Zoom – Fluch oder Segen?

VIDEOKONFERENZSYSTEME *Man muss nicht mehr begründen, warum alle Welt auf der Suche nach dem optimalen Videokonferenztool ist. Aber welches Tool erfüllt auch die Anforderungen an Sicherheit und Datenschutz? Leider ist eine große Zahl von Publikationen bei der Beantwortung weder hilfreich noch ehrlich.*

VON KARIN SCHULER

DARUM GEHT ES

1. Videokonferenzen erfreuen sich aktuell weiterhin großer Beliebtheit.

2. Auch Gremien dürfen nach den Änderungen im BetrVG und BPersVG per Videokonferenz Beschlüsse fassen.

3. Aber welches Tool ist sicher? Klare Empfehlungen gibt es leider nicht.

Wenn Fakten in irreführende Zusammenhänge gebracht, Äpfel mit Birnen verglichen und unterschiedliche Maßstäbe angelegt werden, misslingt eine objektive Bewertung der – nicht ganz einfachen – Sachverhalte. Auch angesehene Datenschützer und Datenschutzbehörden sind leider nicht vor solch einseitigen Darstellungen gefeit. Das ist insoweit nachvollziehbar, als es eine einfache Antwort auf die Frage nach einem für alle Anwendungsszenarien gleichermaßen geeigneten Tool nicht geben kann.

Sicherheit entsteht immer erst durch das Analysieren der eigenen Anforderungen, die Überlegungen zu möglichen Angriffsszenarien und durch die Prüfung möglicher Gegen- oder Schutzmaßnahmen. Ein Tool muss daher immer auch in seinem konkreten Anwendungsszenario betrachtet werden. Die Bewertung möglicher Risiken unterscheidet sich bereits anhand erster Nutzungsüberlegungen: Will ich hauptsächlich Termine und Tagesordnungen absprechen oder ganze Betriebsratssitzungen durchführen? Fürchte ich mehr die Indiskretion eines Dienstanbieters oder die meines eigenen Arbeitgebers?

So verständlich also der Wunsch nach einer schlichten Empfehlungsliste ist, so unmöglich ist es, diesen seriös zu erfüllen. Daher wird auch am Ende dieses Beitrags keine Empfehlung ausgesprochen. Allerdings soll in Bezug auf das Tool Zoom die Faktenlage beleuchtet werden, um Ihren Entscheidungsprozess zu unterstützen. Interessant ist Zoom vor allem deswegen, weil man fast wie im Zeitraffer studieren kann, was bei der Software-Entwicklung und -bereitstellung alles schiefgehen kann – und dass Verbesserung möglich ist.

Die Ausgangslage

Bis April 2020 häuften sich Berichte über Sicherheitslücken und fehlende Datenschutzstandards. Eine Verbesserungsinitiative des Unternehmens sollte den Befreiungsschlag bringen. Das für Nutzer sichtbarste Ergebnis ist das Release einer neuen Version 5.0, die seit dem 1. Juni 2020 ausschließlich eingesetzt wird. Aber auch darüber hinaus gab es Änderungen, die mehr Transparenz und Datenschutzfreundlichkeit bewirken sollen (vgl. dazu den Beitrag auf S. 31: »Was ist neu in Version 5.0?«).

Die Popularität von Zoom – bis vor Kurzem noch trotz bekannter Mängel – liegt nicht zuletzt an der einfachen Bedienbarkeit, einer weitgehenden Unabhängigkeit von Hardware und einer sehr guten Performance. Ist es also unter Umständen vertretbar, das Tool nun zu nutzen?

Wie funktioniert eine Videokonferenz?

Stark vereinfacht ausgedrückt wird zwischen den Teilnehmenden einer Konferenz eine sternförmige Verbindung aufgebaut. Damit je-

der mit jedem kommunizieren kann, verbindet man sich mit einem vermittelnden Server, der als zentrale Schaltstelle dient. Gehört einem dieser vermittelnde Server selbst, hat man die volle Kontrolle darüber und muss »nur« noch darauf achten, dass die Wege zwischen Teilnehmenden (bzw. deren Geräten) und dem zentralen Server vor unberechtigter Einsichtnahme geschützt werden. Dies geschieht üblicherweise durch eine Transportverschlüsselung.

Etwas anders stellt sich die Situation dar, wenn einem der zentrale Konferenzserver nicht selbst gehört. Man verlässt sich dann auf einen Dienstleister, der diesen Server und den darauf laufenden Konferenzdienst betreibt. Dieser Betreiber wäre rein technisch in der Lage, auf die während einer Konferenz fließenden Daten Zugriff zu nehmen.

Diesem Risiko kann man entweder normativ (durch Abschluss eines Vertrags, der dem Dienstleister den Zugriff verbietet; dazu unten mehr) oder technisch durch eine E2E-Verschlüsselung begegnen (siehe Infokasten).

Wie verschlüsselt Zoom?

Zoom bietet (noch) keine E2E-Verschlüsselung an – wie übrigens die überwiegende Mehrheit verfügbarer Konferenzsoftware. Man kann vermuten, dass das zumindest teilweise an der technischen Komplexität eines solchen Features liegt. Außerdem entwickelt Zoom seine Software ganz besonders in Hinblick auf sehr große Teilnehmergruppen und Webinare. Eine E2E-Verschlüsselung für 500+ Teilnehmende dürfte nach derzeitigem Kenntnisstand bei gleichbleibender Performance sehr schwer zu realisieren sein.

Zumindest wird, und das muss man von einer Konferenzsoftware auch verlangen, eine Transportverschlüsselung zwischen Teilnehmergerät und zentralem Konferenzserver eingesetzt. Der hierfür seit der aktuellen Version 5.0 (endlich) verwendete Algorithmus AES-256-Bit (für Interessierte: im Galois/Counter-Mode) gilt nach derzeitigem Kenntnisstand als sicher. Damit sind die Daten von Teilnehmenden jeweils zwischen ihrem eigenen Endgerät und dem Zoom-Konferenzserver verschlüsselt, wo sie entschlüsselt werden und für den Weitertransport zu den anderen Teilnehmenden mit deren Schlüssel wieder verschlüsselt werden. Man muss Zoom also vertrauen, dass sie die Umschlüsselung nicht verwenden, um den Datenverkehr mitzulesen – so, wie man jedem anderen Konferenz-Dienstanbieter vertrauen muss, der die technisch schwierig umzusetzende E2E-Verschlüsselung nicht anbietet.

Darüber hinaus hat Zoom nun angekündigt, an der Implementierung einer echten E2E-Ver-

ENDE-ZU-ENDE-VERSCHLÜSSELUNG

Will man technisch ausschließen, dass der Betreiber eines zentralen Kommunikationsservers Einblick in Konferenzdaten erhält, muss eine Verschlüsselung etabliert werden, die den gesamten Datenstrom zwischen je zwei Teilnehmenden unterbrechungsfrei verschlüsselt – eine sogenannte Ende-zu-Ende-Verschlüsselung (E2E). Das ist keine triviale Aufgabe, weil bei mehreren Teilnehmenden jede mit jedem verschlüsselt kommunizieren möchte, also entsprechend viele Verbindungen verschlüsselt werden müssen.
Das Generieren und Verteilen von Schlüsseln für eine solche E2E-Verschlüsselung ist technisch wesentlich aufwändiger, als wenn der zentrale Server »nur« die Wege zwischen sich und allen Teilnehmenden (auf der Transportebene) verschlüsselt. Daher gibt es wenige Konferenzsysteme, die diese echte E2E-Verschlüsselung anbieten.
Zusätzlich geht der Einsatz von E2E-Verschlüsselung aus technischen Gründen meist mit einer Einschränkung bestimmter Funktionen einher: Es sind dann weder Aufzeichnungen möglich, noch kann die Kommunikation mit über eine Telefonleitung (Einwahl) zugeschalteten Teilnehmenden verschlüsselt werden.
Damit der Betreiber des zentralen Konferenzservers selbst keine Konferenzdaten einsehen kann, darf die Hoheit über die Schlüssel der E2E-Verschlüsselung nicht beim Betreiber liegen, weil er die Verschlüsselung sonst im Einzelfall rückgängig machen könnte. Daher stellt die Schlüsselverwaltung eine wesentliche technische Herausforderung beim Einsatz einer E2E-Verschlüsselung dar.

KRITISCHE PUNKTE

Beim Einsatz von Zoom verzichtet man i.d.R. auf:

- Einen selbst betriebenen und administrierten zentralen Kommunikationsserver.
- Auf Ende-zu-Ende-Verschlüsselung.
- In der kostenlosen Version: Auf eine Auswahl der Rechenzentrumsregion.
- Zoom ist ein amerikanischer Anbieter, der dem CLOUD Act unterliegt.
- Das Privacy Shield als Garantie für das angemessene Datenschutzniveau ist eine schwache Garantie.

schlüsselung zu arbeiten. Würde das fachgerecht gelingen, wäre das ein großer Fortschritt, den viele der Branchenriesen bis heute anscheinend nicht einmal erwogen haben.

Welche Daten werden von Zoom erhoben?

Bei der Planung, Durchführung und Teilnahme an einer Zoom-Videokonferenz werden verschiedene Arten von Daten erhoben. Will man selbst Videokonferenzen durchführen, benötigt man ein kostenloses Benutzerkonto. Als nicht-zahlender Kunde muss man bei dessen Anlage eine Mailadresse, einen Benutzernamen und ein Passwort angeben bzw. wählen. Verwendet man die Bezahlversion von Zoom, werden zusätzlich Zahlungsinformationen (Konto, Kontoinhaber, Zahlungsmethode, Rechnungsadresse) erfasst. Einige Angaben, wie z. B. eine Telefonnummer, sind freiwillig.

Die während einer Videokonferenz entstehenden Inhaltsdaten können naturgemäß variieren, je nachdem, ob die Konferenz mitgeschnitten wird, ob parallel gechattet wird oder Bildschirminhalte geteilt werden. Im Hintergrund werden während einer Konferenz Daten der Teilnehmergeräte zur Dienststeuerung (»technische Daten«) erfasst. Dazu gehören insbesondere IP-Adresse, MAC-Adresse, eindeutige ID von Apple-Geräten (UDID), Gerätetyp, Betriebssystemtyp und -version, Client-Version, Kameratyp, Mikrofon oder Lautsprecher und die Art der Verbindung. Auch wird erfasst, ob man sich über Telefon oder »Voice over IP« in eine Konferenz zugeschaltet hat, einen mobilen Client (z. B. Smartphone) oder einen Desktop-Rechner nutzt.

Außerdem versucht Zoom die ungefähre geografische Position in Bezug auf die nächstgelegene Stadt zu ermitteln, um das Routing zu optimieren (also das nächstgelegene Rechenzentrum zu finden) und die richtige Spracheinstellung vorzuschlagen. Es wird keine Standortverfolgung durchgeführt.

Alle zu beeinflussenden Einstellungen werden erfasst, damit sie wunschgemäß umgesetzt werden können. Dazu gehören beispielsweise die Aktivierung des Wartezimmers (Teilnehmende werden vom Moderator einzeln kontrolliert in den Konferenzraum »eingelassen«), die Aktivierung der Aufzeichnung oder die Sperrung der Bildschirmfreigabe für Teilnehmende.

Zu guter Letzt entstehen auch sogenannte Metadaten, also u. a. der Name des Meetings, das geplante Datum und der geplante Zeitraum sowie die tatsächliche Start- und Endzeit (Dauer) und Identifizierungsdaten von Teilnehmenden. Aktiviert der Moderator die Aufzeichnung, wird die gesamte Konferenz audiovisuell aufgezeichnet und in einer Datei gespeichert.

Wo werden die Daten gespeichert?

Alle beschriebenen Daten werden auf Servern gespeichert, die Zoom in Rechenzentren weltweit betreibt. Das Hauptrechenzentrum befindet sich in den USA.

Welche der zentralen Konferenzserver im Einzelfall aktiv sind, hängt nicht zuletzt von den geografischen Regionen ab, aus denen sich die an einer Konferenz Teilnehmenden zuschalten. In der Bezahlversion besteht seit der Version 5.0 die Möglichkeit, bestimmte Weltregionen auszuschließen und zu erzwingen, dass beispielsweise nur europäische Rechenzentren an der Durchführung von Konferenzen beteiligt sind. Will man also amerikanische, chinesische, indische und sonstige außereuropäische Rechenzentren vermeiden, ist eine Lizenzierung der Bezahlversion erforderlich. Hat man diese gewählt, kann man sich als Lizenzadministrator auch während einer Konferenz auf einer Übersichtsseite (Dashboard) anzeigen lassen und prüfen, über welche Wege und Rechenzentren Teilnehmende zugeschaltet sind.

Wer sich allerdings mit seinem eigenen, kostenlosen Zoom-Client in die Konferenz eines lizenzierten Veranstalters einwählt (statt den durch den Veranstalter per Link bereitgestellten Zoom-Client zu nutzen), wird in jedem Fall über US-amerikanische Rechenzentren verbunden – selbst wenn der Veranstalter nur europäische Rechenzentren ausgewählt hat. Ein unerwarteter und unschöner Effekt, denn so kann eine einzelne teilnehmende Person die vermeintliche europäische Konferenz kompromittieren.

Ausgenommen von der zentralen Speicherung aller anfallenden Daten ist die Erstellung von Aufzeichnungen. Hat der Moderator diese eingeschaltet, kann er bestimmen, wo diese gespeichert werden sollen, also auch lokal auf einem eigenen Speichermedium. Für die Erstellung von Aufzeichnungen ist der jeweilige

DIE PFLICHTEN EINES VERANTWORTLICHEN

Neben den allgemeinen Pflichten (z.B. Eintrag im Verzeichnis der Verarbeitungstätigkeiten, Meldepflichten bei Datenpannen usw.) gelten hinsichtlich des Veranstaltens von Videokonferenzen die folgenden Pflichten.
Sofern man den Konferenzserver nicht selbst betreibt:

- Prüfung des Dienstleisters und des Diensts in Bezug auf datenschutzkonforme Nutzungsmöglichkeit (Datenschutzerklärung prüfen; weitere Quellen auswerten)
- Abschluss eines Vertrags zur Auftragsverarbeitung

Darüber hinaus immer:

- Informationen gem. Art. 13 DSGVO bereithalten, um sie Teilnehmenden übergeben zu können (wie eine solche Information aussehen könnte, hat der Kollege Stephan Hansen-Oest öffentlich bereitgestellt)
www.datenschutz-guru.de/download/101800
- Mitteilen des Starts von Aufzeichnungen und den rechtskonformen Umgang damit
- Beantworten von Auskunftsersuchen ehemaliger Teilnehmender
- Nutzen der Sicherheitseinstellungen
- Rechtskonformer Umgang mit Daten aus Meetings inkl. Nutzungsberichte

LESETIPP

Für tiefergehende Betrachtungen empfehlenswert: Kompendium Videokonferenzsysteme des Bundesamts für Sicherheit in der Informationstechnik unter **www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Videokonferenzsysteme/videokonferenzsysteme_node.html**

Moderator im datenschutzrechtlichen Sinne verantwortlich und muss dafür sorgen, die Einwilligungen aller Teilnehmenden einzuholen. Er wird dabei durch technische Funktionen von Zoom (u.a. eine automatisierte Pop-up-Benachrichtigung) unterstützt.

Eine Offenlegung von Daten an Dritte erfolgt nur im Rahmen der Konferenz selbst gegenüber anderen Teilnehmenden (Teilnahmeliste, Videobild, Chatinhalte) und gegenüber Dienstleistern, die auf der Grundlage von Auftragsverarbeitungsverhältnissen für Zoom tätig werden (z.B. Rechenzentrumsbetrieb, Zahlungsdienstleister). Zoom sagt ausdrücklich zu, Daten, die bei der Nutzung des Konferenzdiensts entstehen, weder an Dritte zu verkaufen noch für Marketingzwecke zu verwenden.

Wer ist verantwortlich für Datenschutz?

Für die Einhaltung datenschutzrechtlicher Pflichten ist immer der Verantwortliche im Sinne der Datenschutz-Grundverordnung (DSGVO) zuständig. Zoom wird rechtlich im Auftrag seiner Kund(inn)en (der Konferenzveranstalter) tätig. Den Einladenden treffen damit alle datenschutzrechtlichen Pflichten in Zusammenhang mit der Durchführung einer Konferenz. Das gilt wohlgemerkt immer, ob man den Konferenzserver nun selbst betreibt oder nicht, und bei Zoom genauso wie z.B. bei Skype/Teams, WebEx oder Jitsi Meet auf fremden Instanzen.

Die Datenschutzrichtlinie von Zoom

Die Datenschutzrichtlinie von Zoom[1] wurde im Rahmen der erwähnten Verbesserungsinitiative grundlegend überarbeitet. Sie enthält nun recht übersichtliche Erläuterungen zu den erhobenen Daten und deren Zwecken. Insbesondere kann ihr der Durchführende einer Konferenz entnehmen, welche Informationen nach Art. 13 DSGVO er den Teilnehmenden geben muss.

Deutlich verbesserungswürdig sind allerdings die Angaben zu den von Zoom beauftragten Subunternehmern.[2] Der Verantwortliche muss alle Empfänger der verarbeiteten personenbezogenen Daten benennen (Art. 13 Abs. 1e) i.V.m. Art. 4 Nr. 9 DSGVO). Darunter fallen auch Auftragsverarbeiter. Das kann dem Konferenzveranstalter nur gelingen, wenn Zoom seine Subunternehmer so offenlegt, dass man erkennen kann, welche Auftragnehmer zu welchen Zwecken beauftragt werden und welche Verarbeitungen sie jeweils durchführen. Derzeit wird jedoch nicht deutlich, welcher Auftragsverarbeiter welche Daten erhält, insbesondere ist nicht erkennbar, welche der Unterauftragsverarbeiter überhaupt mit dem Videokonferenzservice in Zusammenhang stehen. Hier sollte unbedingt nachgebessert werden.

Zusätzlich gibt es ein Dokument, in dem in Anlehnung an die Anforderungen des Art. 13 DSGVO dargestellt wird, wie wesentliche Datenschutzanforderungen erfüllt werden. Hier findet man beispielsweise den Namen der Da-

1 https://zoom.us/de-de/privacy.html

2 https://zoom.us/subprocessors

WAS IST EINE AVV?

Eine Auftragsverarbeitung ist ein juristisches Konstrukt, bei dem der Verantwortliche dem Empfänger personenbezogener Daten die Verarbeitungszwecke streng und ausschließlich vorgibt. Der Auftragnehmer (der Dienstleister) ist an die Vorgaben des Auftraggebers (des Kunden) strikt gebunden und darf keinerlei eigene Zwecke mit der Verarbeitung dieser Daten verfolgen.

tenschutzbeauftragten. Eine Zusammenführung mit der Datenschutzrichtlinie wäre aus Gründen der Übersichtlichkeit sehr zu wünschen.

Der Auftragsverarbeitungsvertrag (AVV)

Sofern nicht nur die Software auf einem eigenen Konferenzserver genutzt wird, sondern der zentrale Server von einem Dienstleister betrieben wird, handelt es sich datenschutzrechtlich um eine Datenverarbeitung im Auftrag, die einen entsprechenden Vertrag (AVV) erforderlich macht. Dieser stellt sicher, dass der Dienstleister Konferenzdaten seines Kunden nicht einsieht und nicht auswertet, es sei denn, er wird von seinem Kunden z. B. im Rahmen einer Fehlersuche zur Unterstützung aufgefordert.

Dass man mit der Registrierung bei Zoom automatisch einen AVV abschließt, ist vielleicht nicht allen bewusst. Das Unternehmen bedient sich nämlich einer etwas unübersichtlichen Verweisstrategie. Bei der verpflichtenden Registrierung muss man die Geltung der Datenschutzrichtlinie und der Nutzungsbedingungen akzeptieren. Hinter den Links bei der Registrierung stehen englische Dokumente; die deutschen Versionen muss man sich selbst heraussuchen.[3] In Ziffer 20 der Nutzungsbedingungen werden alle Dokumente unter »www.zoom.us/de-de/privacy-and-legal.html« zu Vertragsinhalten gemacht. Darunter findet sich dann auch der Vertrag zur Auftragsverarbeitung gemäß Art. 28 DSGVO.

Was die zusätzlich erforderliche Sicherstellung des angemessenen Datenschutzniveaus angeht (wegen der Verarbeitung außerhalb der EU), ist Zoom, wie andere Anbieter auch (z. B. Microsoft Teams, GoToMeeting, Jitsi Meet) durch den Privacy Shield zertifiziert. Dabei handelt es sich um eine unter Datenschützern sehr umstrittene Lösung, formaljuristisch ist derzeit aber von einem ausreichenden Datenschutzniveau für die zertifizierten Daten auszugehen. Da Zooms Privacy-Shield-Zertifizierung jedoch keine Beschäftigtendaten umfasst, dürfen diese streng genommen nicht auf außereuropäischen Zoom-Servern verarbeitet werden. Es bleibt also für diese Daten nur die Nutzung der Bezahlversion von Zoom mit der Möglichkeit, die ausschließliche Nutzung europäischer Rechenzentren zu erzwingen.

Was bedeutet das für die Anwendung?

Aus Sicherheits- und Datenschutzsicht besteht die beste Lösung darin, ein System einzusetzen, dessen Server unter eigener Hoheit steht, sodass die Konferenzdaten auf eigenen Systemen verarbeitet und gespeichert werden.

Ist dies nicht möglich, lautet die zweitbeste Lösung, einen Dienstleister zu beauftragen, der mit seinem Konferenzsystem eine echte E2E-Verschlüsselung anbietet. Da es derartige Systeme derzeit nicht eben zahlreich auf dem Markt gibt (und diese nicht notwendigerweise gerade die eigenen Anforderungen z. B. an Performance und Ausfallsicherheit abdecken), kommt als drittbeste Lösung eine Anwendung in Betracht, bei der der Dienstleister zwar keine E2E-Verschlüsselung anbietet, aber alle daraus erwachsenden datenschutzrechtlichen und sicherheitsrelevanten Anforderungen nachvollziehbar und transparent erfüllt bzw. unterstützt.

Ob man es bei der drittbesten Lösung für einen weiteren Vorteil hält, die Kommunikation ausschließlich über europäische Rechenzentren abzuwickeln, hängt davon ab, ob man dem Anbieter (zu)traut, die versprochenen Schutzmechanismen auch weltweit einzuhalten und für wie relevant man den Einfluss und eventuelle Druckentfaltung durch außereuropäische Geheimdienste hält. Auch wenn eine rein europäische Kommunikationslösung formal (durch die Geltung der DSGVO) stärker geschützt erscheint: Angriffe durch Geheimdienste und Sicherheitsbehörden halten sich, wie wir spätestens seit Edward Snowden wissen, höchstens an eigene nationale Gesetze, wenn überhaupt. Und rein technisch kann ein Angriff im Internet genauso gut auf europäische wie auf US-amerikanische Server zielen.

Sollte man sich nach Abwägung aller Fakten entscheiden, Zoom einzusetzen, muss einem bewusst sein, über welche Hürden man, trotz aller hoffnungsvollen Verbesserungen des Diensts in letzter Zeit, springen muss. Viele dieser Hürden gelten übrigens so oder ähnlich auch für andere populäre Videokonferenzanwendungen. ◁

Karin Schuler,
Datenschutz & IT-Sicherheit, Netzwerk Datenschutzexpertise, Bonn
buero@schuler-ds.de

3 https://zoom.us/de-de/terms.html und https://zoom.us/de-de/privacy.html

Was bringt Version 5.0?

ZOOM *Die Videokonferenzsoftware hat sich in der Vergangenheit bei Datenschutz- und Sicherheitsthemen nicht gerade mit Ruhm bekleckert. Seither gab es viele Versprechungen und eine neue Version 5.0. Ist jetzt alles anders?*

VON KARIN SCHULER

Spätestens Anfang April 2020 hat Zooms Chef Eric Yuan wohl begriffen, dass er es mit der IT-Sicherheit »richtig verbockt« hat, wie er in einem Interview mit dem Wall Street Journal einräumte.

Zu den öffentlich diskutierten Mängeln gehörten u. a.:

- Lange behauptete das Unternehmen, eine Ende-zu-Ende-Verschlüsselung (E2E-Verschlüsselung) umzusetzen. Dies hat sich allerdings als Schönfärberei herausgestellt.
- Durch Nutzung eines Programmteils von Facebook zur Erleichterung der Anmeldung gab es unerwartete und unzulässige Datenübermittlungen an Facebook.
- Es gab Probleme mit dem sogenannten Company Directory, wonach Zoom-Nutzende, deren Mailadresse auf die gleiche Domain lautete (z. B. @t-online.de, @gmx.de) sich plötzlich gegenseitig im Adressverzeichnis wiederfanden.
- Die Installationsroutine für Geräte mit MacOS war unsicher. Es gab die theoretische Möglichkeit von Manipulationen bei der Installation und des Kaperns der Kamera.
- Die Äußerungen des Unternehmens bezüglich des Umgangs mit Daten ihrer Kund(inn)en waren bestenfalls missverständlich. Es klang so, als ob das Unternehmen sich vorbehielte, deren Daten zu verkaufen.
- Die Analyse des Windows-Clients durch den IT-Sicherheitspezialisten Thorsten Schröder ergab noch Mitte April 2020 erschreckende Erkenntnisse in Bezug auf die Verwendung veralteter, unsicherer Software-Bibliotheken und Angriffsmöglichkeiten durch schlampige Programmierung.
- Der sogenannte »Warteraum« einer Konferenz war unsicher programmiert (man konnte dort das Meeting verfolgen, ohne eingelassen worden zu sein). Der Fehler wurde innerhalb einer Woche nach Meldung behoben, was für eine Software-Firma eine schnelle Reaktion darstellt.

Zoom hat mittlerweile eine Reihe von Sicherheitsfunktionen verbessert, die nun in der Version 5.0 verfügbar sind. Einige Aspekte sind darüber hinaus von den Nutzenden zu beachten und umzusetzen.

▸ Registrierung & Anmeldung

Nur wer sich in Zoom registriert hat, kann Videokonferenzen veranstalten. Sowohl beim Registrierungsvorgang als auch bei den folgenden Anmeldungen ist Vorsicht geboten. Gleich bei der Registrierung wird versucht, einen zur Eingabe von Daten Dritter zu animieren (»Laden Sie Freunde ein!«). Das sollte man auf jeden Fall unterlassen! Auch sollte die Anmeldung bei Zoom immer direkt und mit eigens für Zoom reservierten Zugangsdaten erfolgen. Eine Anmeldung über andere Dienste (Facebook, Google) sollte vermieden werden, um diesen Diensten keine Querprofile zu ermöglichen.

▸ Aufmerksamkeitstracking & Aufzeichnungen

Das Aufmerksamkeitstracking scheint Geschichte zu sein. Dabei handelte es sich um eine Funktion, mit deren Hilfe der Moderator sich anzeigen lassen konnte, wenn auf Endgeräten von Teilnehmenden mehr als 30 Sek. der Fokus nicht auf dem Zoom-Fenster lag

DARUM GEHT ES

1. Zoom ist ein beliebter Anbieter von Software für Videokonferenzen.

2. Etwa bis Mitte April 2020 häuften sich Beschwerden über Mängel bei Sicherheit und Datenschutz.

3. Zoom hat mittlerweile eine neue Version 5.0 im Einsatz, die viele Mängel behoben hat.

HINTERGRUND

Angriffe wie das »Zoombombing«, also die Übernahme einer Konferenz, indem man die Konferenz-ID zu raten versucht und dann den Bildschirm übernimmt, haben mediale Aufmerksamkeit auf die diversen Schwächen von Zoom gelenkt.

SICHERHEITSFUNKTIONEN NUTZEN

- Pro Konferenz sollte ein neues Passwort vergeben werden.
- Konferenzen sollten als geplante (scheduled) Meetings veranstaltet werden, weil sie dann eine einmalige ID erhalten, die für Außenstehende schwerer zu erraten ist.
- Niemand sollte für Zoom Authentisierungspaare (E-Mail-Adresse, Passwort) nutzen, die auch in anderen Zusammenhängen zur Authentisierung genutzt werden, damit bei Sicherheitslücken keine weiteren Dienste kompromittiert sind (allgemeine Regel).
- Nutzung des Warteraums, um Teilnehmende nach und nach explizit durch den Moderator in den Konferenzraum zulassen zu können.
- Schließen des Meetingraums (lock), sobald alle Teilnehmenden anwesend sind. Niemand sollte während der Konferenz Links (UNCs) versenden oder anklicken, weil diese z.B. zum Ausspähen des Windows-Passworts missbraucht werden könnten. Hierbei handelt es sich allerdings um ein Problem »klickbarer Links«, nicht um ein Zoom-Problem.

TIPP

Aufzeichnungen sollten immer sehr zurückhaltend eingesetzt und der Zweck allen Teilnehmenden zuvor klar erläutert werden (siehe Info gem. Art. 13 DSGVO). Wenn sie durchgeführt werden, sollte die resultierende Datei unbedingt lokal und geschützt vor unberechtigtem Zugriff abgelegt werden. Die festgelegte Löschfrist muss eingehalten werden.

(weil jemand beispielsweise parallel E-Mails beantwortete).

Sobald ein Moderator für eine Konferenz eine Aufzeichnung startet, werden alle Teilnehmenden automatisch hierüber informiert, sodass man die Möglichkeit hat, die Konferenz zu verlassen.

▸ Clients für Teilnehmende

Konferenz-Tools verfolgen unterschiedliche Strategien, wie sich Teilnehmende in eine Konferenz zuschalten können. Entweder wird ein eigener Software-Client oder eine App installiert oder aufgerufen oder man kann mit dem eigenen Browser an der Konferenz teilnehmen. Sichere Clients für PC und Handy können immer nur so sicher sein, wie das Gerät selbst. Da sind bei einem Handy schon »konstruktionsbedingt« Grenzen gesetzt. Der Vorteil von eigenen Clients (im Gegensatz zum Browser) besteht in der grundsätzlich besseren Kontrollierbarkeit durch den Anbieter. Traut man dem Anbieter nicht und möchte die Software nicht installieren, bietet Zoom die Nutzung des eigenen Browsers an. Dann allerdings kann sich dessen Grundeinstellung und Sicherheit auf die Sicherheit der Konferenz auswirken. Sofern Teilnehmer über das Zoom-Webportal teilnehmen möchten, sollte der Moderator für sie per Einstellung eine besonders sichere 2-Faktor-Authentisierung erzwingen.

▸ Vertraulichkeit & Einbruchsschutz

Was man in einer Videokonferenz nicht gebrauchen kann, sind Mithörende und Mitschauende, die sich unerkannt in den Konferenzraum geschlichen haben und im schlimmsten Fall sogar unbemerkt Mitschnitte herstellen. Ähnlich katastrophal ist es, wenn ein unberechtigter Außenstehender eine Konferenz »sprengen« kann – sei es durch offensichtliche technische Übernahme der Sitzung oder durch Kapern und Abbruch des Meetings. Zoom hat derartige Angriffe in der Vergangenheit und vor Entwicklung seiner Version 5.0 durch bestimmte nachlässige Gestaltung seines Diensts sehr leicht gemacht – auch wenn manche Lücken letztlich erst durch fahrlässige Moderatoren richtig zum Tragen kamen, denen schon die Vergabe eines Passworts für eine Konferenz zu viel des Aufwands schien.

Software-Entwicklung

Zoom hat drei Tochterfirmen in China, die bei der Programmierung der Software involviert sind. Ob man Transparenzbemühungen von Zoom Glauben schenken mag oder nicht, die schlichte Begründung, alles was »mit China zu tun habe« sei unakzeptabel, scheint sehr kurz gesprungen. Zwar kann nicht ausgeschlossen werden, dass die chinesische Regierung versucht, Einfluss auf Software-Entwickler zu nehmen, um Daten abzugreifen. Nur können wir das Gleiche auch von den USA annehmen. ◁

Karin Schuler,
Datenschutz & IT-Sicherheit, Netzwerk Datenschutzexpertise, Bonn
buero@schuler-ds.de