Foto: Weissblick - stock.adobe.com

Ggf. schnell nachholen: Die datenschutzrechtliche Basis für den Betrieb eines Videokonferenzsystems sicherstellen.

Datensicher per Video kommunizieren

Auch die Sozialwirtschaft setzt in Corona-Zeiten Videokonferenzsysteme ein. Datensicherheit und -schutz erhalten dabei nicht immer sofort ausreichend Aufmerksamkeit. Sollten sie aber.

Manchmal treten Situationen ein, auf die man nicht oder nicht ausreichend vorbereitet ist – dann gilt es, schnell zu reagieren und Prioritäten zu setzen. Die COVID-19-Pandemie ist ein gutes Beispiel hierfür. Hinter der Fürsorgepflicht den Mitarbeitenden gegenüber und den betriebswirtschaftlichen Notwendigkeiten müssen an und für sich unverzichtbare Dinge wie Datensicherheit und Datenschutz unter Umständen zunächst zurückstehen. So ist es verständlich, dass viele Unternehmen unter dem Druck, den Geschäftsbetrieb aufrecht zu erhalten, häufig Mitarbeitende ins Homeoffice geschickt haben, ohne vorher alle erforderlichen Prozesse etablieren zu können. Womit wir beim Thema dieses Beitrages sind: Angesiedelt irgendwo zwischen Telefonat, E-Mail und Meeting ist die Videokonferenz in der gegenwärtigen Situation oft ein wesentlicher Baustein in der Kommunikation mit firmeninternen und –externen Gesprächspartnern geworden. Führten die Tools bisher oft eher ein Schattendasein, erleben die Anbieter derzeit einen globalen Boom.

Features

Dabei ist Videokonferenzsystem nicht gleich Videokonferenzsystem. So zahlreich die Hersteller, so unterschiedlich ist das Leistungsportfolio der Produkte. Das reicht von einfacher „Video-Telefonie“ mit einer relativ begrenzten Anzahl von Teilnehmern 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.

Analog verhalten sich die Kosten für die Systeme, denn Leistung will bezahlt sein. Es ist also wichtig, den Bedarf genau zu prüfen, um das richtige Tool wählen zu können. Als Kriterien seien etwa die maximale Anzahl der Konferenzteilnehmer und die Möglichkeit zu Screensharing und kollaborativem Arbeiten genannt.

Ein Sonderfall 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. Am 06.04.2020 waren 24 Anbieter entsprechend zertifiziert und damit etwa doppelt so viele wie noch vor einem Monat – ein klarer Trend. Befördert wird er von zahlreichen temporär kostenfreien Angeboten der Marktteilnehmer.

„Kriterien zur Auswahl eines Tools können sein: Maximale Anzahl Konferenzteilnehmer und Möglichkeiten zu Screensharing und kollaborativem Arbeiten.“

Arne Wolff, Althammer & Kill, Hannover, info@althammer-kill.de

Implementation

Erfolg ist keine Konstante, die bestehen bleibt, nachdem sie einmal erreicht wurde. Das spiegelt sich wider im „PDCA-Zyklus“ („Plan – Do – Check – Act“, zu deutsch „Planen – Umsetzen – Über-prüfen – Handeln“) aus der Qualitätssicherung. Nachdem nun oft der erste Schritt übersprungen werden musste, ist es umso wichtiger, zu einem strukturierten Vorgehen zurückzufinden. Es gilt jetzt, Erkenntnisse aus der Praxis zu gewinnen: Was funktioniert gut, wo gibt es Probleme? Reicht der Funktionsumfang des gewählten Tools für den sich u.U. verändernden Bedarf? Die nächsten Schritte sind dann, diese Erkenntnisse zu bewerten, daraus Maßnahmen abzuleiten und schließlich, diese umzusetzen.

Und der Datenschutz?

Schnellstmöglich nachgeholt werden sollte auch die Sicherstellung der datenschutzrechtlichen Basis für den Betrieb des Videokonferenzsystems. Schließlich können als personenbezogene Daten mindestens Name, E-Mail-Adresse und Videobild/Stimme der Konferenzteilnehmer, je nach eingesetztem System aber auch Chat-Inhalte, geteilte Dokumente und wie im Falle der Videosprechstunde sogar Gesundheitsdaten übertragen werden.

Exkurs: Kirchliche Träger

Im Bereich von DSG-EKD (Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland) und KDG (Gesetz über den Kirchlichen Datenschutz) gelten zum Teil besondere Vorgaben. So sind etwa die EU-Standardvertragsklauseln als Möglichkeit für Auftragsverarbeitungsverträge im Kontext des KDG nicht erwähnt. Hier ist z.Zt. nur der EU-US Privacy Shield als Grundlage anwendbar, die Auslegung bei Subunternehmen in Drittländern ohne Angemessenheitsbeschluss ist jedoch noch unklar. Die Evangelische Kirche fordert für Clouddienste eine HYOK- (Hold-your-own-Key-) Verschlüsselung und die Unterbindung der Übermittlung von Telemetriedaten. Als Folge ist der Einsatz dieser Dienste also immer eine (risikoorientierte) Einzelfallentscheidung; eine Datenschutz-Folgenabschätzung wird empfohlen.

„Aus der Verfügbarkeit eines Videokonferenzsystems kann Unternehmen künftig ein Wettbewerbsvorteil erwachsen."

Arne Wolff, Althammer & Kill, Hannover, info@althammer-kill.de

Foto: a

Vorteile bewahren – Risiken minimieren

Was bleibt vom jetzigen Hype, wenn die gerade gültigen Maßnahmen wieder zurückgenommen werden? Wahrscheinlich wird sich die Videokonferenz dauerhaft etablieren – zu groß sind die Nutzeffekte dieser flexiblen, „agilen" Kommunikationsmethode gerade in der Sozialbranche. Zu Kosteneinsparungspotentialen besonders in ländlichen Regionen kommen z.B. optimierte Ressourcennutzung, Beschleunigung von Abstimmungsprozessen und nicht zuletzt gesteigerte Attraktivität als Arbeitgeber. Es gilt also, die Vorteile zu bewahren und die Risiken zu minimieren, dann erwächst für die Zukunft aus der Verfügbarkeit eines Videokonferenzsystems ein Wettbewerbsvorteil. Unternehmen, die es im Regelbetrieb nutzen oder zumindest im Bedarfsfall darauf zurückgreifen können, sind in der Lage, flexibler und besser auf Ausnahmesituationen zu reagieren und sind damit robuster aufgestellt. ARNE WOLFF ■

Einen kostenlosen Leitfaden zum Thema können Sie anfordern bei: info@althammer-kill.de

Checkliste

- Beteiligen Sie die Mitarbeitervertretung und den **Datenschutzbeauftragten.**
- Schließen Sie einen Vertrag zur **Auftragsverarbeitung** mit dem Systemanbieter ab.
- Erstellen Sie **Leit- und Richtlinien** für Nutzer und führen Sie Schulungen und Einweisungen in die Tools durch. Dies sorgt für eine höhere Akzeptanz und schnellere Einarbeitung.
- Regeln Sie, wofür eine Videokonferenz genutzt werden darf. Klären Sie die Nutzer auf, wie sie sich zu verhalten haben, um mögliche **Datenabflüsse** zu vermeiden.
- Reduzieren Sie das **Screensharing** auf ein Minimum. Einige Tools bieten Weichzeichner, die den Hintergrund unscharf werden lassen – nutzen Sie sie.
- Erstellen Sie für ein selbst gehostetes Videokonferenztool eine **Datenschutzerklärung**.
- Konfigurieren Sie die **Software** sorgfältig und datenschutzfreundlich. Gehen Sie alle Einstellungs-möglichkeiten durch und handeln Sie dabei nach dem Minimalprinzip; geben Sie also nur so viele **Funktionen** frei wie nötig. Bei Bedarf können weitere Features auch später noch freigeschaltet werden.
- Achten Sie auf eine vollständige **Verschlüsselung** der Übertragung.
- Prüfen Sie die Handhabung der **Benutzerverwaltung** – bspw. Integrationsmöglichkeiten in bestehende Dienste, wie z.B. Active Directory.
- Regeln Sie die **Aufzeichnung** von Ton und Bild – diese sollten nur wenn nötig erstellt werden.
- Prüfen Sie Logfiles, in denen **personenbezogene Daten** gespeichert werden könnten.
- Schalten Sie das **Profiling** der Nutzer möglichst ab.
- Prüfen sie die Transportwege und Speicherorte und klären Sie, wo **Daten gespeichert** werden wenn diese ausgetauscht werden können. Gastteilnehmer sollten zunächst in einem Wartebereich gehalten und erst durch Moderatoren zugelassen werden.
- Nehmen Sie Einstellungen zum **Screensharing** vor – die Steuerung sollte nur nach Freigabe erfolgen.