Handelsblatt

HandelsblattNr. 114 vom 17.06.2019 Seite 043

Ali Sunyaev

„Vertrauen ist gut, Zertifizierung ist besser“

Der Informatik-Professor über die Herausforderung, Gesetze in technische Vorgaben zu übersetzen.

Gemeinsam mit Datenschützern arbeitet die IT-Branche im Projekt „Auditor“ an einem Zertifikat, das Cloud-Anbietern den verantwortungsvollen Umgang mit Personendaten bescheinigen soll – Treiber ist die vor einem Jahr in Kraft getretene europäische Datenschutzgrundverordnung (DSGVO). Ali Sunyaev, Professor für Informatik am Karlsruher Institut für Technologie, koordiniert das vom Bundeswirtschaftsministerium finanzierte Vorhaben.

Privat

Herr Sunyaev, was bringt ein weiteres Zertifikat für Cloud-Anbieter?
Es gibt schon einen Dschungel an Zertifikaten, aber die meisten konzentrieren sich auf die IT-Sicherheit. Die DSGVO gibt jetzt ein einheitliches europäisches Rahmenwerk für den Umgang mit personenbezogenen Daten vor. Mit einem Zertifikat können Cloud-Anbieter die sichere und sorgfältige Datenverarbeitung nachweisen. Dies könnte auch helfen, das negative Image der Unternehmen als Datenkraken abzuschütteln, welches so oft im Markt vorherrscht. Das Vertrauen in die Einhaltung der Datenschutzregeln ist gut – aber eine Kontrolle durch eine Zertifizierung ist besser.

Mussten Sie dafür bei null anfangen?
Wir bauen auf bestehenden Kriterien auf. Es gab bereits einen Anforderungskatalog nach dem Bundesdatenschutzgesetz. Alles, was nach den Regeln der DSGVO noch Sinn ergibt, haben wir übernommen. Darüber hinaus gibt es zahlreiche neue verschärfte Kriterien – etwa im Hinblick auf die Wahrung der Betroffenenrechte. Cloud-Nutzer haben nun unter anderem das Recht, Auskunft über die Datenverarbeitung zu erhalten. Wir übersetzen die Vorgaben in informatische und sozio-technische Lösungen.

Im Projekt engagieren sich Cloud-Anbieter, -Anwender sowie Datenschutzbehörden und Juristen. Lassen sich die Interessen koordinieren?
Wir haben immer sehr früh versucht, eine Rückmeldung von den verschiedenen Akteuren einzuholen. Die aktuelle Version des Kriterienkatalogs weist etwa schon über 1 000 Downloads auf – wir haben viel gutes Feedback bekommen und dieses entsprechend eingearbeitet.

Wo klaffen die Interessen besonders auseinander?
Ein Beispiel ist die Einbindung von Sub-Anbietern. Das ist alltägliche Praxis bei Cloud-Dienstleistern. Laut den Regeln der DSGVO müsste der direkte Cloud-Anbieter seinen Kunden sämtliche Informationen von allen bei ihm irgendwie beteiligten IT-Firmen liefern, bis hin zur ladungsfähigen Adresse. Es ist fast unmöglich, die zum Teil hochgradig verschachtelten Cloud-Lieferketten zu dokumentieren.

Und wie soll das jetzt in Ihrer Auditor-Zertifizierung geregelt werden?
Unser Vorschlag ist: Ein Cloud-Anbieter muss nur die Daten zu seinen direkten Sub-Anbietern vorweisen und kommunizieren – und dies wiederum von den Sub-Anbietern fordern. Auch die Datenschützer in unserem Projekt unterstützen diese Lösung. So werden innerhalb der gesamten Cloud-Lieferkette die Anforderungen weitergegeben und jeder achtet darauf, dass sein Sub-Anbieter die Regeln einhält. Dann ist automatisch Transparenz da.

Warum sollten Cloud-Anbieter die Mühen und Kosten für eine weitere Zertifizierung auf sich nehmen?
Wenn das Zertifikat ermöglicht, dass Cloud-Anbieter die Datenschutzregeln technisch umsetzen können, schafft das neben Rechtssicherheit und Transparenz auch einen Wettbewerbsvorteil. Viele Anbieter haben durchaus verstanden, dass Kunden bereit sind, höhere Preise zu bezahlen, wenn sie anerkannte Zertifikate vorweisen können.

Überfordern umfangreiche Kataloge nicht kleinere Cloud-Anbieter?
Es gibt verschiedene Schutzklassen, die einen unterschiedlichen Aufwand erfordern. So kann jeder im Einzelfall entscheiden, was wirtschaftlich vertretbar ist. Gerade kleinere Cloud-Anbieter sehen Datenschutz als Chance zur Realisierung von Wettbewerbsvorteilen gegenüber den großen Marktführern.

Die Fragen stellte **Manuel Heckel**.