



Massnahmen für eine sichere Nutzung von Audio- und Videokonferenzlösungen

Die Bevölkerung in der Schweiz und weltweit erlebt im Rahmen der Coronakrise gerade unmittelbar, dass es Ereignisse gibt, welche das gewohnte Umfeld und unsere Verhaltensweisen auf den Kopf stellen können. Von einem Tag auf den anderen ist es nicht mehr möglich, sich mit Verwandten und Bekannten zu treffen oder sich im Büroalltag auszutauschen und Sitzungen abzuhalten. Bürger und Unternehmen werden dadurch gezwungen, schnell auf die Verwendung einer Audio- und Videokonferenzlösung umzustellen, um weiterhin in Kontakt bleiben zu können. Trotz der Eile, mit der Geschäftsmeetings, die Kommunikation von Kindern oder Grosseltern sowie Online-Partys in die virtuelle Welt verlegt werden, ist es wichtig, Informationssicherheits- und Datenschutzverletzungen bei Videokonferenzen zu vermeiden. Dieses Merkblatt richtet sich daher an alle Nutzergruppen – sowohl im privaten wie im geschäftlichen Umfeld.

Dazu empfiehlt der EDÖB in einem ersten Schritt unmittelbar Massnahmen, um die aktuell verwendete Lösung – vorübergehend während einer ausserordentlichen Lage – möglichst sicher verwenden zu können. Danach oder auch bereits während der Nutzung ist der Einsatz dieser Dienste und Produkte im Rahmen einer Risikoanalyse nach den datenschutzrechtlichen Kriterien neu zu beurteilen, allenfalls ein geeigneteres Produkt zu evaluieren und dieses einzusetzen. Hierfür befinden sich in diesem Merkblatt Punkte, welche es bei der Vorbereitung- und danach bei der Einführung einer datenschutzkonformen Audio- und Videokonferenzlösung zu beachten gilt.

Massnahmen zur Verwendung einer Audio- und Videokonferenzlösung

Meeting-IDs nicht öffentlich teilen

Eine Meeting-ID ist eine eindeutige Nummer, welche einem bestimmten Meeting zugeordnet ist. Achten Sie darauf, dass die Meeting-IDs nicht im Internet oder in den sozialen Medien auftauchen. Auch wenn es praktisch ist, führt dies dazu, dass unerwünschte Teilnehmer mittels dieser Nummer in das Meeting verbinden können.

Einmalige Meeting-IDs verwenden und Meetings sperren

Verwenden Sie nicht die gleiche Meeting-ID für aufeinanderfolgende Besprechungen und sperren Sie das aktuelle Meeting, sobald alle Teilnehmenden verbunden sind. So können sich Teilnehmende des nächsten Meetings nicht bereits verbinden und mithören.

Möglichst immer Meeting-Passwörter verwenden

Ein Meeting-Passwort ist ein Kennwort, mit welchem die Verbindung zusätzlich abgesichert werden kann. Meeting-Passwörter bei der Verbindung stellen sicher, dass nur berechtigte Personen mit dem korrekten Passwort am Meeting teilnehmen können. Hierbei wenn möglich, dass Meeting ID und Passwort nicht in der gleichen E-Mail verteilen.

Immer ein Auge auf die Meeting-Teilnehmer halten

Sie sollten periodisch überprüfen, wer am Meeting teilnimmt. Wenn unbekannte Personen auftauchen, sollten Sie diese auffordern, ihre Identität zu bestätigen.

Eine Meeting-Aufzeichnung immer ankündigen

Die Teilnehmenden müssen explizit vorgängig darauf hingewiesen werden, dass eine Aufzeichnung (Ton, Video etc.) des Meetings erfolgt. Sie müssen die Möglichkeit haben, sich ohne Nachteile gegen eine Aufzeichnung auszusprechen und das Meeting allenfalls zu verlassen.

Vorsicht auch hier vor Phishing

Wenn Sie per E-Mail oder über soziale Kanäle den Link für eine Videokonferenz erhalten, sollten Sie sich vor der Verwendung mit dem Absender in Verbindung setzen, um dessen Identität zu überprüfen. Niemals Links und Anhänge von unbekanntem Absendern öffnen!

Kamera bei Nichtgebrauch abdecken und Aufnahmebereich prüfen

Bei Nichtgebrauch der Kamera empfiehlt es sich, diese abzudecken, damit eine heimliche Überwachung über die eigene Webcam verhindert werden kann. Vor der Kamerafreigabe den Aufnahmebereich der Kamera prüfen, welche Informationen für die anderen Teilnehmenden sichtbar sind (z.B. weisse Wand oder Ausdrucke oder ein beschriebenes Whiteboard). Hierzu können auch Videotools mit Blurring-Funktionen, die den Hintergrund unscharf machen, eingesetzt werden.

Bildschirmpräsentation / Screensharing

Präsentieren Sie nur für das Gespräch relevante Informationen. Hierzu sind unnötige Inhalte, Fenster, Tabs zu schliessen. Wenn immer möglich anstelle des Desktops nur das relevante Programm präsentieren. Alternativ kann auch ein separater Desktop eingerichtet werden, auf dem keine Dateien oder Verknüpfungen zu sehen sind.

Datenschutzrichtlinien des Anbieters überprüfen

Einige Anbieter geben persönliche Daten an Dritte weiter oder sie stellen Metadaten wie beispielsweise Dauer, Standort, Teilnehmeridentifikation und Anzahl der Teilnehmer Dritten zur Verfügung. Wenn der Anbieter Ihrer aktuell verwendeten Audio- und Videokonferenzlösung personenbezogene Daten mit Dritten teilt, muss er dies in seinen Datenschutzrichtlinien entsprechend ausweisen. Prüfen Sie daher diese Datenschutzrichtlinien und machen Sie allenfalls von Ihrem Auskunftsrecht Gebrauch.

Folgende Punkte sind bei der Evaluierung, Planung und Vorbereitung einer Audio- und Videokonferenzlösung zu beachten:

Reputation eines Anbieters erfahren

Suchen Sie im Internet Anhaltspunkte über die Nutzerzufriedenheit, nützliche Features oder aber bekannte Sicherheitsprobleme eines Anbieters. Bei Zweifeln lieber einen am Markt etablierte Anbieter auswählen.

Datenschutzrichtlinien des Anbieters überprüfen

Prüfen Sie auch in dieser Phase die Richtlinien des Anbieters betreffend Weitergabe von Personendaten in der Datenschutzerklärung. Handelt es sich um eine Videokonferenzlösung, deren Anbieter ausserhalb der Schweiz oder der EU niedergelassen ist bzw. bei deren Nutzung Daten in diese sogenannten „Drittländer“ übermittelt werden, ist zu klären, ob das jeweilige Land oder der Anbieter ein angemessenes Schutzniveau bietet (bei US-Unternehmen Privacy-Shield-Zertifizierungen) oder ansonsten geeignete Garantien des Anbieters bestehen (Abschluss von Standarddatenschutzklauseln).

Umgang des Anbieters mit Metadaten

Grundsätzlich sollten Sie darauf achten, dass Ihr Anbieter keine Metadaten sammelt, zu eigenen Zwecken verarbeitet und an Dritte weitergibt. Bei diesen Metadaten handelt es sich, neben der bereits genannten Dauer, Standort, Teilnehmeridentifikation und Anzahl der Teilnehmenden der Meetings auch um die E-Mail-Adressen von weiteren Kontakten aus dem Adressbuch oder das verwendete Handymodell und der Browser.

Verschlüsselung der Daten

Alle Daten müssen im gespeicherten Zustand und auch während der Übertragung geschützt werden. Minimal: verschlüsselter Transport; optimal: End-to-End Verschlüsselung.

Physische Sicherheit

Wo genau befinden sich die Datenzentren des Providers der Lösung und erfüllen diese Ihre Sicherheitsanforderungen? Vergewissern Sie sich gerade bei Lösungen mit einer zentralen Datenspeicherung, dass alle Rechenzentren rund um die Uhr abgesichert, regelmässig überprüft und gegen physisches Eindringen geschützt sind. Ein Serverstandort in der Schweiz oder der EU ist dabei von Vorteil.

Sicherheits-Steuererelemente

Einige Videokonferenzdienste bieten fortschrittliche Betrugserkennung, um wiederholte Anmeldefehler zu erkennen. Dadurch können Eindringversuche, wie das gezielte Durchprobieren von Meeting-IDs, erkannt und unterbunden werden.

Das Hinzukommen und Verlassen eines Teilnehmers sollte durch (unterschiedliche) Signalisierungen allen Beteiligten zur Kenntnis gebracht werden. Wünschenswert ist die Möglichkeit der individuellen Abfrage der Anzahl bzw. die Identifikation aller Teilnehmer. Delegationsfunktionen ermöglichen es, die Überwachung und Kontrolle des Meetings zu delegieren oder auch Meetings zu moderieren.

Datenschutzeinstellungen anpassen

Passen Sie die Datenschutzeinstellung innerhalb des Tools standardmässig an, um einer möglichen unzulässigen Datenverarbeitung vorzubeugen. Stellen Sie den Nutzern innerhalb Ihrer Organisation eine Anleitung für die Umsetzung von datenschutzfreundlichen Einstellungen zur Verfügung.

Auch bei der Einführung einer Audio- und Videokonferenzlösung gibt es wichtige Punkte zu berücksichtigen:

Ist eine Registrierung bzw. eine Anmeldung nötig?

Eine Verwendung ohne vorherige Registrierung und Anmeldung kann gerade bei browserbasierten Lösungen ohne Programminstallation sehr praktisch sein. Allerdings ist dabei die Identifizierung der Teilnehmer stark eingeschränkt und sollte daher nicht für die firmeninterne Kommunikation verwendet werden.

Verhindern von unerwünschten App-Zugriffen

Viele Apps greifen – gerade bei mobilen Geräten – unnötigerweise auf persönliche Daten zu. Einerseits sollen die Datenschutzeinstellungen angepasst werden, um einer möglichen unzulässigen Datenverarbeitung vorzubeugen. Andererseits sollten die App-Berechtigungen detailliert konfiguriert (Beschränkung der vergebenen Rechte auf die für den Betrieb der Lösung nötigen Funktionen), dokumentiert und überwacht werden.

Erstellen eines Nutzungsreglements innerhalb der Firma

Wenn kein Nutzungsreglement erlassen wird, besteht Unklarheit über die Berechtigung zur privaten Nutzung der Audio- und Videokonferenzlösung. Ohne ausdrückliche Einschränkung oder Verbot darf der Arbeitnehmer davon ausgehen, dass die private Nutzung im Rahmen des Verhältnismässigen zulässig ist und keine Überwachung vorgenommen wird.

Information über die Überwachung und Aufzeichnung innerhalb der Firma

Anders als beim Nutzungsreglement, das nicht obligatorisch ist, hat der Arbeitgeber die Pflicht, eine eventuelle Überwachung und die Aufzeichnung innerhalb der Audio- und Videokonferenzlösung transparent zu kommunizieren, da sie einen Eingriff in die Privatsphäre des Arbeitnehmers darstellen kann (Prinzip von Treu und Glaube, Art. 4 Abs. 2 DSG).

Bern, April 2020

Weitere Informationen

Liste von Produkten für die [Digitale Zusammenarbeit](#), April 2020, Datenschutzbeauftragter des Kantons Zürich