Europäischer Datenschutztag 2021: Software-Unternehmen wenden sich gegen die Einführung von Crypto-Backdoors

- Am 28. Januar 2021 ist der europäische Datenschutztag. Zu diesem Anlass fordern die vier Software-Unternehmen ProtonMail, Threema, Tutanota und Tresorit: Datensicherheit muss in der EU weiterhin höchste Priorität haben
- Die Softwareanbieter sehen derzeit den Datenschutz in der EU in Gefahr: EU-Politiker beraten über die Einführung von sogenannten Crypto-Backdoors in Ende-zu-Ende-verschlüsselte Lösungen, ob für E-Mail, Messaging oder File-Sharing-Apps
- Crypto-Backdoors zerstören jedoch das Konzept von Ende-zu-Ende-Verschlüsselung und senken somit die Sicherheitslevel für Unternehmen und Bürger – weshalb sich die Software-Unternehmen gemeinsam gegen das Vorhaben wenden

28. Januar 2021 – Am 28. Januar 2021 ist der europäische Datenschutztag. Zu diesem Anlass rückt die aktuelle Diskussion über die Einführung von Crypto-Backdoors in Ende-zu-Ende-verschlüsselte Software erneut in den Fokus, die vier europäischen Software-Unternehmen ProtonMail, Threema, Tutanota und Tresorit fordern zu diesem Anlass gemeinschaftlich die EU-Politiker auf, dieses Vorhaben zu überdenken.

Das vom EU-Ministerrat erklärte Ziel "Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung" zu erlangen, würde beim Einsatz sogenannter Crypto-Backdoors die Datensicherheit von Millionen von Europäern bedrohen und das Vertrauen in die Ende-zu-Ende-Verschlüsselung untergraben. Die vier europäischen Technologieunternehmen ProtonMail, Threema, Tutanota und Tresorit wenden sich deshalb gegen dieses Vorhaben.

Der aktuelle Entwurf der Resolution des EU-Ministerrates beruht auf einem eingeschränkten Verständnis der technischen Aspekte von Ende-zu-Ende-Verschlüsselung. Denn Ende-zu-Ende-Verschlüsselung ist absolut, Daten sind entweder verschlüsselt oder nicht. Während der Wunsch, den Strafverfolgungsbehörden mehr Werkzeuge zur Verbrechensbekämpfung an die Hand zu geben, verständlich ist, ist die Aufhebung der Ende-zu-Ende-Verschlüsselung dabei nicht der richtige Weg, sind sich die Security-Experten von ProtonMail, Threema, Tutanota und Tresorit einig.

Im letzten Jahr haben Millionen von Privatpersonen und Unternehmen auf Technologien wie Ende-zu-Ende-Verschlüsselung gesetzt, um ihre digitale Sicherheit und Privatsphäre zu gewährleisten. Es scheint deshalb nicht konsequent, dass die politischen Entscheidungsträger in der EU jetzt auf solche Gesetze drängen, die den wachsenden europäischen Technologiesektor in diesem Bereich untergraben.

In den kommenden Monaten ist die Ausarbeitung konkreter Vorschläge seitens der Politik geplant. Die Resolution hat der Europäischen Kommission den Weg geebnet, um in den kommenden Monaten mit der Ausarbeitung konkreter Vorschläge zu beginnen. Aber wie ProtonMail, Threema, Tresorit und Tutanota betonen, sollte die Kommission bedenken, dass es aus technologischer Sicht unmöglich ist, einen Zugang zu Ende-zu-Ende-verschlüsselten Inhalten zu gewähren, ohne die Sicherheit der gesamten Systeme zu gefährden.

"Dies ist nicht das erste Mal, dass wir eine verschlüsselungsfeindliche Rhetorik aus einigen Teilen Europas hören, und ich bezweifle, dass es das letzte Mal sein wird. Aber das bedeutet nicht, dass wir

klein beigeben sollten", sagte Andy Yen, CEO und Gründer von ProtonMail, einem Ende-zu-Ende-verschlüsselten E-Mail-Dienst. "Eigentlich unterscheidet sich die Resolution nicht von den vorherigen Vorschlägen, die ebenfalls eine starke Gegenreaktion von datenschutzbewussten Unternehmen, Mitgliedern der Zivilgesellschaft, Experten und Europaabgeordneten hervorgerufen haben. Der Unterschied ist allerdings, dass dieses Mal explizite Worte wie 'Verbot' oder 'Hintertür' vermieden wurden – das Ergebnis ist aber dasselbe. Daher ist es umso wichtiger, dass jetzt Schritte unternommen werden, um diese Vorschläge zu unterbinden und die Rechte der Europäer auf Privatsphäre intakt bleiben."

"Unternehmen setzen auf Ende-zu-Ende-Verschlüsselung, um ihr geistiges Eigentum zu schützen und Bürger nutzen solche Lösungen, um sicher zu kommunizieren und ihr Recht auf Privatsphäre zu nutzen. Europäische Anbieter zu zwingen, die Ende-zu-Ende-Verschlüsselung absichtlich zu schwächen, würde nicht nur die europäische IT- und Startup-Wirtschaft zerstören, sondern auch die IT-Sicherheit für alle verringern. Damit würde sich Europa in die Riege der berüchtigtsten Überwachungsstaaten einreihen und seinen einzigartigen Wettbewerbsvorteil bei dem Schutz der Privatsphäre seiner Bürger leichtfertig aufgeben", sagte Martin Blatter, CEO von Threema, der Ende-zu-Ende-verschlüsselten Instant-Messaging-Anwendung.

"Diese Resolution würde das zunehmende Vertrauen von Privatpersonen und Unternehmen in Ende-zu-Ende-verschlüsselte Dienste ernsthaft untergraben. Insbesondere im Hinblick auf die ansonsten sehr fortschrittliche Haltung der EU in Sachen Datenschutz, ist die neue Resolution alarmierend. Die Datenschutzgrundverordnung (DSGVO) befürwortet ausdrücklich eine starke Verschlüsselung als eine grundlegende Technologie, um die Privatsphäre der Bürger zu gewährleisten. Diese neuen Vorschläge sind unvereinbar mit der aktuellen Haltung der EU zum Datenschutz", so Istvan Lam, Mitegründer und CEO von Tresorit, einem Cloudlösungs-Anbieter für den Austausch von Dateien mit Ende-zu-Ende-Verschlüsselung.

"Verschlüsselung ist quasi das Rückgrat des Internets. Jeder EU-Bürger braucht Verschlüsselungstechnologien, damit seine Daten im Netz sicher sind. Mit dem jüngsten Versuch, Crypto-Backdoors durchzusetzen, wollen Politiker einen einfachen Weg finden, um Verbrechen wie Terroranschläge zu verhindern. Allerdings lassen sie dabei die ganze Reihe an Verbrechen außer Acht, vor denen uns die Verschlüsselung bewahrt. So schützt Ende-zu-Ende-Verschlüsselung Daten und Kommunikation vor Hackern, (ausländischen) Regierungen und Terroristen. Indem Politiker den Einbau von Hintertüren in verschlüsselte Lösungen fordern, würden sie die Sicherheitslevel vermindern", sagte Arne Möhle, Mitbegründer von Tutanota, dem deutschen Anbieter von Ende-zu-Ende-verschlüsselten E-Mails.