoft in den USA sitzen und dort die Daten verarbeiten. Nach der Entscheidung des Europäischen Gerichtshofs im vergangenen Sommer und dem Wegfall des EU-US-Privacy-Shields kann das problematisch sein und teuer werden.

In Deutschland gehostet

Felix Pflüger vom Telefonnetz-Betreiber Peoplefone Deutschland berichtet, dass bei ihm vermehrt Anfragen von Ämtern 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 Service-Abgaben 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.

Webbasierte Software

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

Zusätzlich sollten Dokumente zwischen Videoteilnehmern austauschbar sein – ohne Speicherung auf einem externen Server. Dies ist besonders wichtig für Behörden und kommunale Betriebe. Unter anderen erfüllt die Software peoplefone-Meet diese Ansprüche. Zu beachten ist auch: Wer Videokonferenzsysteme nutzt, um mit Bürgern und Mitarbeitern zu kommunizieren, muss diese Programme in seine Datenschutzerklärung aufnehmen. Dabei sollte sichergestellt sein, dass die Datenübertragung per SSL/TLS verschlüsselt ist.

Tipps für die Konferenz

„Bevor es dann mit Videokonferenzen los geht, vergibt der Einladende Sitzungsnummern, idealerweise variieren diese“, sagt IT-Mann Pflüger. 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 E-Mail 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. (sg)

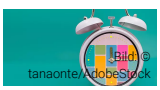
Mehr zum Thema

IT

Auf welche Tools Versorger bei der internen Zusammenarbeit setzen

IT

Cyberkriminalität: KI-Systeme wie ChatGPT fungieren als Booster



IT

Schneller Einstieg ins Organisationsmanagement