Diplomarbeit

Informationssicherheit zwischen Fortschritt und Risiko: Juristischer Leitfaden für Entscheidungsträger

von
Michael Fehrenbach

Erstauflage

Diplomica Verlag 2014

Verlag C.H. Beck im Internet:
www.beck.de
ISBN 978 3 95820 085 2

Leseprobe

Textprobe:

Kapitel II.B.2.a, Rechtliche Aspekte aus der Sicht des Unternehmers:

Die unternehmerische Sorgfaltspflicht findet auch dann Anwendung, wenn sich die Daten des Unternehmens in einer Cloud befinden. Während eine Public Cloud für die Auslagerung sensibler Informationen ohnehin von vornherein ausscheidet, ist die Datenspeicherung in einer Private Cloud durchaus möglich. Hier sind Maßnahmen für den Schutz der Information durch die Anwendung von Kryptografie noch relativ einfach möglich. Datenschutzrechtlich geschützte Informationen, wie beispielsweise personenbezogene Daten iSd § 4 Abs. 1 DSG 2000, müssen einer bestimmbaren Person zugeordnet werden können. Genau das wird durch den Einsatz von Kryptografie erfolgreich verhindert.
Nutzt das Unternehmen die Cloud nicht nur als Speichermedium, sondern auch als Cloud-Service, so können die Daten nur dann verschlüsselt werden, wenn auch der Cloud-Anbieter die Möglichkeit zur Entschlüsselung hat. Jedenfalls müssen die Informationen unverschlüsselt in der Cloud zur Verfügung stehen, um bearbeitet werden zu können. Damit hat zumindest der Betreiber der Cloud die Möglichkeit, auf diese Daten zuzugreifen. Das Hochladen der Daten in die Cloud ist praktisch mit einer Datenübermittlung gleichzusetzen. Überlässt ein Unternehmen im Zuge des Cloud-Service einem Cloud-Betreiber Daten, so hat es sich iSd § 10 Abs. 1 DSG 2000 von der rechtmäßigen und sicheren Datenverwendung zu überzeugen.
Schon das DSG 2000 verweist auf vertragliche Vereinbarungen mit dem Anbieter. Im unternehmerischen Bereich wird im Zuge eines Security Aspect Letter (SAL) der gesamte Aufgabenkreis der Informationssicherheit detailliert geregelt. Sich von der rechtmäßigen und sicheren Datenverwendung zu überzeugen lässt dem Unternehmer weitgehend Handlungsspielraum. Jedenfalls wird man dies voraussetzen können, wenn die Verlässlichkeit des Anbieters durch staatliche oder zertifizierte Stellen nachgewiesen wurde.
Durch die Informationssicherheitskommission (ISK) werden für den Bereich zivil klassifizierter Informationen und durch das Abwehramt (AbwA) für den Bereich militärisch klassifizierter Informationen Sicherheitsunbedenklichkeitsbescheinigungen (SUB) auf Basis der Sicherheitsunbedenklichkeitsbescheinigungsverordnung (SUBV) für verlässlichkeitsgeprüfte Unternehmen ausgestellt. Im internationalen Verkehr wird unter Berücksichtigung der entsprechenden bi- oder multilateralen Verpflichtungen von Facility Security Clearances (FSC) gesprochen. Für den Unternehmer ist in Hinblick auf seinen Cloud-Anbieter von Relevanz, dass jeweils die Verlässlichkeit des Unternehmens als auch die Lagermöglichkeit für klassifizierte Informationen gegeben ist.
Unternehmen ohne SUB können sich einem Informationsicherheitsaudit unterwerfen. Mögliche Zertifizierungen erfolgen hier auf Basis der ISO 27001. Diese Audits sind ausschließlich von solchen Dienstleistern anzubieten, die iSd Akkreditierungsgesetzes 2012 dazu berechtigt sind. Gem. § 3 Abs. 1 AkkG 2012 ist der der Bundesminister für Wirtschaft, Familie und Jugend die zuständige Akkreditierungsstelle.

Verfügt der Cloud-Anbieter über kein entsprechendes Zertifikat, so obliegt die Verpflichtung zur Überprüfung dem Unternehmer selbst. Dies gestaltet sich vor allem in Hinblick auf mögliche Auslagerungen von Servern in verschiedene Staaten und die jeweils unterschiedlichen rechtlichen Regelungen ausgesprochen schwierig.
Der Unternehmer sieht sich hier einem Bedrohungsspektrum gegenüber, das von IKT-Bedrohungen, wie unsicheren Schnittstellen, über mögliche unlautere Mitarbeiter bis hin zur unsicheren Infrastruktur reicht. Gleichzeitig kann der Cloud-Anbieter nicht jedem seiner Kunden seine gesamte Sicherheitsarchitektur offenlegen, ohne diese gleichzeitig ad absurdum zu führen.