Your Key to Cloud Data Protection

MEDIA ALERT

Unzureichender Schutz von sensiblen Daten deutscher Bürger – Eperi fordert: Datenverschlüsselung in der Cloud muss im stärker in den Fokus rücken

Datenschützer sind in großer Sorge um deutsche Daten: Etwa 40 Dienststellen des Bundes speichern Daten bei externen Cloud-Anbietern – so Zahlen aus einer Sitzung des Innenausschusses des Bundestags veröffentlicht auf hr-info. Die Sicherheit der teilweise sensiblen Daten wird vor diesem Hintergrund vermehrt in Frage gestellt. Nachdem Anfang April 2019 bekannt wurde, dass „Bodycam-Daten" der deutschen Bundespolizei in Amazon Web Services (AWS), dem Cloud-Dienst des US-amerikanischen Anbieters Amazon, gespeichert werden, wurden in einer Innenausschusssitzung weitere Fälle offengelegt, in denen Daten deutscher Bürger auf Servern gespeichert werden, deren Rechtsgrundlage zum Datenschutz zumindest umstritten ist.

Europäische Datenschutzrichtlinien wie die EU-DGSVO gelten auch für Cloud-Services außereuropäischer Anbieter wie AWS, die in Europa angeboten werden. Gleichzeitig gilt aber auch beispielsweise der US-amerikanische „Cloud Act", mit dem die US-Behörden Zugriff auf Daten der Kunden dieser Anbieter erhalten wollen, selbst wenn die Daten nicht in den USA gespeichert sind. Auf Servern europäischer Anbieter wäre dies nicht gegeben oder zumindest rechtlich deutlich schwieriger. Konstantin von Notz, Bundestagsabgeordneter der Grünen, fordert deshalb im Podcast mit hr-info, dass die Bundesregierung eine europäische Lösung zur Speicherung von sensiblen Behördendaten erarbeite, die den hiesigen Standards entspreche.

Der Standort der Cloud-Server ist nicht das eigentliche Problem

„Das Problem des unbefugten Zugriffs auf Daten wird in der aktuellen Diskussion nur von einer Seite beleuchtet", mahnt jedoch Elmar Eperiesi-Beck, CEO und Gründer des deutschen Spezialisten für Datenverschlüsselung Eperi. „Selbst wenn die Daten bei einem deutschen Cloud-Anbieter liegen würden, wäre der Datenschutz damit nicht per se gewährleistet. Solange die Daten unverschlüsselt in der Cloud gespeichert werden, können die Cloud-Provider darauf zugreifen."

Das Thema Datenverschlüsselung in der Cloud wird in den Augen von Eperiesi-Beck teilweise stark vernachlässigt: „Niemand kann vollständig verhindern, dass Externe Zugriff auf in der Cloud gespeicherte Daten erhalten. Was Organisationen jedoch sehr wohl aktiv verhindern können, ist dass Unbefugte diese Daten für sich nutzen können – durch Datenverschlüsselung und Pseudonymisierung. Aufgrund der unklaren Rechtslage sollten sich Unternehmen und Behörden dringend mit dem Thema Datenverschlüsselung in der Cloud auseinandersetzen, denn Prävention ist der beste Schutz vor Datenmissbrauch."

Deutscher Spezialist für Datenverschlüsselung mit Fokus auf die öffentliche Hand

Eperi ist ein deutscher Spezialist für Datenverschlüsselung mit mehr als 15 Jahren Erfahrung. Die Basis der Eperi-Gateway-Lösungen wurden in enger Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelt. Zahlreiche Organisationen der öffentlichen Hand, wie die Bundesnetzagentur, zählen zu den Kunden. Eperi ist Gründungsmitglied und Partner der Initiative „Allianz für Cyber-Sicherheit" des BSI und unter anderem Mitglied bei TeleTrust.

Weitere Informationen

Haben Sie Fragen zu diesem Thema? Gerne organisieren wir ein Interview mit Elmar Eperiesi-Beck für Sie.