

PRESSEMITTEILUNG

Achtung, Grauzone: Journalistischer Quellenschutz bei staatlichem Zugriff auf Cloud-Speicher

TeleTrust – Bundesverband IT-Sicherheit e.V. empfiehlt Journalisten Verschlüsselungslösungen

Berlin, 22.05.2013 – Der journalistische Quellenschutz gilt nach Auffassung des Bundesdatenschutzbeauftragten nur für Daten, die sich in direktem Gewahrsam von Journalisten befinden, nicht jedoch für in Cloud-Anwendungen gespeicherte Daten. Der Bundesverband IT-Sicherheit e.V. (TeleTrust) hält die Anwendung des Durchsuchungs- und Beschlagnahmeverbotes bei Journalisten auch für Cloud-Daten für zeitgemäß, empfiehlt jedoch in jedem Fall, Verschlüsselungstechnologie zu nutzen.

Den Quellenschutz für Medienvertreter hat das Bundesverfassungsgericht im Wege der Rechtsprechung bereits 1959 geprägt und regelmäßig weiterentwickelt. Der verfassungsrechtliche Rang wird auf allen Ebenen der Rechtsprechung respektiert. Ein Journalist muss keine Auskunft über die Quelle seiner Informationen geben. Das journalistische Privileg des Zeugnis- bzw. Auskunftsverweigerungsrechts ist in Deutschland in der Strafprozessordnung (§ 53 Absatz 1 Nr. 5 StPO), in der Zivilprozessordnung (§ 383 Absatz 1 Nr. 5 ZPO) und analog z.B. in der Abgabenordnung (§ 102 Absatz 1 Ziffer 4 AO) geregelt.

Dieser weitgehende Schutz erstreckt sich mittelbar nicht nur auf Informanten, sondern auch auf Materialien, die ein Journalist im Zuge von Recherchen erlangt hat oder erstellt, jedenfalls dann, wenn sie sich auf einen Sachverhalt von öffentlichem Interesse beziehen. Das Beschlagnahme- und Durchsuchungsverbot nach § 97 Absatz 1 StPO soll verhindern, dass das Zeugnisverweigerungsrecht durch Beschlagnahme und Auswertung von Recherchematerial ausgehebelt wird. Sowohl Redaktionsräume als auch der private Bereich eines Journalisten sind vor staatlichem Zugriff geschützt.

Der Bundesdatenschutzbeauftragte wies jüngst darauf hin, dass der journalistische Quellenschutz bzw. der entsprechende Schutz vor staatlichem Zugriff allerdings nur für Daten gelte, die sich in direktem Gewahrsam von Journalisten befänden, nicht aber für online gespeicherte Daten, und riet Journalisten, auf solche Speicheranwendungen gänzlich zu verzichten.

TeleTrust-Geschäftsführer Dr. Holger Mühlbauer: "Der Hinweis des Bundesdatenschutzbeauftragten ist wichtig, auch wenn die tatsächliche Rechtslage im Ernstfall noch zu interpretieren wäre. Es ist jedoch fraglich, ob Technologieverzicht der richtige Ansatz ist. Journalistischer Quellenschutz ist ein hohes Gut in einem demokratisch verfassten Gemeinwesen, in dem die freie Presse eine wichtige Wächterfunktion innehat. Gleichzeitig sind gerade Medienvertreter auf die Nutzung von IT angewiesen. Der Quellenschutz muss der technologischen Entwicklung folgen und auch für Daten in Cloud-Anwendungen gelten."

Oliver Dehning, Leiter der TeleTrust-Arbeitsgruppe "Cloud Security": "Die Empfehlung des Bundesdatenschutzbeauftragten unterstreicht einmal mehr die Bedeutung von Verschlüsselung bei online gespeicherten Daten – ganz unabhängig von der Frage der Rechtmäßigkeit des Zugriffs Dritter."

TeleTrust rät Journalisten in jedem Fall, bei Cloud-Anwendungen auf umfassende Verschlüsselungslösungen zurückzugreifen.

TeleTrust – Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrust) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. 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), des Expertenzertifikates "TeleTrust Information Security Professional" (T.I.S.P.) sowie des Qualitätszeichens "IT Security made in Germany". Hauptsitz des Verbandes ist Berlin. TeleTrust ist Mitglied des European Telecommunications Standards Institute (ETSI).