PRESSEMITTEILUNG

Gegen staatliche Hintertüren: Bundesverband IT-Sicherheit e.V. (TeleTrusT) kritisiert geplante EU-weite Aushebelung der Ende-zu-Ende-Verschlüsselung

Berlin, 10.11.2020 - Medienberichten zufolge haben sich die Regierungen der EU-Mitgliedsstaaten darauf verständigt, sichere Verschlüsselung EU-weit zu verbieten. Demnach sollen Technologieanbieter und Dienstebetreiber dazu gezwungen werden, Hintertüren in ihre Verschlüsselung einzubauen. Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) wendet sich gegen diesen wiederholten Versuch, Krypto-Technologie staatlicherseits zu schwächen.

Die Forderung nach staatlichen Nachschlüsseln begleitet die Entwicklung von Krypto-Produkten seit den Neunzigerjahren, hat sich aber in demokratisch verfassten Staaten bislang nicht durchsetzen können. Dass solche Hintertüren jetzt wieder auf der politischen Tagesordnung stehen, hat sicherlich damit zu tun, dass immer mehr Straftäter Verschlüsselung nutzen. Verschlüsselung hat sich inzwischen zu einem massiven Problem für die Ermittlungsbehörden entwickelt, da schon Anwender ohne besondere IT-Kenntnisse mit kostenlosen Tools so sicher verschlüsseln können, dass Experten kaum eine Chance haben, die Verschlüsselung zu knacken.

Dennoch ist die Verschlüsselung ein sehr wirksamer IT-Sicherheitsmechanismus, der hilft, die Werte auf unseren IT-Systemen angemessen zu schützen und damit sicher und vertrauenswürdig in die digitale Zukunft zu gehen.

Rechtsanwalt Karsten U. Bartels LL.M., stellvertretender TeleTrusT-Vorstandsvorsitzender: "Die Herausforderungen in der Strafverfolgung und der Kriminalprävention dürfen nicht ignoriert werden. Eine Aushöhlung der Verschlüsselung bedeutet aber, die ohnehin träge Digitalisierung in der EU zu gefährden. Denn diese gelingt nur nachhaltig, wenn wir das Vertrauen in IT fördern - und nicht mindern. Lösungen mit Hintertür können nicht als dem 'Stand der Technik' entsprechend betrachtet werden. Das Zurückfallen auf einen schlechteren Technologiestand hat nicht nur massive Auswirkungen auf die IT-Sicherheit, es ist rechtlich auch nicht mit der DSGVO und dem IT-Sicherheitsgesetz vereinbar."

Hinzu kommt, dass Hintertüren den eigentlich beabsichtigten Zweck verfehlen. Selbst wenn in Deutschland nur noch Krypto-Produkte mit staatlicher Hintertür verkauft werden dürften, könnten sich Straftäter problemlos Verschlüsselungslösungen ohne eine solche Hintertür besorgen und weiterhin nutzen.

Entscheidende industrie- und sicherheitspolitische Argumente gegen staatliche Hintertüren in Krypto-Technologie sind:

1. Negative Auswirkungen auf das Vertrauen in die Digitalisierung und die Rolle des Rechtsstaates dabei.

2. Schädigung des Rufs der deutschen Krypto-Industrie: Im Gegensatz z.B. zu den USA, wo staatliche Nachrichtendienste Einfluss auf Krypto-Hersteller nehmen, haben sich in Deutschland die Behörden diesbezüglich bislang zurückgehalten. Krypto "Made in Germany" hat auch deshalb international einen sehr guten Ruf.

3. Potentieller Missbrauch: Wenn Nachschlüssel in größerer Zahl in die falschen Hände fallen, könnte dies zu einer Katastrophe führen. Es ist klar, dass sowohl kriminelle als auch staatliche Hacker nichts unversucht lassen werden, um an die Nachschlüssel, die in einer Datenbank gespeichert sein müssen, zu gelangen.

4. Mangelhafte Implementierung der Backdoor-Technologie: Immer wieder auftretenden Fehler im Bereich der Implementierung schaffen ein unkalkulierbares Risiko.

Bartels: "Wer einen Staat mit Generalschlüsseln als Zugang zu verschlüsselter Kommunikation ausstattet, schadet massiv dem liberalen Rechtsstaat. Er schadet dem Vertrauen in sichere IT, der Wirtschaft und nicht minder den rechtsstaatlichen Erwartungen der Bürgerinnen und Bürger.“

Der Bundesverband IT-Sicherheit ist überzeugt, dass eine bessere Strafverfolgung und Tatprävention möglich sind, auch ohne die IT-Sicherheit, die Digitalisierung und das Recht derart zu gefährden.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Bundesverband IT-Sicherheit e.V. (TeleTrusT), Dr. Holger Mühlbauer, Geschäftsführer, Chausseestraße 17, 10115 Berlin, Tel.: +49 30 40054310, holger.muehlbauer@teletrust.de
https://www.teletrust.de