

Kolumne

Datenunsicherheit und ihre Grenzen



Luzi von Salis ist Geschäftsführer der von Salis Engineering GmbH und agiert als Interim-Manager, Konsultant sowie als «Business Troubleshooter» im ICT-Sektor. In seiner Kolumne kommentiert und beleuchtet er aktuelle Themen aus dem ICT-Bereich.

luzi.vonsalis@vseng.ch

Viele Firmen sind leider immer noch im Irrglauben, dass ihre Daten, bei amerikanischen Firmen in Schweizer Datacenter gehostet, sicher vor einem möglichen Zugriff seien. Die Situation ist vielfältig und wird von den US-Anbietern selbstverständlich marketingmässig schöngeredet. Microsoft (hier als exemplarisches Beispiel verwendet, denn dies gilt natürlich für alle anderen US-Cloud-Anbieter ähnlich auch) bietet seinen Microsoft-365- und Azure-Kunden an, ihre Daten in der Schweiz zu halten. Microsoft hat dazu zwei Datacenter in der Schweiz aufgebaut, eines in der Westschweiz und eines im Raum Zürich. Zudem hat das Unternehmen im Mai kommuniziert, dass es einen neuen Service lancieren will, der eine EU-Datengrenze durchsetzen soll. Anders als heute, wo die Daten für den Failover-Fall in Europa oder den USA gespiegelt werden, sollen sie dann in Europa, unter der hiesigen Datenschutz-Gesetzgebung, gespeichert bleiben. Microsoft hat sich vorgenommen, in den USA gegen eine Gesetzesverfügung Widerspruch zu erheben, wenn die Verordnung eindeutig den Gesetzen des Landes, in dem die Daten der Kunden gespeichert sind, widerspricht.

Das tönt grundsätzlich gut und ist kundenfreundlich. Es macht die Daten aber nicht sicherer und schützt sie nicht besser. Zudem ist unklar, wie sich die offiziellen Stellen der USA angesichts eines Widerspruchs von Microsoft verhalten werden.

Nun gibt es ein weiteres wichtiges US-Gesetz, das in diesem Zusammenhang oft untergeht: den US Cloud Act (Clarifying Lawful Overseas Use of Data Act). Der US Cloud Act wurde 2018 in den USA eingeführt und verpflichtet amerikanische Firmen und IT-Dienstleister bei Verdacht und einem richterlichen Befehl, US-Behörden auch dann Zugriff auf

gespeicherte Daten zu gewährleisten, wenn die Speicherung nicht in den USA erfolgt. Wenn der amerikanische Staat also will, kommt er an die Daten – ganz offiziell und ohne Umwege. Somit sind die Firmendaten der Nutzer von Azure, Microsoft 365, G-Suite, AWS und Co. also alles andere als sicher und geheim. Falls eine Firma jedoch aus US-Sicht nicht sonder-

lich negativ auffällt oder wenn sie keine Straftat nach US-Recht begeht, wird es wohl auch keinen Datenzugriff geben. Somit hält sich das Risiko also in Grenzen.

Hier mein Aufruf: Die Verantwortlichen von Firmen sollen sich sehr gut überlegen, wo und bei wem sie ihre Daten auslagern/speichern oder hosten wollen, wenn ihnen ihre Daten derart wichtig sind!

Sie sollen deshalb wachsam sein, ihre IT-Architekturen und Datenmodelle scharfsinnig planen und aufsetzen. Die Vergangenheit hat leider immer wieder gezeigt, dass kein Land und keine Regierung zu-

rückschreckt, bei Bedarf zu spionieren, Daten einzusehen und abzuhören, um sich wirtschaftliche oder politische Vorteile zu verschaffen.

«Wenn der amerikanische Staat also will, kommt er an die Daten – ganz offiziell und ohne Umwege.»

Luzi von Salis