Warum nicht Zoom?

„Trotzdem ist offensichtlich: Bei Zoom hat es Sicherheitsprobleme gegeben. Und es hat Schwierigkeiten gegeben, den Zugang zu vertraulichen Gesprächen abzusichern. Derzeit gibt es keine Ende-zu-Ende-Verschlüsselung. Das heißt: Die Inhalte der Kommunikation liegen unverschlüsselt auf dem Server des Anbieters. *Damit ist von dieser Kommunikationsform abzuraten*, wenn personenbezogene Daten im Spiel sind. Es sollten dann alternative Plattformen gewählt werden, wo eine echte Ende-zu-Ende-Verschlüsselung garantiert ist.“

Ulrich Kelber

Bundesbeauftragter für den Datenschutz

[Interview im Handelsblatt am 24. Mai 2020]

Standpunkt

Zum Thema zoom findet sich viel Begeisterung, da die Übertragungen regelmäßig störungsfrei laufen. Und so kursiert auch der Beitrag des „Datenschutz-Guru“, wonach zoom „die beste Mischung aus Qualität, Leistungsumfang, Preis und auch Datenschutzfreundlichkeit. Das mag bei einem US-Anbieter komisch klingen. Für mich ist das aber so.“[1]

Der Autor kommt gleich mit der ersten Einschränkung, die aufhorchen lässt - das „Aufmerksamkeittracking“. Der Moderator bekommt angezeigt, wenn einer der Beteiligten seinen Fokus nicht mehr auf dem zoom-App hat, sprich beispielsweise er oder sie eine E-Mail schreibt. Diese Funktion mag abschaltbar sein, aber will man Software benutzen, die solche Funktionen einbaut?

Hinter dem Datenschutz-Guru steht ein Rechtsanwalt, welcher die „Datenschutzfreundlichkeit“ von zoom lobt. Diese wird mit dem EU-U.S. Privacy Shield und Art. 6 Abs. 1 lit. b) DSGVO begründet. Nicht erst durch Snowden, sondern bereits seit dem Patriot Act muss man die Augen schon fest verschließen, um die Vorteile des Produkts noch zu loben. Da bedarf es noch keines Blicks in die aktuelle amerikanische Politik. Man mag jetzt denken, dass an diesen Daten die USA kein Interesse haben können. Dass dem nicht so ist, verraten die Nutzungsbedingungen: „Weiterhin verpflichten Sie sich, keine materielle Unterstützung oder Ressourcen (oder die Art, den Ort, die Quelle oder das Eigentum an materieller Unterstützung oder Ressourcen nicht zu verschleiern oder zu verbergen) an Organisationen zu liefern, die von der Regierung der Vereinigten Staaten von Amerika als ausländische Terrororganisation gemäß Absatz 219 des Immigration and Nationality Act„ eingestuft werden.“ Eine solche Verpflichtung macht nur Sinn, wenn deren Einhaltung auch geprüft wird. Die Nutzungsbedingungen halten aber noch ein weiteres Bonbon bereit: „Durch Anmelden geben Sie Zoom Ihr Einverständnis zur Speicherung der Aufzeichnungen für ein oder alle Zoom Meetings oder Webinare, an dem (denen) Sie teilgenommen haben.“ In diesem Fall soll man benachrichtigt werden, aber auch das setzt wieder Vertrauen in zoom voraus.[2]

Wer mit zoom einen Vertrag schließt, gibt seine Einwilligung, dass zoom seine/ihre Daten im Bedarfsfalle - den zoom definiert - auch an ein paar Unternehmen weiterreicht[3]: im Bereich des Vertriebs an People.ai (USA); für „Erfolg und Unterstützung“ an Zendesk (USA), Wootric (USA), Totango (USA), Answerforce (USA), Rocket Science Group LLC (USA), Five9 (USA), EPS Ventures (Malaysia), WKJ Consultancy (Malaysia); für „Beziehungsmanagement“ Salesforce (USA);

„Abrechnung“ CyberSource (USA), Adyen (Europa, scheinbar ist das aus Sicht zooms ein Land), Zuora (USA); „Infrastruktur“ Amazon Web Services (USA, EU, Kanada, Australien) und Bandwidth (USA). Die Frage, ob diese Unternehmens vertrauenswürdig sind, wird nicht extern, sondern von zoom selbst beurteilt.

Die Einbingung einer amazon cloud lässt Menschen wie den „Datenschutz-Guru“ ruhig schlafen, denn: „In rein datenschutzrechtlicher Hinsicht ist gegen einen Einsatz von AWS grundsätzlich nichts einzuwenden. Es gibt manchmal Bereiche, in denen ein AWS ggf. problematisch sein könnte. Dies lässt sich dann aber durch eine Verwendung eigener Verschlüsselungsebenen ggf. beheben.“[4] Ob das bei amazon wirklich so der Fall ist, will ich hier jetzt gar nicht vertiefen.[5] Ob zoom diese Verschlüsselungsebene einzieht, ist weder bekannt, mindestens aber nicht nachprüfbar - es handelt sich schließlich um keine offene Software. Aber sind das wirklich alle Unternehmen, an die Daten ausgereicht werden? Nein! Wer sich etwas weiter auf Seiten umschaut, findet in einem der Dokumente, dass auch Google Ads und Google Analytics ausgereicht werden.[6][7] Falls man dazu Fragen hat, wird man im gleichen Dokument auf den „Data Privacy Officer“ in San Jose, Kalifornien verwiesen. Aber das Dokument hilft schon an einer entscheidenden Stelle bei der Frage weiter, wie Google mit sensiblen Daten umgeht: „Beispielsweise können diese Daten von Google dazu genutzt werden, um ihre Werbedienste für sämtliche Unternehmen zu verbessern, die Google-Dienste verwenden.“

Was passiert eigentlich, wenn was mit den Daten schief läuft? „Unter keinen Umständen haftet Zoom in irgendeiner Weise für Daten oder andere Inhalte, die während der Nutzung der Dienste angezeigt werden, einschließlich, aber nicht beschränkt auf, Fehler oder Auslassungen in solchen Daten oder Inhalten oder Verluste oder Schäden irgendeiner Art, die sich aus der Nutzung von, dem Zugang zu oder der Verweigerung des Zugangs zu Daten oder Inhalten ergeben. Sollten Sie zu irgendeinem Zeitpunkt mit den Diensten nicht zufrieden sein, besteht Ihr einziger Rechtsbehelf darin, die Nutzung der Dienste einzustellen.“[8]

Falls der Fall der Fälle eintritt, helfen bestimmt die Gerichte… dazu die Nutzungsbedingungen: „Diese Vereinbarung unterliegt den Gesetzen des Bundesstaates Kalifornien, Vereinigte Staaten von Amerika, und wird nach diesen Gesetzen ausgelegt, insoweit diese Gesetze auf Vereinbarungen angewendet werden, die innerhalb von Kalifornien zwischen Einwohnern von Kalifornien geschlossen werden. Die Parteien erklären sich damit einverstanden, dass die ausschließliche Zuständigkeit und Gerichtsbarkeit bei den zuständigen Landesgerichten in Santa Clara County, Kalifornien, und den Bundesgerichten im Northern District of California liegt.“ Wer Zoom einsetzt, bedarf eines Rechtsanwalt mit einer Zulassung für den Staat Kalifornien.

Werfen wir einen Blick auf die Datenschutzrichtlinien von Zoom [9]: „Unter bestimmten Umständen können Sie wählen, ob Sie personenbezogene Daten an Zoom bereitstellen.“ Welche Umstände das sind und was passiert, wenn man nicht wählen kann, bleibt verborgen. Was gesammelt wird, wird in verschiedenen Kategorien aufgeteilt. Interessant ist der Punkt „Andere Informationen, die Sie während der Nutzung des Service („Kundeninhalte“) hochladen, bereitstellen oder erstellen, wie im Abschnitt „Kundeninhalte“ ausführlicher beschrieben.“ Dieser Abschnitt ist aufschlussreich: „Kundeninhalte sind Informationen, die vom Kunden durch die Nutzung des Dienstes an Zoom zur Verfügung gestellt werden. Kundeninhalte umfassen die Inhalte, die in Cloud-Aufzeichnungen und Instant Messages, Dateien und Whiteboards enthalten sind und während der Nutzung des Dienstes freigegeben werden.“ Wer glaubt, dass irgendwelche Daten von zoom nicht gesammelt werden, sollte hier geheilt sein. Aber was macht Zoom jetzt eigentlich mit den Daten? Das verraten sie etwas weiter unten: „Wir können Identifikatoren, Beschäftigungsinformationen, Zahlungsinformationen, Facebook-Profilinformationen, technische Informationen, demografische Informationen, Nutzungsinformationen und benutzergenerierte Informationen verwenden, um: […] - Zustimmungswettbewerbe, Gewinnspiele und anderen Marketing- oder Werbeaktivitäten auf den Zoom.us-Websites oder

Websites von Tochtergesellschaften bereitzustellen und zu organisieren - Informationen und Angebote von uns oder Dritten für Sie bereitzustellen […]“

Man könnte meinen, dass dies nur für zoom-eigene Zwecke erfolgt. Dem ist aber nicht so: „Verkauft Zoom personenbezogene Daten? Das hängt von Ihrer Definition von „verkaufen“ ab. Wir gestatten es weder Marketingfirmen, Werbetreibenden noch anderen Personen, gegen Bezahlung auf personenbezogene Daten zuzugreifen.“

Die Frage beantwortet sich also nach der zoom-eigenen Definition von Verkaufen. Zugutehalten muss man an dieser Stelle, dass es nach dem Dokument wohl den Verkauf ausschließen kann: „Sie können beantragen, dass Sie von bestimmten Werbepraktiken im Zusammenhang mit Ihren persönlichen Daten ausgeschlossen werden, indem Sie auf den Link „Meine personenbezogenen Daten nicht ‚verkaufen‘“ klicken.“ Wo dieser Button ist, weiß ich nicht. Ich habe keinen Account geklickt, sondern bis jetzt nur zusammengefasst, was ich auf den ersten Blick gesehen habe. Um nochmal auf den Anfang zurückzukommen - der Kollege hat ja darauf verwiesen, dass hier DSGVO gelte. Da ist Zoom wohl selbst nicht so sicher: „Wenn Sie Ihren Wohnsitz in der Europäischen Union („EU“), im Vereinigten Königreich, in Liechtenstein, Norwegen, Island oder der Schweiz haben, können Sie möglicherweise zusätzliche Rechte hinsichtlich Ihrer personenbezogenen Daten in Anspruch nehmen, einschließlich derjenigen, die in der Datenschutz-Grundverordnung (DSGVO) der EU dargelegt sind.“ Mir jedenfalls reicht es nicht, „möglicherweise zusätzliche Rechte“ zu haben.

Gibt es zusammenfassend Anlass für Misstrauen? Die englischsprachige Wikipedia hat dies kurz zusammen gefasst. Im Übrigen mag die unten anstehende Linkliste weiterhelfen. Hier kann sich jeder sein eigenes Urteil bilden. Bei dieser Urteilsbildung möge bitte mitbedacht werden, dass andere Produkte zeigen, dass andere Wege machbar sind. Dort fehlen nur die großen Werbetafeln.

Nachtrag: Wer glaubt, die Verschlüsselung - so sie denn diesmal wirklich existiere - sei für jeden - nein. Das gilt nur für zahlende Kunden. Bei nicht-zahlenden Nutzern gibt es eine enge Zusammenarbeit mit dem FBI, die eine Verschlüsselung ausschließt.[12] Und an jenen, die sagen, Zoom hätte ja nachgebessert habe und jetzt alles gut sei - Datenschutz ist nicht alles; aber jetzt kam heraus, dass unter Umständen schädlicher Code im Zoom-App ausgeführt werden kann.[13]

Kai Kobschätzki, Rechtsanwalt

[1] https://www.datenschutz-guru.de/datenschutzhinweise-zoom/

[2] https://zoom.us/de-de/terms.html

[3] https://zoom.us/de-de/subprocessors.html

[4] https://www.datenschutz-guru.de/tom-dokument-aws/

[5] beispielsweise aber hier:
https://www.datenschutzbeauftragter-info.de/amazon-cloud-sicher-ist-anders/

[6] https://zoom.us/privacy

[7] https://zoom.us/de-de/privacy.html

[8] https://zoom.us/de-de/terms.html

[9] https://zoom.us/de-de/privacy.html

[10] https://www.heise.de/suche/?q=zoom&make=security&sort_by=date

[11] https://en.wikipedia.org/wiki/Zoom_Video_Communications#Security_issues

[12] https://www.bloomberg.com/news/articles/2020-06-02/zoom-transforms-hype-into-huge-jump-in-sales-customers

[13] https://blog.talosintelligence.com/2020/06/vuln-spotlight-zoom-code-execution-june-2020.html

Linksammlung

1. Berliner Beauftragte für Datenschutz und Informationsfreiheit
2. Standpunkt der Uni Kassel
3. Golem.de: Zoom übermittelt heimlich Daten an Facebook
4. handelsblatt.de: Datenschützer warnen vor Videochat Software Zoom
5. Vice.com: Zoom is Leaking Peoples' Email Addresses and Photos to Strangers
6. Zeit.de: Unter Beobachtung
7. Zeit.de: Zoom schließt Sicherheitslücken nach Kritik
8. DerStandard.de: Zoom-CEO zu Sicherheitsproblemen: "Ich habe es wirklich vergeigt"
9. Handelsblatt.de: Auswärtiges Amt untersagt Nutzung von Zoom auf dienstlichen Geräten
10. DerAktionaer.de: Zoom: Jetzt warnt auch die Politik – das sollten Anleger und Nutzer wissen
11. BBC.com Coronavirus: Teachers in Singapore stop using Zoom after 'lewd' incidents
12. Heise.de: Zugangsdaten für hundertausende Zoom-Accounts zum Kauf im Darknet entdeckt
13. Universität Kassel: Videokonferenzen und Datenschutz in der Corona-Krise
14. riffreporter: Dank Zoom kann dein Computer zum Spionage-Tool werden
15. Heise.de: Videokonferenz-Software: Ist Zoom ein Sicherheitsalptraum?
16. Tagesschau.de: Zweifel an Zoom
17. Heise.de: Meeting-Zwang: Mac-Kameras lassen sich über Zoom-Sicherheitslücke anschalten
18. Heise.de: New Yorker Staatsanwältin prüft Datenschutz bei Konferenz-App Zoom
19. The Intercept: ZOOM MEETINGS AREN'T END-TO-END ENCRYPTED, DESPITE MISLEADING MARKETING
20. BleepingComputer: Zoom Lets Attackers Steal Windows Credentials, Run Programs via UNC Links
21. ZDNet: Windows 10 alert: Zoom client can leak your network login credentials
22. The New York Times: A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles
23. Handelsblatt.de: Datenschützer warnen vor Videochat-Software Zoom
24. golem.de: Trolle übernehmen Zoom-Konferenzen
25. Heise.de: Sicherheitsmängel: Google blockiert Zoom auf Arbeitsplatzrechnern
26. Heise.de: Zoom-Meeting-Passwörter geknackt
27. dev.io: Zoom Endpoint-Security Considerations - Who put the "Zoo" in "Zoom"?

Zitat aus dem Papier des Berliner Beauftragten für Datenschutz und Informationsfreiheit:

„Wir weisen darauf hin, dass einige verbreitet eingesetzte Anbieter die aufgeführten Bedingungen nicht erfüllen, darunter Microsoft, Skype Communications und Zoom Video Communications."

Zitat aus dem Dokument der Uni Kassel

„12. Für die Nutzung von Zoom durch die Universität Kassel ist zu beachten, dass sie dadurch nicht nur rechtswidrige Datenverarbeitungspraktiken dieses Unternehmens unterstützt und befördert, sondern auch ihre Lehrenden und Studierenden durch die Nutzung von Zoom diesen Datenverarbeitungspraktiken aussetzt. Für viele Studierende könnten sich Zwangssituationen zur Nutzung von Zoom ergeben.“