28. April 2020 (v3)

Datenschutzkonformer Einsatz von Zoom bei adelphi

Von: Daniel Högele – Head of IT, adelphi

An: alle adelphis und deren Partner / Auftraggeber

Liebe KollegInnen, PartnerInnen und AuftraggeberInnen,

von vielen Seiten bekomme adelphi **besorgte Anfragen**, ob der **Einsatz von Zoom datenschutzrechtlich überhaupt zulässig** ist. Zoom wird derzeit in den Medien (z.B. Financial Times, Computerbild) kontrovers diskutiert und teilweise als totalen „Datenschutzskandal“ gebrandmarkt. Wir finde solche öffentlichen Diskussionen gut, da Sie i.d.R. dazu führen, dass die betroffenen Unternehmen schnell reagieren. Jedoch sollten mediale Aussagen eingehend geprüft werden, bevor sich ein Unternehmen dazu entschließt, seine Compliance anzupassen.

adelphi beobachtet daher die Entwicklungen seit Wochen sehr genau und will mit diesem Statement etwas Licht in den Dschungel bringen und mit dem nötigen Sachverstand über die Umstände und getroffenen Maßnahmen bei adelphi informieren.

Was genau ist überhaupt passiert?

Sobald eine Lösung populär wird, gelangt sie zunehmend in den Fokus von Datenschützern, Sicherheitsexperten und Hackern. Somit ist es überhaupt nicht verwunderlich, dass irgendwann auch „Probleme“ in Zoom gefunden wurden.

Der Zoom CEO hat hierzu umfassend Stellung bezogen und die Kritikpunkte wurden immer extrem schnell und vorbildlich durch Anpassungen am System oder Guidelines für sichere Einstellungen aus der Welt geschafft. Zudem wurden wöchentliche Webinare mit dem Zoom CEO ins Leben gerufen, wo Sicherheitsfragen für jeden öffentlich und transparent erörtert werden. Auch eine kontinuierlich aktualisierte Roadmap für Sicherheitsverbesserungen wurde veröffentlicht. Schlussendlich wurde ein namhafter Ex-Facebook Sicherheitsexperte ins Team geholt und ein Bug-Bounty Programm in Leben gerufen.

Wie man an der nachfolgenden Aufstellung sehen kann, hat Zoom vorbildlich und sehr transparent reagiert und alle Probleme innerhalb kürzester Zeit adressiert und gelöst. Ein Vorgehen, wie es bisher bei keinen anderen uns bekannten IT-Lösungsanbieter der Fall war.

Von den 11 zuletzt in der Presse heiß diskutierten Vorfällen waren 3 Fälle echte Sicherheitslücken (mac Client, Windows Client, Warteraum), je nach Auslegung 3-5 Datenschutzpannen (Facebook, LinkedIn, China-RZ, Datenschutzerklärung? Aussage zu Verschlüsselung?) und der Rest resultierte schlicht aus einer schlechten Organisation der Meetings durch Nutzer / Administratoren.

Die Fälle im Einzelnen in chronologischer Folge:

Datenschutzrechtlich bedenkliche Überwachung der Aufmerksamkeit der Meeting Teilnehmer (Es handelt sich hierbei um keinen „Fehler“ sondern eine gewollte Funktion, die man schon immer selber EIN/AUS schalten konnte.)
Berichtet am 16.3. https://www.vice.com/en_us/article/qjdnmm/working-from-home-zoom-tells-your-boss-if-youre-not-paying-attention
Funktion entfernt am 1.4. https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

Unzureichende Datenschutzerklärung hinsichtlich Informationen zur Sammlung und Weitergabe von Daten
Beanstandet am 20.3. https://securityboulevard.com/2020/03/using-zoom-here-are-the-privacy-issues-you-need-to-be-aware-of/
Gefixt am 29.3. https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

Zoombombing: Unerwünschte Teilnehmer stören Meetings (kein Fehler sondern zu laxe Zugriffseinstellungen durch die Organisatoren / Administratoren oder öffentliches Teilen der Meeting IDs durch unbedarfte Anwender. Meetings lassen sich schon immer durch ein Passwort schützen und der Beitritt der Teilnehmer selektiv genehmigen)
Berichtet am 20.3.: https://www.nytimes.com/2020/03/20/style/zoombombing-zoom-trolling.html
Am selben Tag wurden bereits Guidelines veröffentlicht:
https://blog.zoom.us/wordpress/2020/03/20/keep-uninvited-guests-out-of-your-zoom-event/
Bis zum heutigen Tage wurden zudem zahlreiche Systemanpassungen vorgenommen, unter anderem wurde die Meeting ID im Fenster versteckt und auf 11 Ziffern verlängert, ein Schnellzugriffs auf Sicherheitseinstellungen eingeführt, Passworte für Webmeetings und Aufnahmen standardmäßig aktiviert https://blog.zoom.us/wordpress/2020/04/14/enhanced-password-capabilities-for-zoom-meetings-webinars-cloud-recordings/ , Administratoren eine Übersicht zu ungeschützten Meetings bereitgestellt, eine Meldefunktion für unerwünschte Benutzer eingeführt uvm.

Versteckte Übermittlung von iOS Gerätedaten an Facebook (betraf nur apple User)
Aufgedeckt am 26.3. https://www.vice.com/en_us/article/k7e599/zoom-ios-app-sends-data-to-facebook-even-if-you-dont-have-a-facebook-account
Einen Tag später bereits gefixt https://blog.zoom.us/wordpress/2020/03/27/zoom-use-of-facebook-sdk-in-ios-client/

Sicherheitslücken im mac Zoom Client, über die Angreifer erweiterte Rechte und Webcam/Mikrofon Zugriff erlangen könnten (betraf nur apple User)
Aufgedeckt am 30.3. https://objective-see.com/blog/blog_0x56.html
Zwei Tage später bereits gefixt https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

Falsche Angaben zur verwendeten Verschlüsselung (Unschön, aber für Alltagskommunikation nicht tragisch. In vielen Fällen wird TLS verwendet, nur wenn

Telefone, Browser oder H.323 involviert sind, wird es abgeschaltet. Ähnlich machen es die Wettbewerber.)
Aufgedeckt am 31.3. https://theintercept.com/2020/03/31/zoom-meeting-encryption/
Bereits am nächsten Tag gab es eine Stellungnahme:
https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/
Seit dem 27.4. und erscheinen von Version 5 wird AES-256-GCM Verschlüsselung unterstützt. Ab 30. Mai wird es global aktiviert.
https://blog.zoom.us/wordpress/2020/04/27/its-here-5-things-to-know-about-zoom-5-0/

Sicherheitslücke im Chat, die das Ausspähen der Windows-Anmeldeinformationen ermöglichte (betraf nur Windows User)
Aufgedeckt am 1.4. https://www.tomsguide.com/news/zoom-password-malware-flaw
Einen Tag später bereits gefixt https://blog.zoom.us/wordpress/2020/04/01/a-message-to-our-users/

Versteckte Übermittlung von Daten aus LinkedIn Profilen (betraf nur User mit LinkedIn Profil)
Aufgedeckt am 1.4.: https://www.nytimes.com/2020/04/02/technology/zoom-linkedin-data.html
Am selben Tag bereits gefixt https://threatpost.com/zoom-removes-data-mining-linkedin-feature/154404/

Datentransfer erfolgte im Februar unter extrem seltenen Umständen über neue Rechenzentren in China
Aufgedeckt am 3.4. https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/
Am selben Tag Stellung bezogen https://blog.zoom.us/wordpress/2020/04/03/response-to-research-from-university-of-torontos-citizen-lab/
Neue Funktion ab 18.4.: Kontoadministratoren können selber festlegen, welche regionalen Rechenzentren verwendet werden. https://blog.zoom.us/wordpress/2020/04/13/coming-april-18-control-your-zoom-data-routing/
In Version 5 kann man sich nun auch anzeigen lassen, mit welchem Rechenzentrum man verbunden ist.

Öffentlich zugängliche Cloud Recordings (kein Fehler, sondern zu laxe Zugriffseinstellungen durch die Organisatoren / Administratoren. Aufnahmen lassen sich schon immer durch ein Passwort schützen)
Aufgedeckt am 3.4. https://www.washingtonpost.com/technology/2020/04/03/thousands-zoom-video-calls-left-exposed-open-web/
Kein Fix nötig, aber am 10.4. ist die Passworteinstellung standardmäßig aktiviert worden.
https://blog.zoom.us/wordpress/2020/04/14/enhanced-password-capabilities-for-zoom-meetings-webinars-cloud-recordings/

Warteräum könnten von Hackern umgangen werden
Aufgedeckt und gefixt am 8.4. https://citizenlab.ca/2020/04/zooms-waiting-room-vulnerability/

500.000 Logindaten zum Kauf angeboten (Keine Datenpanne bei Zoom. Die Daten wurden vor Ewigkeiten bei LinkedIn gestohlen und die betroffenen und grob fahrlässigen User haben dieselben Logins auch bei Zoom verwendet.)

Berichtet am 13.4. https://www.bleepingcomputer.com/news/security/over-500-000-zoom-accounts-sold-on-hacker-forums-the-dark-web/
Kein Fix nötig.

Warum hält adelphi trotz der „Skandale“ weiterhin an Zoom fest?

Zoom ist derzeit die Lösung mit der besten Userexperience am Markt. Sie ermöglicht eine zuverlässige, hürdenlose und schnelle Teilnahme an Meetings über alle erdenklichen Verbindungswege (Software, Browser, App, Telefon, Raumsystem) hinweg. Zoom trug somit wie keine andere zuvor eingesetzte Lösung zum großen Erfolg der durch adelphi organisierten Besprechungen und Webinare bei und führte zu einer hohen Akzeptanz im Unternehmen und verdrängte schnell alle anderen zuvor eingesetzten Lösungen (Skype, WebEx, GoToMeeting, apper.in, Spreed), die immer wieder Probleme hinsichtlich Usability, Qualität und Zuverlässigkeit an den Tag brachten und somit zu Frust bei adelphi Mitarbeitern und unseren Partnern führten. Niemand möchte die ersten 15 Minuten eines Meetings mit der Lösung technischer Probleme verbringen!

Neben den technischen Vorteilen vernachlässigt adelphi natürlich nicht den Datenschutzaspekt und ist der Meinung, dass sich Zoom hier trotz aller gefundenen Mängel vorbildlich verhält! Alle Probleme wurden äußerst transparent kommuniziert und unmittelbar behoben.

Diese Auffassung teilen mittlerweile auch viele andere IT- und Datenschutzexperten und Anwälte, was dem finalen Kapitel „Stimmen von Datenschützern / Sicherheitsexperten / Universitäten“ entnommen werden kann.

Ist Zoom datenschutzkonform nach DSGVO?

Dieser rechtliche Aspekt basiert auf Regelungen wie der EU-Datenschutzverordnung (DSGVO) oder auch dem Bundesdatenschutzgesetz (BDSG), dem Telemediengesetz (TMG) und diversen anderen Gesetzen. Wenn wir Europäer Dienste einsetzen, die personenbezogene Daten verarbeiten, muss dafür zwischen dem Auftraggnehmer (adelphi) und und dem Anbieter (Zoom) eine rechtliche Grundlage geschaffen werden. Befindet sich der Anbieter in der EU, so muss mit ihm eine Vereinbarung zur Auftragsverarbeitung (AV) abgeschlossen werden. Befindet er sich außerhalb der EU, lassen sich AV oftmals nicht realisieren. Daher reicht es aus, wenn das Datenschutzniveau in dem Land den Anforderungen der DSGVO entspricht. Derzeit gilt das nur für eine Hand voll Staaten. Die USA, wo Zoom und die meisten anderen Cloudlösungen beheimatet sind, gehören NICHT dazu. Aus diesem Grund gibt es zwischen der EU und den USA das Privacy-Shield-

Abkommen. Von allen US-Unternehmen, die sich dort zertifizieren, dürfen Europäer ein für die DSGVO ausreichendes Datenschutzniveau annehmen. So auch bei Zoom.

Wäre das US-Unternehmen nicht auf der Liste, müsste ein Vertrag mit sogenannten EU-Standardklauseln abgeschlossen werden. Auch wenn das bei Zoom wegen des Privacy-Shield nicht nötig ist, hat adelphi dies trotzdem gemacht, da unter der Administration Trump mehrfach Zweifel bestanden, ob das Abkommen noch lange Bestand hat.

Um den Anforderungen der DSGVO, alle verfügbaren technischen und organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes auszuschöpfen gerecht zu werden, hat adelphi einen Absatz zu Zoom in die adelphi.de Datenschutzerklärung (auch EN) sowie Datenschutzhinweise in die Vorlage der Meetingeinladungen, der Zoom-Loginseite https://adelphi.zoom.us sowie bei Cloudrecordings eingefügt.

Mit all diesen Maßnahmen erfolgt der Einsatz von Zoom datenschutzkonform!

Sind andere Lösungen sicherer?

Ein Blick in die Datenbank der Sicherheitsprobleme (CVE - Common Vulnerabilities and Exposures) zeigt, dass natürlich auch die Wettbewerber immer wieder mit Lücken zu kämpfen haben. Das liegt in der Natur der Softwareentwicklung! Ein Rating von 1 bis 10 stellt dabei die Schwere der Lücke dar.

Zoom ist dort derzeit mit 4 Lücken und maximalen Rating von 7.5 erfasst (die aktuellen Lücken sind noch nicht registriert).

Im Vergleich dazu kommen die anderen Systeme deutlich schlechter weg, siehe z.B. WebEx (9 Lücken, davon 7x Rating >9), Adobe Connect (21 Lücken, davon 1x Rating 10), Microsoft Lync (40 Lücken, davon 27x Rating >9), Skype for Business (27 Lücken, davon 16x Rating >9), Skype (6 Lücken, davon 1x Rating 10).

Welche technischen Unzulänglichkeiten hatten wir mit anderen Lösungen?

WebEx: Da bei deutschen Verträgen nur zwei Einwahlnummern existieren (DE+UK) welche zudem oftmals überlastet waren, ist die Lösung für global operierende Unternehmen, bei denen manche Partner auf Telefoneinwahl angewiesen sind, nicht sinnvoll einsetzbar. Abgehende Telefonate waren nicht möglich. Auch die browserbasierten Verbindungen sind immer wieder unvermittelt zusammengebrochen und oftmals erst nach dem Neustart des Computers wieder mit Audio nutzbar gewesen. Zudem gibt es keine H.323 Unterstützung für professionelle Raumsysteme. Bei manchen Browsern war die Installation von Plugins mit administrativen Rechten nötig. Die Teilnahmemöglichkeit via „temporary Application“ war zu sehr versteckt.

GoToMeeting: Die wenigen internationalen Telefoneinwahlpunkte passten nicht zu den Regionen, in denen adelphi tätig ist. Das System unterstützt keine reinen Telefonkonferenzen und kein H.323 für Raumsysteme. Die Usability war ungenügend, so hatten Teilnehmer oft Probleme Ihr Computeraudio zu aktivieren.

Lync, Skype-for-Business: Unsere Partner setzten z.T. unterschiedliche Versionen ein, deren Browserplugns nicht zueinander kompatibel waren. Das ständige Austauschen der Plugins führte immer wieder zu Schwierigkeiten und daraus resultierendem erhöhtem Supportaufwand. Die enge Verzahnung mit der Microsoft Cloud auf Betriebssystemebene passt zudem nicht zu den Complianceansprüchen von Unternehmen mit hohen Datenschutzstandards. Selbiges gilt auch für den Nachfolger **Microsoft Teams.**

Adobe Connect: Sehr schlechte Usability und komplizierte Integration von reiner Telefonie (nativ nichtg gegeben, 3rd Party nötig)

Selbst gehostete Lösungen (Jitsi, Apache OC Server): Die Bereitstellung einer Videokonferenzinfrastruktur für ein global operierendes Unternehmen erfordert weltweit verteilte Rechenzentren mit optimierten Providerpeerings. Eine lokal in Deutschland installierte Instanz wird z.B. aus Indien heraus nicht ausreichend performant nutzbar sein. Zudem würden damit auch international verfügbare Telefoneinwahlpunkte fehlen. Auch werden H.323 Raumsysteme nicht unterstützt. Für eine firmeninterne Kommunikation mag es eine aus Datenschutzsicht sinnvolle Variante sein, für den globalen Einsatz in Projekten ist es aber ungeeignet.

Pexip: Keine eigenen Erfahrungen, aber aus verschiedensten Quellen haben wir erfahren, dass es beim DFN damit immer wieder Auslastungsprobleme gibt.

Was tut adelphi zur Einhaltung des Datenschutzes bei Zoom?

adelphi überwacht neben Zoom auch zu allen anderen eingesetzten IT-Lösungen täglich die aus verschiedensten Quellen eingehenden Sicherheitsmeldungen.

Daraus resultierende Sicherheitsupdates werden über ein zentrales Deployment zeitnah auf allen Systemen eingespielt.

Alle Lösungen werden hinsichtlich der Einhaltung der DSGVO überprüft, Vereinbarungen zur Auftragsverarbeitung abgeschlossen und zentrale Einstellungen anhand von Best-Practices so datenschutzkonform wie möglich vorgegeben.

Regelmäßige Trainings und Handreichungen schulen die Mitarbeiter zum sicheren Umgang speziell mit Zoom aber auch anderen IT-Lösungen.

Teilnehmer an Zoom Meetings werden in der E-Mail-Einladung auf den Zoom-Abschnitt unsere Datenschutzerklärung hingewiesen.

Stimmen von Datenschützern / Sicherheitsexperten / Universitäten

Tom Lukaß - Senior Berater Datenschutz/ Teamleiter Akademie Datenschutz nord

„Nach dem was für uns sichtbar ist, können wir Zoom ein solides Datenschutzniveau attestieren. Die richtigen Einstellungen und Verträge vorausgesetzt, sollte einem datenschutzkonformen Einsatz der Lösung nichts im Wege stehen. Positiv fällt zudem auf, dass der Anbieter berechtigte Kritik ernst zu nehmen scheint und zügig nachbessert."

https://www.datenschutz-notizen.de/videochats-datenschutz-heute-zoom-4325330/

Stephan Hansen-Oest - Rechtsanwalt & Fachanwalt für IT-Recht.

„Gegen die Nutzung von „Zoom" für Webinare, E-Learning und ähnliche Angebote gibt es aus rechtlicher Sicht jetzt schon keine grundlegenden Bedenken. Alle kritischen Ausführungen dazu ließen sich bei näherem Hinschauen meinerseits widerlegen bzw. wurden nicht substantiiert belegt. Es scheint also aktuell eher ein „Gefühl" zu sein, „Zoom" nicht nutzen zu können bzw. zu wollen. Dieses Gefühl steht jedem zu. Niemand muss „Zoom" nutzen. Allerdings meine ich schon, dass ein Einsatz von „Zoom" immer noch rechtlich und auch technisch vertretbar ist. Für einige alternative Anbieter kann ich das leider nicht sagen."

https://www.datenschutz-guru.de/zoom-ist-keine-datenschleuder

David Kennedy - founder TrustedSec, Binary Defense

„Zoom is not malware. Zoom is safe to use for both you personally and businesses, but you should read through on how to best protect yourself and your company."

https://medium.com/@0xamit/zoom-isnt-malware-ae01618e2046

Ashley Boyd - Vice President, Advocacy & Engagement at Mozilla Foundation

"Zoom has been criticized for privacy and security flaws. Because there are many other video call app options out there, Zoom acted quickly to address concerns. This isn't something we necessarily see with companies like Facebook, which don't have a true competitor"

https://blog.mozilla.org/blog/2020/04/28/which-video-call-apps-can-you-trust/

„Full disclosure, here at Mozilla we use Zoom and have worked closely with the company to get its privacy and security features right for us. (Overall Security Rating: 5/5)"
https://foundation.mozilla.org/en/privacynotincluded/products/zoom/

Prof. Dr. Andreas Breiter - Chief Digital Officer Universität Bremen

„In der aktuellen Situation hat sich die Universität Bremen nach intensiven Beratungen und Abwägungen von Funktionalität und Datenschutz für eine Campus-Lizenz von Zoom entschieden.

Wir basieren diese Entscheidung auf Empfehlungen externer Gutachter und auch des Bundesamts für Sicherheit in der Informationstechnik (BSI). Aus deren Sicht gibt es bei der Nutzung des zoom Video-Kommunikations-Services keine grundsätzlichen datenschutzrechtlichen Bedenken.

Wir haben andere Alternativen evaluiert und sie werden entweder ausdrücklich von der Landesbeauftragten für Datenschutz und Informationsfreiheit nicht empfohlen (Teams und Office365), oder für große Gruppen und virtuelle Lern-/Lehr-Szenarien ungeeignet. Leider sind auch die Dienste des DFN-Vereins aufgrund der Kapazitätsengpässe für Lehrveranstaltungen nicht sicher nutzbar.

Ich hoffe, dass erklärt unsere Entscheidung. Wesentlich besser wäre eine deutschland- oder europaweite sichere Cloud-Lösung. Die ist aber derzeit nicht vorhanden.“

https://www.uni-bremen.de/coronavirus/#collapse-258487

Computer und Medienservice Humboldt-Universität zu Berlin

„Wir haben im CMS schon seit drei Jahren Zoom als Ergänzung der Videokonferenz-Angebote des DFN evaluiert und zu Testzwecken eingesetzt. Dabei hat es sich als eine sehr verlässliche Lösung mit hoher Konferenzqualität gezeigt. Darüber hinaus haben wir viele andere Lösungen wie WebEx, Skype for Business oder Lifesize evaluiert und getestet. Abwägungen wie Funktionalität, Stabilität, Sicherheit und Datenschutz wurden bei der Entscheidung für Zoom berücksichtigt. [..]

Wir konnten bisher feststellen, dass Zoom sehr schnell auf Anfragen reagiert und auch entsprechende technische Lösungen bereitgestellt hat.

Nach dem derzeitigen Stand sind wir zuversichtlich, dass alle bisher diskutierten Sicherheitsfragen für HU-Zoom aufgelöst werden können. Für alle hier aufgeführten Diskussionen konnten bereits Fixes umgesetzt werden.“

https://www.cms.hu-berlin.de/de/dl/multimedia/bereiche/tele/zoom/sicherheit