Videokonferenzsystem Zoom im Sicherheitscheck

FERNKOOPERATION MIT RISIKO?

Mit den Reisebeschränkungen in der Corona-Krise ist der Bedarf an einfach zu handhabenden Videokonferenzsystemen sprunghaft gestiegen. Krisengewinner war dabei ohne Zweifel der amerikanische Hersteller Zoom Video Communications. Mit seinem „Zoom Meeting"-Dienst preschte das junge Unternehmen an bisherigen Branchenlieblingen vorbei. Derzeit gilt Zoom als populärstes Konferenzsystem auf dem Markt. Mitten im Aufstieg ist Zoom jedoch auch heftig in Kritik geraten: Schlechte Umsetzung des Datenschutzes, hohe Angreifbarkeit durch klaffende Schwachstellen und unzureichende Verschlüsselung lauteten die Vorwürfe. Der Hersteller zeigte sich bei der Behebung der Schwachstellen kooperativ. Doch ist jetzt alles sicher und vertrauenswürdig?

Mit dem Erfolg stieg auch die Aufmerksamkeit bei einschlägigen Security-Unternehmen. Und das, was diese im April über den Shooting-Star unter den Videoconferencing-Tools herausfanden, war wenig vertrauenserweckend: So konnten Angreifer recht einfach öffentliche Zoom-Meetings mithören, zweckentfremden und sogar zum Absturz bringen – das sogenannte „Zoom Bombing". Über eine Schwachstelle im UNC-Handling (Uniform Naming Convention) konnten die Kriminellen via Chat die Windows-Anmeldedaten der Nutzer ergattern. Generell wurden Schwächen bei der Verschlüsselung moniert.

Zoom hat sehr schnell auf die Vorwürfe regiert und zur Verbesserung der Sicherheit 90 Tage (das war der Zeitraum vom 23.04.2020 bis zum 21.07.2020) für die Kontestation zur Behebung von Sicherheitsproblemen festgesetzt. Im Rahmen dieses 90-Tage-Plans wurde regelmäßig ein Fortschrittsbericht veröffentlicht, welcher die Entwicklungen in Sachen Security dokumentierte. Zusätzlich stellt Zoom jetzt regelmäßig White Paper zur Sicherheit und Verschlüsselung bereit. Zoom geht im Verbesserungsprozess der Sicherheit seiner Software sehr transparent vor, und die dazu publizierten Informationen sind auch für Nicht-Informatiker verständlich. Inzwischen hat das Unternehmen Zoom in Version 5.0 veröffentlicht – die bis zum Beginn des 90-Tages-Plans bekannten Sicherheitsmängel sind ab dieser Version behoben.

ZOOM IM VERGLEICH ZU ANDEREN VIDEO-KONFERENZ-LÖSUNGEN

Das Erstaunliche an Zoom ist, dass es auch die ganz großkalibrigen Platzhirschen am Markt, wie Microsoft Teams und Google Meet, innerhalb kurzer Zeit auf die Plätze verwies. Bild 1 zeigt die täglichen Nutzer von Zoom, Google Meet, Microsoft Teams.

ZOOM UND SEIN ERFOLG

Zoom startete seinen Betrieb im Frühjahr 2011, zwei Jahre später kam das erste Produkt auf den Markt. Im Jahr 2019 verzeichnete Zoom bereits einen Umsatz von 622,7 Millionen US-Dollar.[1] Der Erfolg von Zoom lässt sich auf drei wesentliche Faktoren zurückführen:

- die einfache Nutzung und Zugänglichkeit,
- die Qualität der Konferenzen und
- die vergleichsweise niedrigen Kosten.

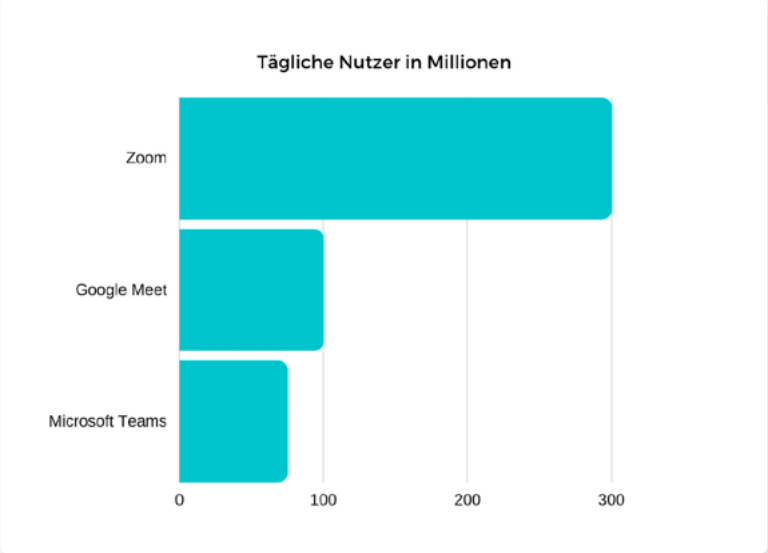


Bild 1: Zoom verzeichnet ca. 300 Millionen Nutzer täglich. Google Meet ca. 100 Millionen und Microsoft Teams ca. 75 Millionen tägliche Nutzer.[2]

Im Vergleich zu anderen Videoplattformen ist Zoom für jeden zugänglich. Zu Beginn des Jahres 2020 war es nicht erforderlich, einen Zoom Account zu besitzen, um an Meetings teilzunehmen. Aus Sicherheitsgründen ist dies heute nicht mehr der Fall und jeder Nutzer von Zoom muss einen Account anlegen. Dennoch ist Zoom für jeden zugänglich, da ein Account nicht speziell an ein Unternehmen oder eine Institution, wie Schulen oder Universitäten, gebunden ist. Gerade gegenüber Microsoft Teams ist die Verwendung von Zoom auch für nicht IT-affine Nutzer einfacher. Nur ein Klick ist ausreichend, um an einem Meeting teilzunehmen. Dazu ist dank der Browser-Funktion keine weitere Software nötig.

Die Qualität der Konferenz hängt hauptsächlich von Quality-of-Service-Parametern ab, die bei leistungsstarken Endgeräten und Netzwerken sehr hoch sind. Dabei werden die Übertragungskapazität, die Laufzeitverzögerung, die Laufzeitschwankung und der Paketverlust betrachtet. Zoom empfiehlt eine verfügbare Bandbreite von 600 KBit/s für qualitativ hochwertige Videos und 1,2 MBit/s für HD-Videos. Eine einfache Sprachverbindung (Voice-over-IP-Verbindung) kann bereits mit 60–80 KBit/s realisiert werden. Im Zoom Client können die Parameter unter „Einstellung und Statistiken" eingesehen werden. Die Laufzeitverzögerung wird als Latenz, die Laufzeitschwankung als Jitter angegeben. Diese Werte sollten so klein wie möglich sein, um eine gute Gesprächs- und Bildqualität zu gewährleisten.

Der Zoom Account kann in einer Basisversion kostenlos genutzt werden. Einschränkungen, wie die Dauer von Meetings, die für einen kostenlosen Account bei 40 Minuten liegt, sind anlässlich der Corona-Pandemie deaktiviert worden. Kostenpflichtige Accounts beginnen bei Zoom mit 13,99 Euro pro Monat pro Moderator oder 18,99 Euro pro Monat pro Moderator.[3] Microsoft Teams ist im Businessbereich in Office-365-Paketen enthalten, diese liegen preislich zwischen 4,20 und 16,90 Euro pro Monat pro Nutzer.[4] Google Meet bietet neben dem kostenlosen Paket mit Einschränkungen ebenfalls Enterprise-Lösungen an. Die Kosten liegen bei 10 bis 20 Dollar pro Monat pro aktiven Nutzer.[5] Im Gegensatz zu Zoom benötigen bei Microsoft Teams und Google Meet alle Teilnehmer ein Konto. Auch für die private Nutzung ist ein Konto erforderlich.

Zusätzlich bietet Zoom eine Handvoll Plug-ins an, um die Nutzung so einfach wie möglich zu gestalten. Die Plug-ins sind für die Webbrowser Chrome und Firefox sowie für das E-Mail-Programm Outlook verfügbar und ermöglichen die Planung eines Meetings in gleicher Form.

Ebenfalls ist die Planung mittels des Google-Kalenders möglich.

SICHERHEITSASPEKTE DER SOFTWARE

In den vergangenen Monaten sind mehrere Schwachstellen rund um die Zoom-Software bekannt geworden. Bei einer maßgeblichen Schwachstelle handelt es sich um die Verschlüsselung von Daten und Gesprächen. Ein wesentlicher Sicherheitsaspekt ist die Ende-zu-Ende-Verschlüsselung, die nicht gewährleistet war. Zoom stellte nur eine Verbindungsverschlüsselung (Link Encyption) bereit, dabei waren die Daten unverschlüsselt auf den Zoom-Servern vorhanden. Außerdem behauptete Zoom, dass die Verschlüsselung mit AES-256 umgesetzt wurde. Tatsächlich wurde AES-128 im Electronic-Codebook-(ECB-)Modus verwendet und Schlüssel wurden von nicht näher bestimmten „chinesischen Servern" generiert. Natürlich lässt sich nicht mit Bestimmtheit sagen, ob die chinesische Regierung Zugriff auf die Schlüssel hat – die Wahrscheinlichkeit ist jedoch hoch. Daraus ergibt sich ein unkalkulierbares Risiko für die Nutzer. Die Übermittlung von sensiblen Daten über ausländische Server stellt sogar einen veritablen Sicherheitsverstoß dar, wenn die Regeln auf Nutzerseite generell kein Routing über bestimmte Länder zulassen. Der bekannte IT-Sicherheitsexperte Bruce Schneier sagte dazu: „I'm okay with AES-128, but using ECB (electronic codebook) mode indicates, that there is no one at the company, who knows anything about cryptography."[6] (frei übersetzt: „Mit AES-128 könnte ich noch leben, aber die Verwendung des ECB-Mode zeigt, dass in diesem Unternehmen offenbar niemand auch nur einen Schimmer von Verschlüsselung hat") Zwischenzeitlich hat Zoom zunächst für zahlende Kunden eine Ende-zu-Ende-Verschlüsselung zur Verfügung gestellt.

Eine weitere Schwachstelle, die medial viel Aufmerksamkeit bekam, war der Diebstahl von Zugangsdaten mittels UNC-Hyperlinks. Diese beschreiben Adressen zu Webseiten (Server) im Internet (Netz). Beispielsweise führt der Link \\evil.server.com\images\cat.jpg auf eine vom Angreifer kontrollierte Infrastruktur und öffnet dort eine Bild-Datei. Dabei konnten Angreifer UNC-Hyperlinks in den Chat des Zoom-Meetings schreiben, welche von Zoom als Hyperlinks angezeigt wurden. Ein Klick auf diese Links führte dann über eine durch den Angreifer kontrollierte IT-Infrastruktur dazu, dass das Windows-Betriebssystem den Nutzernamen und Passwort als NTLM-Hash verschickte.

Im April dieses Jahres wurden Schwachstellen des Zoom-Client für eine halbe Million Dollar zum Verkauf angeboten. Dabei handelte es sich um sogenannte Zero-Day-Exploits für Windows und MacOS. Diese Schwachstellen ermöglichten es Angreifern, Zoom-Meetings auszuspionieren. Bei Windows wird dies durch eine Remote Code Execution ermöglicht, also das Ausführen von Schadcode auf fremden Endgeräten.[7] Der hohe Preis verdeutlicht, wie schwer es ist, eine fatale Schwachstelle zu entdecken. Ob Zoom sie gekauft hat, ist nicht bekannt.

MÄNGEL BEIM DATENSCHUTZ

Wegen der gravierenden Mängel beim Datenschutz wurde die Verwendung von Zoom in zahlreichen Unternehmen und Organisationen beschränkt – zum Teil, etwa in politischen Institutionen, sogar verboten. Beispielsweise haben Google und SpaceX, aber auch deutsche Konzerne und mittelständische Unternehmen, die Nutzung von Zoom eng limitiert. Regierungen und Behörden in Ländern wie England, USA und Taiwan untersagen die Verwendung von Zoom. In Deutschland riet das Auswärtige Amt ebenfalls davon ab.

Die größten Probleme hinsichtlich des Datenschutzes war die Übermittlung von Daten an Drittanbieter, die nicht angegeben worden waren. Auch das sogenannte Zoom-Bombing, welches das unerwünschte Eindringen und Stören von Unbefugten in einer Videokonferenz beschreibt, stellte einen Verstoß gegen den Datenschutz, die Privatheit und die Vertrauenswürdigkeit dar. Unter anderem konnten sich Unbefugte in Konferenzen einwählen und dort unberechtigt mithören sowie Straftaten begehen. Beispielsweise durch pornografische, gewaltverherrlichende oder rechtsextreme Inhalte.[8] Ebenfalls wurden Namen von Teilnehmern der Anonymen Alkoholiker erkannt und veröffentlicht. Zusätzlich machte Zoom negative Schlagzeilen, da Daten von der iOS-App an Facebook übermittelt worden sind.

Funktionen wie „Attention Tracking", also das Beobachten von Aktivitäten der Teilnehmer während eines Meetings, stellt in Deutschland nicht nur einen Datenschutzverstoß, sondern auch einen Verstoß gegen das Arbeitsrecht dar: Die Administratoren und Hosts von Meetings konnten die Aktivitäten der Teilnehmer (Mitarbeiter) verfolgen und überwachen – beispielsweise, ob das Meeting über Zoom als primäres Fenster geöffnet ist, oder ob der Teilnehmer zusätzlich anderen Tätigkeiten an seinem IT-System nachgeht. Die Rolle des Administrators beschreibt den Verantwortlichen für die gesamte Zoom-Instanz innerhalb eines Unternehmens oder Organisation. Er ist in der Lage, globale Einstellungen für Meetings vorzunehmen. Der Host ist für die einzelnen Meetings verantwortlich. Er kann bestimmte Sicherheitseinstellungen vornehmen, kann Teilnehmer zulassen oder entfernen etc. Ein Teilnehmer kann keine generellen sicherheitsrelevanten Einstellungen im Meeting vornehmen, dafür aber einige persönliche Einstellungen vornehmen.

Die Datenschutzerklärung von Zoom wurde zum 29. März 2020 aktualisiert.[9] Außerdem wurde das „Attention Tracking" entfernt. Dadurch ist es nicht mehr möglich, die Aktivitäten der Teilnehmer während eines Meetings nachzuverfolgen. Zoom speichert nur noch Basisinformationen, wie E-Mail-Adresse, Passwort, sowie Vor- und Nachname. Alle weiteren Angaben sind optional vom Nutzer anzugeben.

Zoom versichert, dass sie niemals Informationen über Nutzer verkaufen wollten und werden. Ebenfalls sichert Zoom zu, dass Meetings nicht überwacht werden. Damit ist die Datenschutzerklärung konform mit der Europäischen Datenschutz-Grundverordnung – in Deutschland also der DS-GVO.

ZOOM-PLATTFORMEN UND IHRE RISIKEN

Ist der Einsatz von Zoom damit nun bedenkenlos möglich? Nicht ganz – einige Risiken bestehen nach wie vor. An manchen Stellen ist es für den sicheren Einsatz sehr ratsam, die Einstellungen entsprechend zu justieren. Doch zunächst ein Blick auf die Zoom-Plattformen.

1. Client

Der Zoom-Client bietet eine komfortable Lösung, um Zoom auf dem Notebook oder PC zu nutzen. Die Teilnehmer können unter anderem

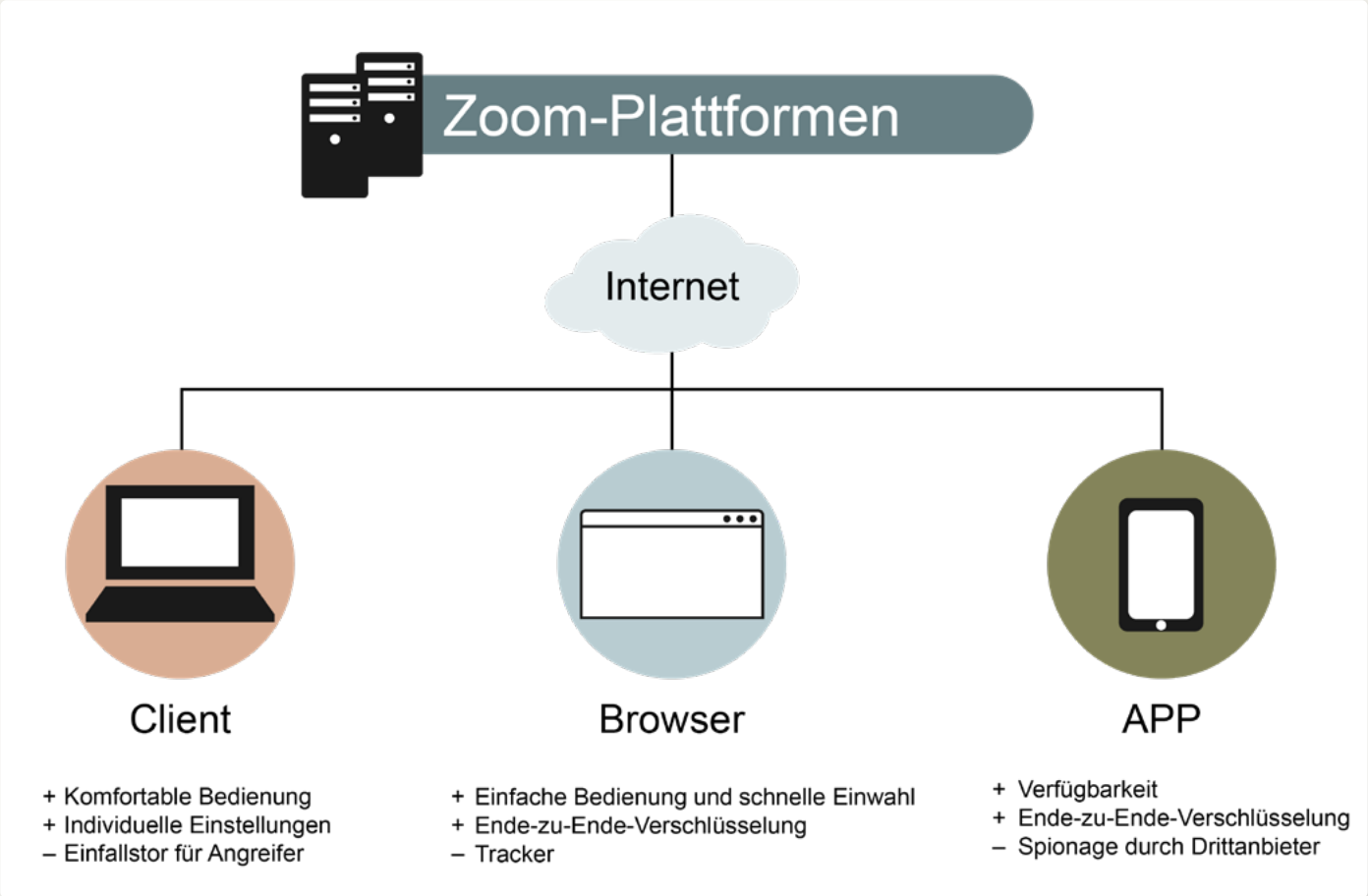


Bild 2: Technologien und Zusammenhänge der Zoom-Videokonferenz-Lösung.

einen virtuellen Hintergrund verwenden und individuelle Einstellungen vornehmen. Auch das Teilen von Ansichten während eines Meetings ist komfortabel, da alle Teilnehmer eine Präsentation zeigen und auch angezeigt bekommen können. Mitschnitte von Meetings können außerdem direkt lokal gespeichert werden. Ein Risiko bei der Verwendung des Zoom-Clients besteht darin, dass er direkt auf dem IT-System installiert wird und so Angreifer potenziell Zugriff auf das IT-System der Nutzer erlangen konnten.

2. App

Die App bietet dem Nutzer die Möglichkeit, von überall an Meetings teilzunehmen. Die App ist für Android- und iOS-Betriebssysteme verfügbar. Die App für iOS geriet stark in die Kritik, da Informationen an Facebook weitergegeben worden sind, ohne dass der Nutzer darüber in Kenntnis gesetzt worden ist. Da die App auch über Ende-zu-Ende-Verschlüsselungen kommuniziert, sind Informationen von Dritten geschützt.

3. Browser

Der Browser bietet dem Nutzer die Möglichkeit, ohne die Installation weiterer Software an Zoom-Meetings teilzunehmen. Dabei sind die Konfigurationsmöglichkeiten des Nutzers gegenüber den Client- und App-Versionen etwas eingeschränkt. Sofern die Nutzer nicht auf Links klicken oder sich in nicht vertrauenswürdigen IT-Infrastrukturen bewegen, bietet die Anwendung im Browser eine hohe Sicherheit, da diese keinen direkten Zugriff auf das System des Nutzers ermöglicht. Auch die Kommunikation über den Browser ist Ende-zu-Ende-Verschlüsselt.

SICHERHEITSUPDATES

Am 27. April 2020 veröffentlichte Zoom die Version 5.0. In dieser Version sind alle soweit bekannten Schwachstellen behoben worden, und es wurden enorme Verbesserungen an der Verschlüsselung vorgenommen.[10] Die Sicherheitsrichtlinien von Zoom sind an die Cloud-Sicherheitsrichtlinien des National Cyber Security Centre (NCSC) angelehnt und können in einem externen Dokument eingesehen werden. Das Ziel der NCSC-Cloud-Sicherheitsrichtlinien ist unter anderen der Schutz der Daten von Nutzern sowie der Zugriff auf das Zoom-System. Ebenfalls wird der Umgang mit Schwachstellen und sicherheitsrelevanten Vorfällen klar definiert.[11]

Seit der Version 5.0 werden Daten auch tatsächlich mittels AES 256-Bit verschlüsselt und zwar im Galois/Counter Mode (GCM) . Der GCM ist der neuste und fortschrittlichste Betriebsmodus und bietet einen authentifizierten Verschlüsselungsmodus mit assoziierten Daten.[12] Das Verfahren ist seit 2007 im NIST-Standard 800-38D spezifiziert. Seit dem 30. Mai 2020 verwenden alle Nutzer des Zoom-Clients die Version 5.0 oder höher. Clients mit niedrigeren Versionen sind nicht mehr der Lage, an Meetings teilzunehmen. Dadurch ist die Verschlüsselung für alle Clients garantiert. Ursprünglich war geplant,

eine Ende-zu-Ende-Verschlüsselung (E2EE) nur zahlenden Nutzern zur Verfügung zu stellen. Nach massiven Anwenderprotesten arbeitet das Unternehmen an einer Lösung, sie zeitnah auch Nutzern der freien Version anzubieten. Allerdings will Zoom dafür eine Verifikation des Accounts per Handy.[13] Außerdem können Hosts nun beim Planen eines Meetings auswählen, über welches Rechenzentrum der Zoom-Dienst umgesetzt und der Datenverkehr laufen soll, zum Beispiel ein US- oder EU-Rechenzentrum. Diese Information kann im Client-Fenster eingesehen werden.

EMPFEHLUNGEN FÜR DEN SICHEREN UMGANG MIT ZOOM

Um Zoom weiterhin verwenden zu können und die maximale IT-Sicherheit zu gewährleisten, sind einige Konfigurationen notwendig. Dabei handelt es sich größtenteils um Einstellungen, die bereits vor dem Erstellen eines Meetings durch die verantwortlichen Administratoren umgesetzt werden. Allerdings sind auch während eines Meetings diverse Einstellung zu beachten. Diese werden im folgenden Abschnitt genauer erläutert. Darüber hinaus bietet Zoom eine Zwei-Faktor-Authentifizierung an, die einen zusätzlichen Sicherheitsfaktor für den Schutz des Zoom-Accounts darstellt. Für die Verwendung des Browsers können zusätzliche kostenlose Add-ons installiert werden, die den Nutzer vor unerwünschtem Verhalten schützen. Zusätzlich sollten allgemeine Sicherheitshinweise für den Umgang mit Videoplattformen beachtet werden.

Pre-Meeting-Einstellungen

Pre-Meeting-Einstellungen sind Sicherheitseinstellungen, die bereits beim Erstellen des Meetings durch den Host oder den Administrator vorgenommen werden müssen. Eine von Zoom empfohlene Einstellung ist die Nutzung von Warteräumen. Startet ein Teilnehmer den Zugang zum Meeting, gelangt er erst einmal in einen Warteraum. Der Host des Meetings holt dann jedem Teilnehmer aus dem Warteraum zum Meeting. Somit ist es für Unbefugte nicht mehr möglich, einem Meeting beizutreten, außer der Host lässt ihn rein. Darüber hinaus sollte ein Meeting immer mit einem Passwort versehen werden. Dabei kann entweder das von Zoom generierte Passwort oder ein Individuelles verwendet werden. Das Passwort sollte durch eine aktive Eingabe der Teilnehmer abgefragt werden und nicht bereits im Einladungslink enthalten sein. Durch die manuelle Eingabe des Passworts wird weiterhin festgestellt, dass der Teilnehmer berechtigt ist, an dem Meeting teilzunehmen. Da Meetings nur authentifizierten Nutzern zugänglich gemacht werden sollten, kann so ein Missbrauch des Einladungslinks mit Passwort vorgebeugt werden. Diese Einstellungen können auch global vom Administrator der Zoom-Instanz vorgegeben werden.[14]

In-Meeting-Einstellungen

Während eines Meetings können vom Host weitere Einstellungen vorgenommen werden, diese werden In-Meeting-Einstellung genannt. Seit der Version 4.6.10 verfügt Zoom über ein Security-Icon in der Toolbar des Hosts. Dem Host ist es möglich, ein Meeting zu schließen, sodass keine neuen Teilnehmer dem Meeting beitreten können. Dadurch kann der unbefugte Beitritt in ein Meeting auch nachträglich unterbunden werden. Ebenfalls ist es möglich, die Video- und Audioverbindung einzelner Teilnehmer zu unterbinden. Der Host kann Teilnehmer aus dem Meeting entfernen und bei Verstößen einen Nutzer dem Zoom Trust & Safety Team melden. Zusätzlich kann der Host den Dateitransfer über den Chat sowie die Whiteboard-Funktion für geteilte Bildschirme sperren. Dies stellt einen enormen Sicherheitsgewinn dar, da somit die Verteilung von möglicherweise schadhafter Software unterbunden wird. Außerdem lässt sich das Teilen eines Bildschirms sowie das Aufnehmen von Meetings durch Teilnehmer vom Host deaktivieren. Somit sichert sich der Verantwortliche des Meetings in Hinblick auf den Datenschutz rechtlich ab. Das Ändern der ID von Teilnehmern kann ebenfalls vom Host unterbunden werden. Auch während eines bereits laufenden Meetings kann der Warteraum aktiviert werden. Ist bei einem Meeting auch die Teilnahme per Telefon zugelassen, ist zuvor die entsprechende Telefonnummer zu checken.[14]

WEITERE SICHERHEITSHINWEISE

Zwei-Faktor-Authentifizierung

Zoom stellt seit kurzem die Möglichkeit zur Zwei-Faktor-Authentifizierung bereit. Dadurch können Konten von Nutzern und Administratoren geschützt werden. Die Authentifizierung kann mittels einer App von Google, Microsoft oder FreeOTP durchgeführt werden.

Verwendung im Browser

Für die Nutzung von Zoom im Browser wird ein Werkzeug zum Blockieren von Trackern, kostenlos erhältlich von Antivirus-Herstellern, sowie ein Add-on für den Schutz von persönlichen Daten (beispielsweise Privacy Badger) empfohlen. Weiterhin sollten Teilnehmer nicht auf Links klicken, die nicht vertrauenswürdig sind.

BEWERTUNG VON VIDEOKONFERENZ-SYSTEMEN

Wichtig für die Bewertung der Sicherheit und Vertrauenswürdigkeit von Videokonferenz-Systemen sind unter anderen die angebotenen Sicherheitsfunktionen der Videoplattformen. Gerade die Verschlüsselung, die für den Datenverkehr verwendet wird, ist ein entscheidendes Kriterium. Zur Verschlüsselung sollte eine Ende-zu-Ende-Verschlüsselung verwendet werden. Dazu sollte mindestens ein Verschlüsselungsverfahren AES-128, besser noch AES-256, eingesetzt werden. Außerdem sollte der Videoplattformanbieter in Europa niedergelassen sein oder den Datenverkehr über europäische Rechenzentren leiten. Am besten ist eine Videokonferenzlösung, die in der eigenen IT-Infrastruktur betrieben werden kann, um eine hohe Souveränität zu erreichen. Der Vorteil von Open-Source-Lösungen ist eine hohe Unabhängigkeit. Weiteres Kriterium für die Vertrauenswürdigkeit eines Video-Systems ist die Einhaltung der DS-GVO.

Auch Google verzeichnet mit seinem Videokonferenz-System seit Ausbruch der Corona-Pandemie einen deutlichen Zuwachs. Google nutzte die öffentliche Diskussion um Zoom, um eine sichere Grundkonfiguration für sein Meet (ehemals Hangout) aufbauen. Beispielsweise können Hosts jetzt standardmäßig kontrollieren, welche Teilnehmer in einem Meeting erlaubt sind.

Microsoft Teams ist als Teil von Office 365 oder als Einzellösung erhältlich. Für die private Nutzung ist es kostenlos, allerdings muss ein Account bei Microsoft verknüpft werden. Im April dieses Jahres machte Teams durch eine Schwachstelle auf sich aufmerksam, bei der es den Angreifern möglich war, den Account ihres Opfers zu übernehmen.[15] Die Schwachstelle wurde bereits behoben. Im Office-365-

Enterprise-Paket bietet Teams eine Handvoll Sicherheitseinstellungen – unter anderem eine teamübergreifende und organisationsweite zweistufige Authentifizierung. Ebenfalls integrierte Microsoft einen erweiterten Bedrohungsschutz (Advanced Threat Protection, ATP), um Anwendungen zu überprüfen und Zugriffe blockieren zu können. Die Datenschutzrichtlinien in Teams sind identisch mit denen aus Office 365.

Der Vorteil von Open-Source-Videokonferenz-Systemen liegt ganz klar in der souveränen Nutzung und Verfügbarkeit. Ein Beispiel ist das Videokonferenz-Systemen Jitsi Meet. Jitsi Meet bietet Videokonferenzen über einen Webbrowser oder über eine App für Android und iOS an. Die Funktionen und die Übertragungsqualität können sich sehen lassen. Die maximale Anzahl an Meeting-Teilnehmern ist allerdings deutlicher geringer als bei Zoom. An einem Jitsi Meeting können maximal 75 Personen teilnehmen, für eine besser Qualität werden maximal 35 empfohlen. Bei Zoom sind 100 Teilnehmer Standard, erweiterbar auf 1.000 – ohne qualitative Einbußen. Jitsi Meet verfügt über eine Hop-by-hop-Verschlüsselung, in der jede Phase der Videokonferenz verschlüsselt wird.[16]

FAZIT & AUSBLICK

Zoom ist ein einfach zu bedienendes Videokonferenz-Tool. Die Zoom-Lösungen machen es dem Nutzer sehr leicht, sich zurechtzufinden und bieten eine intuitive Bedienbarkeit. Aber gerade am Anfang wurde die IT-Sicherheit stark vernachlässigt und kein „Security by Design" umgesetzt. Durch den enormen wirtschaftlichen und gesellschaftlichen Druck wurde Zoom dazu gezwungen, Schwachstellen ernst zu nehmen und schnellstmöglich zu beheben. Damit Zoom auch nach der Corona-Pandemie erfolgreich bleibt, sind nach IT-Sicherheitsmaßnahmen, wie dem 90-Tage-Plan, aber weitere IT-Sicherheits- und Datenschutzverbesserungen zwingend notwendig. Mit Version 5.0 sind bereits viele Schwachstellen innerhalb der Software behoben worden, auch dem Datenschutz wird bei der Verwendung von Zoom nun Rechnung getragen. Es ist zu erwarten, dass Zoom sich nun weiterhin allen Schwachstellen stellen und diese beheben wird. Eine wünschenswerte Erweiterung von Zoom wäre die Möglichkeit, die Zoom-Technologie in der eigenen IT-Infrastruktur zu betreiben, um eine höhere Souveränität/unabhängigere Verfügbarkeit zu erreichen.

Besonders erwähnenswert ist, dass während der Corona-Pandemie vielseitige und erfolgreiche Veränderungen der Sicherheitsaspekte in Zoom umgesetzt wurden. Aber auch andere Anbieter von Videokonferenz-Systemen partizipieren stark von den in Zoom gefunden Schwachstellen und der damit verbundenen medialen Aufmerksamkeit.

Insgesamt lässt sich feststellen, dass sich bei den Videokonferenz-Systemen sehr viel getan hat und der Datenschutz und die IT-Sicherheit deutlich besser geworden sind. Mit der immer größeren Beliebtheit der Videokonferenz-Systeme sollten die Hersteller allerdings „Privacy and Security by Design" berücksichtigen und einen kontinuierlichen IT-Sicherheitsprozess aufrechterhalten, der bei neuen Schwachstellen unmittelbar Updates zur Verfügung stellen kann. ■

Literatur

[1] *Zoom: https://www.sec.gov/ix?doc=/Archives/edgar/data/1585521/000158552120000095/zm-20200131.htm , 2020*

[2] *Alex Kannenberg: „Zoom korrigiert runter: Nicht 300 Millionen Nutzer, sondern Teilnehmer" , https://heise.de/-4712509, 2020*

[3] *Zoom: https://zoom.us/pricing, 2020*

[4] *Microsoft Pricing: https://www.microsoft.com/de-de/microsoft-365/business?market=de#compareProductsRegion*

[5] *Google: https://apps.google.com/meet/pricing/,2020*

[6] *Bruce Schneier: „Security and Privacy Implications of Zoom", https://www.schneier.com/blog/archives/2020/04/security_and_pr_1.html, 2020*

[7] *Lorenz Franceschi-Bicchierai: „Hackers Are Selling a Critical Zoom Zero-Day Exploit for $500,000", https://www.vice.com/en_us/article/qjdqgv/hackers-selling-critical-zoom-zero-day-exploit-for-500000, 2020*

[8] *Max Hoppenstedt: „Polizei ermittelt wegen Kinderpornografie in Videokonferenzen", https://www.spiegel.de/netzwelt/web/zoombombing-polizei-ermittelt-wegen-kinderpornografie-in-zoom-videokonferenzen-a-a51c49f3-40b3-4614-a347-d071f8b4089f, 2020*

[9] *Zoom Privacy Policy https://zoom.us/privacy, 2020*

[10] *Zoom 5.0 https://zoom.us/docs/de-de/zoom-v5-0.html, 2020*

[11] *Zoom: „Zoom Video Communications Cloud Security Principles", https://zoom.us/docs/doc/NCSC-Cloud-Security-Principles-Zoom-%282005%29.pdf, 2020*

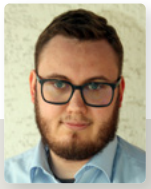
[12] *N. Pohlmann: „Cybersicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cybersicherheitssystemen in der Digitalisierung", Springer-Vieweg Verlag, Wiesbaden 2019*

[13] *Dirk Srocke, Peter Schmitz: "E2E-Verschlüsselung für alle Zoom-Nutzer", https://www.security-insider.de/e2e-verschluesselung-fuer-alle-zoom-nutzer-a-942802/?cmp=nl-36&uuid=A74996FA-CB6C-4565-8D3EB1C2810899A5, 2020*

[14] *Zoom Privacy & Security for Zoom Video Communications, https://zoom.us/docs/en-us/privacy-and-security.html?zcid=3797&creative=437995777397&keyword=zoom%20security&matchtype=e&network=g&device=m&gclid=Cj0KCQjwz4z3BRCgARIsAES_OVfhWlXwBrGFhr4lGOjSDGuS8wuiF2-MCH5t6zDO_JGspitYS3knNBoaAjbKEALw_wcB, 2020*

[15] *Omer Tsarfati: „Beware oft he GIF: Account Takeover Vulnerability in Microsoft Teams", https://www.cyberark.com/resources/threat-research-blog/beware-of-the-gif-account-takeover-vulnerability-in-microsoft-teams , 2020*

[16] *Gavin Phillips: „What Is Jitsi and Is it More Secure Than Zoom?", https://www.makeuseof.com/tag/jitsi-secure-zoom/#:~:text=It%20means%20that%20the%20server,eavesdropping%20on%20private%20video%20conversations, 2020*



CHRISTIAN BÖTTGER
studiert im Master Internet-Sicherheit an der Westfälischen Hochschule Gelsenkirchen und beschäftigt sich im Rahmen des Studiums mit der Bewertung von Video-Systemen.

NORBERT POHLMANN
ist Professor für Informationssicherheit und Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen sowie Vorstandsvorsitzender des Bundesverbands IT-Sicherheit – TeleTrusT und im Vorstand des Internetverbandes – eco.