Aufgelöste Verantwortung

Schneller als gedacht sind Cloud-Dienste zum neuen Standard geworden. Und kaum ein Dienst darunter, der keine personenbezogenen Daten verarbeitet – mindestens die IP-Adresse der Dienstnutzer.

Doch unsere Vorstellung, dass es bei der Nutzung von Cloud-Diensten im Wesentlichen auf die Wahl eines vertrauenswürdigen Anbieters ankäme, ist zu kurz gesprungen. Denn tatsächlich bestehen viele Cloud-Lösungen inzwischen selbst wieder aus zahlreichen Einzeldiensten, die über die Cloud eingebunden werden: Ticketsystem, E-Mail-Services, Zahlungssystem, Benutzersupport, Shopsystem, Chat, Telefonie, Adressdatenbank, Tracking, Videostreaming, … – warum sollte ein Anbieter auch alle diese Dienste neu implementieren, wenn er sie günstig und in hoher Qualität hinzukaufen kann?

Das Ergebnis ist – zumindest aus der Perspektive des Datenschutzes – fatal. Die Auftragsverarbeitungsverträge der Lösungsanbieter lesen sich wie das Who-is-who einschlägiger Cloud-Dienstleister: Im Anhang finden sich oft seitenlange Tabellen mit Unterauftragnehmern. Und schaut man sich wiederum deren AV-Verträge an, finden sich dort weitere solche Listen. Viele der angeführten Unterauftragnehmer haben ihren Sitz im nichteuropäischen Ausland, und wenn nicht, dann nutzen sie selbst (oder ihre Unterauftragnehmer) nichteuropäische Dienstleister.

Dass alle Verträge in dieser Kette korrekt als Auftragsverarbeitung oder nach Standardvertragsklauseln geschlossen und die darin dokumentierten Schutzmaßnahmen sowie die Listen der Unterauftragnehmer der Wirklichkeit entsprechen, ist erfahrungsgemäß wenig wahrscheinlich – und praktisch nicht mit vertretbarem Aufwand überprüfbar. So führt schon allein eine sehr lange Vertragskette bei der verantwortlichen Stelle zu der praktischen Schwierigkeit, von einem Datenschutzvorfall bei einem nachgelagerten Dienstleister so rechtzeitig zu erfahren, dass überhaupt eine termingerechte Meldung bei der zuständigen Aufsichtsbehörde innerhalb von 72 Stunden möglich ist.

Die Idee der Auftragsverarbeitung – die juristische Fiktion eines „ausgelagerten IT-Betriebs" unter der Kontrolle der verantwortlichen Stelle – wird damit ad absurdum geführt. Denn im zerstückelten „Klein-Klein" atomarer Cloud-Dienste bleibt die Verantwortung auf der Strecke. Wie sollte eine verantwortliche Stelle, deren Sub-Sub-Sub-Auftragsverarbeiter seine Tickets in den USA verarbeiten lässt, den datenschutzkonformen Umgang mit den dort verarbeiteten personenbezogenen Daten sicherstellen?

Da werden Erinnerungen an die Finanzkrise 2008 wach. Deren eigentliche Ursache war schließlich die Marginalisierung der Ausfallrisiken von Immobilienkrediten durch deren Zerstückelung und Verteilung auf unzählige Investitionspapiere. Die Verantwortung für das jeweilige Risiko wurde damit so lange verwässert, bis davon nichts übrigblieb – und vermeintlich auch nichts vom Risiko.

Bis dieses sich durch das Platzen der Immobilienblase plötzlich äußerst wirkungsvoll manifestierte.

Dirk Fox