c/o RZ Universität Würzburg Am Hubland 97074 Würzburg

Für die bayerischen staatlichen Hochschulen

Stabsstelle IT-Recht
der bayerischen staatlichen Universitäten und Hochschulen

Ihr Zeichen, Ihre Nachricht	Unser Zeichen, Unsere Nachricht	Telefon, Name	Datum
	-	+49(0)931/31-84217, Nehlsen	28.10.2020

Einsatzszenarien von Zoom für Besprechungen mit vertraulichen Inhalten

Sachverhalt

Die von Zoom Video Communications, Inc. (Zoom) angebotene Konferenzlösung ist für ihre Zuverlässigkeit, ihren geringen Bandbreitenbedarf und ihre Geräteunabhängigkeit bekannt. Offen ist jedoch die Frage, ob Zoom auch in Bezug auf Datensicherheit und Vertraulichkeit für vertrauliche Besprechungen genutzt werden kann.

Die technische Umsetzung stellt Zoom auf den unternehmenseigenen Internetseiten dar.

Daneben ermöglicht Zoom den Transfer der Lizenzen in europäische Rechenzentren, so dass amerikanische Rechenzentren für Besprechungen deaktiviert werden kann.

Diese Stellungnahme bewertet, inwieweit Zoom im Hinblick auf strafrechtliche und datenschutz-rechtliche Vorgaben (abseits der Fragen der Auftragsverarbeitung mit Zoom) für Besprechungen mit vertraulichen Inhalten eingesetzt werden kann.

Einschätzung

Der Einsatz von Zoom kann, (abseits der Fragen der Auftragsverarbeitung mit Zoom), bei der Nutzung der Ende-zu-Ende-Verschlüsselung von Zoom, ohne nennenswerte datenschutz- und strafrechtliche Risken erfolgen.

Dienstort
Universität Würzburg
Am Hubland Z 8
97074 Würzburg

Telefon
Telefon +49(0)931/31-84217
Telefax +49(0)931/31-84217-0

elektronische Post
johannes.nehlsen
@uni-wuerzburg.de

Internet
https://www.rz.uni-wuerzburg.de/
dienste/it-recht/

Im Einzelnen

Vertraulichkeit in der Besprechung

Der oder die Besprechungsorganisatorin trägt die Verantwortung bezüglich der Personen, denen eine Teilnahme am Meeting gestattet wird. Neben der individuellen Möglichkeit einer Identitätskontrolle der teilnehmenden Personen bietet Zoom die Möglichkeit, Kenncodes für Besprechungen zu nutzen, Warteräume einzurichten, die Besprechung nach dem Beginn für weitere Teilnehmer zu sperren oder Personen während einer Besprechung zu entfernen.

Es wird empfohlen, von den teilnehmenden Personen die Sicherheitscodes zur Verifikation der Ende-zu-Ende-Verschlüsselung auf Gleichheit zu prüfen und das Ergebnis zu dokumentieren[1]. Als weitere Optionen können je nach Vertraulichkeit Regelungen z.B. zur Unterlassung von Aufnahmen einer Besprechung in Erwägung gezogen werden.

Vertraulichkeit der Besprechung

Die latenten Risiken aus dem internationalen Datentransfer (u.a. Spionage oder fremde Gerichtsbarkeiten) können durch einen Wechsel der Verwaltung der Lizenzen von amerikanischen Rechenzentren in deutsche bzw. europäische Zoom-Rechenzentren minimiert werden. Dadurch wird ein Zugriff für ausländische Geheimdienste auf die "Netzverbindungen" zunehmend erschwert bzw. nur durch rechtmäßige Kooperation mit dem BND möglich.

Datenhoheit

Die Möglichkeit des hybriden Betriebs schafft für eine Hochschule mehr Datenhoheit, jedoch zum Preis einer geringeren Verlässlichkeit bei der Verfügbarkeit des Dienstes durch die Abhängigkeit von der eigenen Infrastruktur. Es ist zu beachten, dass Sitzungs-Metadaten auch beim hybriden Betrieb über die Zoom-Infrastruktur transportiert werden.

Verschlüsselung

Die von Zoom einsetzte Verschlüsselung für den Transport von Daten entspricht nach den verfügbaren Unterlagen dem Stand der Technik. Zoom stellt zum einen ein Whitepaper zur Sicherheit[2] bereit und hat zum anderen das Konzept seiner Ende-zu-Ende-Verschlüsselung offengelegt.[3] Für die Verschlüsselung von Besprechungen setzt Zoom auf AES 256-bit GCM.[4] Dieses Verschlüsselungsverfahren zusammen mit der Schlüssellänge entspricht den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI).[5] Ferner sind alte Protokolle für den Datentransport deaktiviert[6], wie auch vom BSI empfohlen.[7]

Potenziell könnten nicht am Meeting beteiligte Personen bei Verwendung der Verschlüsselung von Zoom nur noch in den Besitz von Metadaten gelangen– genau so, wie dieses bei der Verwendung anderer Kommunikationslösungen (einschließlich Telefon) möglich wäre. Ein manipulativer Eingriff durch Zoom oder einen Dritten, welcher Kontrolle über die Server erlangt hat, wäre nicht mehr unentdeckt möglich.

Rechtliche Bewertung

Wird eine Besprechung mit Ende-zu-Ende-Verschlüsselung durchgeführt, kann durch den Einsatz von Zoom weder der Tatbestand eines unbefugten Offenbarens von fremden (§ 203 StGB) noch von dienstlichen Geheimnissen (§ 353b StGB) erfüllt werden noch ein unbefugtes Offenlegen personenbezogener Daten vorliegen.

Auch zur Gewährleistung der Vertraulichkeit in Personalangelegenheiten ist eine Ende-zu-Ende-Verschlüsslung eine wichtige Schutzmaßnahme, wobei hier noch weitere Vorgaben aus dem Fachrecht zu beachten sein können.

---

[1] Vgl. https://blog.zoom.us/zoom-rolling-out-end-to-end-encryption-offering/
[2] https://zoom.us/docs/doc/Zoom-Security-White-Paper.pdf
[3] https://github.com/zoom/zoom-e2e-whitepaper
[4] https://zoom.us/docs/doc/Zoom%20Encryption%20Whitepaper.pdf
[5] Technische Richtlinie BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen u.a. 1.2, 5.3 und C.1.
[6] https://support.zoom.us/hc/en-us/articles/360031328671-Zoom-Disabling-TLS-1-0-and-1-1
[7] Technische Richtlinie TR-02102-2 Kryptographische Verfahren: Empfehlungen und Schlüssellängen 3.2