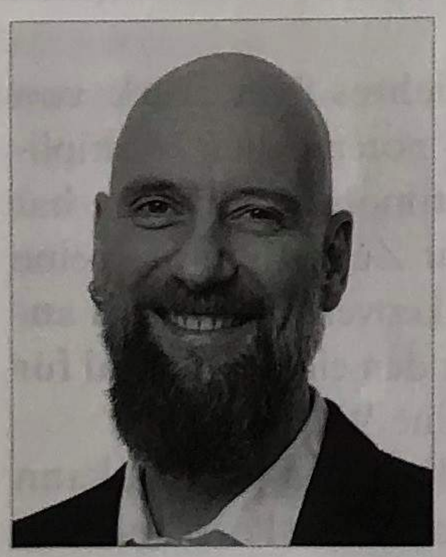
HOMEOFFICE

Videokonferenztools datensicher einsetzen

VON THOMAS ALTHAMMER UND ARNE WOLFF

Thomas Althammer leitet das Unternehmen Althammer & Kill GmbH & Co. KG in Düsseldorf, das seinen Schwerpunkt im Gesundheits- und Sozialwesen hat. Er ist zudem bei Einrichtungen bundesweit als externer Datenschutzbeauftragte tätig.
www.althammer-kill.de



Arne Wolff ist Berater für Datenschutz und IT-Sicherheit Althammer & Kill GmbH & Co. KG.
www.althammer-kill.de

Die IT-Sicherheit und den Datenschutz stellt das Arbeiten an Heimarbeitsplätzen vor große Herausforderungen. Das betrifft nicht nur die Bereitstellung und den Austausch von Informationen, sondern auch die Nutzung von Videokonferenzsystemen.

Die Corona-Pandemie hat die Arbeitswelt verändert, auch in der Sozial- und Gesundheitsbranche. Wurde vor dem ersten Lockdown in den wenigsten Organisationen »remote« gearbeitet, musste digitales und kollaboratives Arbeiten plötzlich schnell umgesetzt werden, um weiter handlungsfähig zu bleiben. Einer Umfrage des Digitalverbandes bitkom zufolge arbeitet inzwischen fast jeder vierte Erwerbstätige im Homeoffice, auf fast 20 weitere Prozent trifft dies zumindest teilweise zu. Viele Beschäftigte wünschen sich auch in Zukunft zumindest teilweises Arbeiten im Homeoffice.

Videokonferenzen erlauben ein hohes Maß an Flexibilität, effiziente Teamarbeit auch im Lockdown sowie das Einsparen von Ressourcen. Belasten Videokonferenzen die Umwelt doch weit weniger, beispielsweise im Hinblick auf Geschäftsreisen und CO2-Ausstoß. Hinsichtlich IT-Sicherheit und Datenschutz gilt es allerdings einiges zu bedenken.

Bei einigen Videokonferenzsystemen – die zum Teil auch gratis genutzt werden können – fließen Daten ab, es gibt keine Verschlüsselung der Informationen und es können sogar personenbezogene Daten gespeichert werden. Das Spektrum der Angebote ist breit. Es reicht von einfacher »Video-Telefonie« mit einer begrenzten Anzahl von Teilnehmer*innen wie etwa Microsoft Skype oder Google Duo bis hin zu dem aktuell in die Kritik geratenen, aber mit sehr umfangreichen Leistungsmerkmalen ausgestatteten Zoom oder teilweise tief integrierten und verflochtenen Komponenten wie Microsoft Teams. Einige Systeme können auch On-Premise, also selbstgehostet, betrieben werden, was eine weitreichende Kontrolle über Konfiguration und Datenflüsse erlaubt, aber eine kompetente und mit ausreichend Ressourcen versehene IT voraussetzt. Gerade kleine Organisationen oder Verbänden können solche Ressourcen oft nicht vorhalten.

Was zu beachten ist

Welche Maßnahmen des Datenschutzes sind bei Videokonferenzsystemen zu berücksichtigen? Jede Organisation sollte sich im Vorfeld Gedanken über Videokonferenzsysteme machen und Voreinstellungen und Freigaberichtlinien so einstellen, dass möglichst wenige Daten gespeichert werden oder abfließen. Dies sind die wichtigsten Punkte zur Erhöhung des Datenschutzes:

- Das System sollte datenschutzfreundliche Voreinstellungen zulassen, wie eine Deaktivierung der Datenanalyse, Senden von Fehlermeldungen oder Erstellung automatischer Protokolle.
- Es sollten Freigaberichtlinien vorhanden sein, die etwaige Bildschirmübertragungen (»Screen-Sharing«) oder anderweitige Bildschirmmitschnitte (»Screen-Capping«) nur ermöglichen,

DOI: 10.5771/1613-0707-2021-4-36

wenn die Verwender*innen im Vorfeld zustimmen können und die Teilnehmenden über die Bildaufzeichnung informiert werden.

- Die Anwendung sollte Informationsmöglichkeiten bereitstellen, um betroffene Personen vor dem Beginn einer jeden Videokonferenz die notwendigen Datenschutz-Informationen im Sinne von Art. 12 ff. der Datenschutz-Grundverordnung (DSGVO) in eindeutiger und klarerweise bereitstellen zu können.
- Viele Videokonferenzsysteme führen Datenanalysen und Bewertungen von Teilnehmer*innen durch. Diese Funktion sollte ausgeschlossen oder abgeschaltet werden können. Gleichzeitig sollte unterbunden werden, dass das Videokonferenzsystem nicht zwingend benötigte Log-Files, beispielsweise zu Wartungszwecken, aufzeichnet. Das gilt auch für Datenerhebungen, welche für die Erbringung des Dienstes nicht zwingend erforderlich sind, wie beispielsweise Verhaltensanalysen der Benutzer.
- Etwaige Aufzeichnungen, Chatverläufe, Transkripte oder ausgetauschte Dateien sollten nach Kommunikationsende gelöscht werden können oder nur so lange gespeichert werden, wie es erforderlich ist. Dazu sollten entsprechende Vorgaben zu Löschfristen eingestellt werden können.
- Die Anwendung sollte die Möglichkeit bieten, die Privatsphäre der Anwender zu schützen, beispielsweise den Hintergrund der Videoteilnehmer*innen unkenntlich zu machen oder auszugrauen (»Weichzeichnungs-Funktion«).
- Ein Anbieter sollte Daten zwischen den einzelnen Teilnehmer*innen verschlüsselt übertragen können, bestenfalls durch eine aktuelle Ende-zu-Ende-Verschlüsselung. Für nicht-sensible Daten können gegebenenfalls bereits standardisierte Verschlüsselungstechniken ausreichend sein.
- Videokonferenzen dürfen nicht für alle zugänglich sein, sodass es einer Anmelde-Funktion bedarf, damit nur Berechtigte an der jeweiligen Videokonferenz teilnehmen können und hierdurch ansonsten mögliche Datenpannen verhindert werden.

Welche Videokonferenzsysteme empfehlenswert sind

Die Systeme schneiden im Hinblick auf DSGVO-Compliance mal besser, mal schlechter ab. Unsere Berater haben die gängigsten Videokonferenzsysteme in den letzten Monaten regelmäßig überprüft. (Alle Angaben sind dabei ohne Gewähr, da sich die Anbieter dynamisch auf die Bedürfnisse einstellen und sich Einschätzungen dadurch verändern können.) Wir haben insbesondere bewertet, ob das europäische Datenschutzniveau sichergestellt und ein Auftragsverarbeitungs-Vertrag nach Art. 28 DSGVO geschlossen werden kann:

- BigBlueButton von BigBlueButton Inc.
- ClickMeeting von ClickMeeting Spółka z ograniczoną odpowiedzialnością
- Teamviewer von TeamViewer Germany GmbH
- Tixeo von Tixeo SARL
- whereby von Video Communication Services AS

Beliebte Videokonferenzsysteme wie Zoom (als Cloud-Dienst), CiscoWebex, GotoMeeting oder FaceTime sind aus datenschutzrechtlicher Sicht risikobehafteter und weniger empfehlenswert.

Was die Anforderungen aus dem Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD) und dem Gesetz über den kirchlichen Datenschutz der Katholischen Kirche (KDG) angeht, so ist ihr Einsatz bei allen genannten fraglich (vgl. Kasten). Die Katholische Datenschutzaufsicht Ost ist allerdings unlängst von ihrem generellen Zoom-Verbot abgerückt und hält den Einsatz unter bestimmten Voraussetzungen für zulässig. (1)

Ein Sonderfall bei den Videokonferenzsysteme ist die »Videosprechstunde« bei Haus- und Fachärzten; hier verlangt die Kassenärztliche Bundesvereinigung vom Anbieter eine Zertifizierung nach Anlage 31b zum Bundesmantelvertrag-Ärzte (BMV-Ä), die sowohl Aspekte der Datensicherheit als auch des Datenschutzes berücksichtigt.

Wann eine Datenschutz-Folgenabschätzung erforderlich ist

Eine Datenschutz-Folgenabschätzung ist immer dann durchzuführen, wenn ein hohes Risiko für die Rechte der betroffenen Nutzer*innen besteht. Dies ist im Hinblick auf Videokonferenztools in der Regel der Fall, denn diese sind neue (Computer-) Technologien im Sinne von Art. 35 Abs. 1 DSGVO.

Berücksichtigt werden muss beispielsweise, ob die Verarbeitung auf eigenen (mobilen) Endgeräten der Mitarbeitenden und dadurch auch in deren privatem Umfeld erfolgt, um letztlich bestimmen zu können, ob eine Datenschutz-Folgenabschätzung notwendig ist. Organisationen, die hier unsicher sind, sollten sich umfassend beraten lassen.

Anforderungen für kirchliche Träger

Organisationen mit kirchlichen Trägern haben besondere Vorgaben zu beachten, die sich aus dem Kirchengesetz über den Datenschutz der Evangelischen Kirche (DSG-EKD) und dem Gesetz über den Kirchlichen Datenschutz (KDG) ergeben. So sind etwa die EU-Standardvertragsklauseln als Möglichkeit für Auftragsverarbeitungsverträge im Kontext des KDG nicht erwähnt. Das EU-US Privacy Shield ist nach dem jüngsten EuGH-Urteil als Grundlage entfallen und die Auslegung bei Subunternehmen in Drittländern ohne Angemessenheitsbeschluss ist nicht endgültig geklärt; das katholische Datenschutzzentrum in Dortmund erklärte aber auf Anfrage die EU-Standardvertragsklauseln für anwendbar. Die Evangelische Kirche fordert – je nachdem, welche Datenkategorien verarbeitet werden und je nach Ursprungsland des Anbieters – für Cloud-Dienste eine HYOK-Verschlüsselung (Hold-Your-Own-Key). Außerdem muss die Übermittlung von Telemetriedaten unterbunden werden können. Als Folge ist der Einsatz dieser Dienste also fast immer eine (risikoorientierte) Einzelfallentscheidung; eine Datenschutz-Folgenabschätzung wird empfohlen.

Thomas Althammer und Arne Wolff

Anmerkungen

(1) www.katholisch.de/artikel/29109-katholische-datenschutzaufsicht-ost-haelt-zoom-fuer-zulaessig.

(2) www.datenschutzkonferenz-online.de/media/oh/20201023_oh_videokonferenzsysteme.pdf. ■