Webmeetings unter datenschutzrechtlichen Gesichtspunkten

»Restrisiken verbleiben bei jeder der untersuchten Lösungen. Die quelloffenen Angebote Jitsi und Big Blue Button bieten weniger Ansatzpunkte für datenschutzseitige Bedenken, sofern die Rahmenbedingungen geschaffen werden.«

NUR IM EINZELFALL UND AUFGRUND VERTRAGLICHER VEREINBARUNG KÖNNEN DATENÜBERMITTLUNGEN IN DIE USA ZULÄSSIG SEIN. DER VERTRAGSPARTNER IN DEN USA MUSS GEEIGNETE GARANTIEN DAFÜR GEBEN, DASS DIE DATEN NICHT IN FREMDE HÄNDE FALLEN – AUCH NICHT IN DIE DER DORTIGEN SICHERHEITSDIENSTE. DIE EINHALTUNG IST ZUDEM ZU ÜBERPRÜFEN. WERDEN DIE GARANTIEN NICHT EINGEHALTEN, MUSS DIE DATENÜBERMITTLUNG AUSGESETZT WERDEN. GEGEBENENFALLS KÖNNEN DATENSCHUTZBEHÖRDEN ALSO INTERVENIEREN UND EIN AUSSETZEN DER ÜBERMITTLUNG ANORDNEN – DAMIT WÄRE DER BETREFFENDE DIENST NICHT MEHR NUTZBAR.

AUTOR Anselm Rohrer ist Bereichsleiter ISMS bei der Allgeier IT-Solutions. Die Allgeier IT-Solutions unterstützt Kunden bei der Identifikation und Umsetzung eines adäquaten Sicherheitsniveaus. Sie stellt externe Beauftragte für Datenschutz und Informationssicherheit sowie umfangreiche Werkzeuge zur IT-Security bereit. Der Beitrag entstand in Zusammenarbeit mit RA Georg Kleine, LL.M.

Was bedeutet all das nun für die derzeit zahlreich durchzuführenden Webkonferenzen und Webmeetings? Welche Anbieter bergen welche Risiken bzw. sind zu empfehlen?

Gelangen aufgrund einer Datenübermittlung in die USA Daten in die Hände Unbefugter, kann, sofern Betroffenen ein Schaden entsteht, ein Schadenersatzanspruch entstehen. Weil die Datenübermittlung ohne geeignete Garantien in die USA unzulässig ist, kann zudem ein Bußgeld von der Aufsichtsbehörde verhängt werden.

Daher bedürfen die gerade während der Corona-Krise beliebten Videokonferenz-Lösungen einer datenschutzrechtlichen Überprüfung.

Zoom und Microsoft Teams

Bei den Angeboten von Zoom und Microsoft (Teams) muss grundsätzlich ein Vertrauen in den jeweiligen Anbieter vorliegen, dass dieser der Verpflichtung zur Verarbeitung der Daten innerhalb der EU gerecht wird. Beide Anbieter gehen prinzipiell mit der DSGVO konform. Die Frage nach der Überprüfbarkeit sowie US-Gesetzen, die für diese Unternehmen Vor-rang haben können, bleibt damit jedoch unbeantwortet.

Abseits vertraglicher Regelungen ist hinsichtlich des Datenschutzes insbesondere Verschlüsselungstechnologie relevant, da diese geeignet ist, eine Einsichtnahme Unbefugter auf technischer Ebene zu unterbinden.

Die sog. Ende-zu-Ende-Verschlüsselung (E2EE) von Zoom wurde mehrfach kritisch untersucht (https://www.schneier.com/blog/archives/2020/06/zoom_will_be_en.html, https://sbscyber.com/resources/zoom-is-it-safe) und scheint eher Marketing als echte E2EE zu sein. Hier müssen Sie damit rechnen, dass die Informationen durch Zoom eingesehen und auch anderweitig genutzt werden können.

Microsoft gibt für Teams schon nur „in transit" und „at rest" an (https://docs.microsoft.com/en-us/microsoftteams/security-compliance-overview): Hier muss also klar sein, dass die Informationen zwischendurch lesbar sind und damit anderen Zwecken zukommen können.

Bei beiden Unternehmen muss mit Einsicht durch US-Behörden gerechnet werden. Für beide Dienste können Einstellungen vorgenommen werden, die zumindest die Privatsphäre der Teilnehmer schützen.

Jitsi und Big Blue Button

Demgegenüber stehen quelloffene Angebote von Jitsi und Big Blue Button. Beide können (und sollten!) selbst gehostet werden, um die bei anderen Anbietern bestehenden Bedenken zu umgehen. Bei Angeboten von Hosting-Dienstleistern ist zu beachten, ob die Lösungen dann selbst administriert werden und inwieweit ein Zugriff von deren Seite noch möglich wäre.

Diese Einsichtnahme durch Dritte lässt sich durch E2EE unterbinden, da die Daten dann nur noch durch die Teilnehmer entschlüsselt werden können. Dies ist bei Jitsi in Arbeit (https://jitsi.org/blog/e2ee/). Big Blue Button bietet dagegen nur Transportverschlüsselung (https://docs.bigbluebutton.org/support/faq.html).

Die Auftragsverarbeitungsverträge (AVVs) der Anbieter hat der Berliner Datenschutz geprüft (https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/orientierungshilfen/2020-BlnBDI-Hinweise_Berliner_Verantwortliche_zu_Anbietern_Videokonferenz-Dienste.pdf). Er kam zu dem Ergebnis, dass die kommerziellen US-Anbieter durchweg ungenügend waren. Seitdem haben die Anbieter Anpassungen vorgenommen. Die Anbieter der quelloffenen Systeme sind im Einzelfall separat zu untersuchen, da diese von der Software unabhängig sind.