Kurzinformation: Ende-zu-Ende-Verschlüsselung bei Zoom

Projekt Rechtsinformationsstelle Digitale Hochschule NRW, Leitung Prof. Thomas Hoeren

Veröffentlicht am 06. Juli 2020

Am 17.6.2020 kündigte Zoom an, *im Juli 2020* mit der Ende-zu-Ende-Verschlüsselung (E2E-Verschlüsselung) in der *Beta* zu beginnen, das heißt in einer vorläufigen Version, die noch fortlaufend getestet und aktualisiert wird. Neben der E2E-Verschlüsselung wird die schon implementierte Transportverschlüsselung weiterhin standardmäßig verwendet werden. Ähnlich wie vormals beim Update von der AES-128 auf die AES-256-Transportverschlüsselung können an Meetings, bei denen der Host die E2E-Verschlüsselung aktiviert hat, nur Teilnehmer teilnehmen, die bereits die aktuelle Programmversion installiert haben und sich für die E2E-Verschlüsselung einmalig registriert haben (Bestätigungscode auf dem Handy zum Zwecke der Missbrauchsvorbeugung).
Durch den Einsatz von E2E-Verschlüsselung werden nur noch die Teilnehmer eines Meetings auf die Inhaltsdaten (z.B. Video-, Audiospur, Chat) zugreifen können. Serverseitige Zugriffe und Entschlüsselung - wie bei der Transportverschlüsselung - sind dagegen nicht möglich. Bei einer solchen vollumfänglichen E2E-Verschlüsselung werden die Inhaltsdaten der Teilnehmer damit vollständig vor dem Zugriff Dritter geschützt.

Eine funktionierende E2E-Verschlüsselung wäre im Bereich von Videokonferenzen mit mehreren Dutzend Teilnehmern, welche alle Audio- und Videosignale parallel senden, ein Meilenstein. Die Methode ist in diesem Bereich technisch schwer umzusetzen und gehört bisher nicht zum Stand der Technik

Die Aussicht auf eine zeitnahe E2E-Verschlüsselung ist für Hochschulen interessant, die weiterhin auf Videokonferenzsysteme setzen, besonders mit Blick auf etwaige Online-Prüfungen, in denen sensiblere personenbezogene Daten übertragen werden als im Rahmen von Vorlesungen.
Interessant ist indes auch die Information, dass Studierende rechtzeitig die Software updaten und sich authentifizieren müssten.

Um ein besseres und sicheres Code-Design zu erhalten, veröffentlichte Zoom im Vorfeld den Programm-Code für die E2E-Verschlüsselung, reagierte auf das Feedback von Organisationen und Experten hierzu und veröffentlichte mit der o.g. Ankündigung eine überarbeitete Designvariante des Codes (Link). Feedback zum kryptografischen Design ist ausdrücklich erwünscht.

Die Funktion soll sowohl für kostenpflichtige als auch kostenlose Konten zur Verfügung stehen. Damit lenkt Zoom nach heftiger Kritik ein, nachdem erst beabsichtigt war, die E2E-Verschlüsselung nur für kostenpflichtige Accounts verfügbar zu machen. Vor der Nutzung der E2E-Verschlüsselung wird es aber für Nutzer von kostenlosen Konten erforderlich sein, eine einmalige Authentifizierung über die Telefonnummer durchzuführen. Dies soll dem eventuellen (Massen-) Missbrauch der Software für illegale Aktivitäten vorbeugen. Nicht bekannt ist bislang, wie diese Informationen von Zoom gespeichert werden.

Nach der bisherigen Beschreibung von Zoom wird die E2E-Verschlüsselung vom Host ein- und ausschaltbar sein. Bei eingeschalteter E2E-Verschlüsselung werden einige Funktionen von Zoom nicht oder nur eingeschränkt nutzbar sein. So wird es beispielsweise nicht möglich sein, sich über klassische PSTN-Telefonverbindungen oder mit Konferenzraumsystemen mit SIP/H.323-Hardware in das verschlüsselte Meeting einzuwählen. Die Aktivierung bzw. Deaktivierung der E2E-Verschlüsselung wird vom Administrator auf der Konto- und Gruppenebene möglich sein. Schließlich ist darauf hinzuweisen, dass die E2E-Verschlüsselung zunächst nur für Zoom-Meetings verfügbar sein wird. Zoom-Videowebinare sind von der Verschlüsselung im Rahmen der Erstveröffentlichung noch nicht umfasst, sollen jedoch in späteren Versionen ebenfalls verschlüsselt werden können.

Weiterführende Links: https://blog.zoom.us/end-to-end-encryption-update/

https://blog.zoom.us/90-day-security-plan-progress-report-june-17/