Zugriff von außen

Bundesdatenschutzgesetz versus US-Behörden

> Das deutsche Bundesdatenschutzgesetz ist eines der sichersten weltweit. Doch unter welchen Bedingungen gilt es auch in der Cloud und unter welchen nicht? Und was können Unternehmen und Dienstleister tun, um sich bestmöglich gegen den Zugriff von außen – durch US-Behörden oder andere Neugierige – zu schützen?

Spätestens seit ein US-Gericht Microsoft erfolgreich auf die Herausgabe von Daten verklagt hat, die auf Servern in Irland gespeichert waren, wird die öffentliche Diskussion um den Datenschutz in der Cloud besonders hitzig geführt. Und das zu Recht. Microsoft wehrt sich zwar noch gegen das Urteil und hat namhafte Mitstreiter um sich versammelt, doch der Fall zeigt, dass Unternehmen, die Cloud Services einsetzen wollen, einige rechtliche Details kennen sollten.

Der auf IT-Recht spezialisierte Rechtsanwalt Mike Rasch aus der Kanzlei Linnemann und Geschäftsführer der Datarea GmbH beschreibt das Vertragsverhältnis zwischen Kunde und Cloud-Service-Anbieter so: „Es handelt sich zumeist um eine klassische Auftragsdatenverarbeitung, genau wie bei der Beauftragung eines sonstigen Rechenzentrum- bzw. Hosting-Providers. Das bedeutet, der beauftragte Dienstleister verarbeitet automatisiert Daten im Namen des Auftraggebers. Der Cloud-Anbieter leistet dem Auftraggeber in einer oder mehreren Phasen der Datenerhebung, -verarbeitung oder -nutzung weisungsgebundene Unterstützung." Der Kunde schließt mit dem Cloud-Service-Anbieter eine entsprechende Vereinbarung ab, die als Rechtsgrundlage dient. Wie diese Vereinbarungen inhaltlich auszusehen haben, ist im Bundesdatenschutzgesetz (BDSG) geregelt. Sowohl für die Sicherheit der Übertragung der Daten zum Dienstleister als auch für die Nutzung durch diesen bleibt im übrigen der Kunde als „Herr der Daten" selbst verantwortlich. So weit, so gut. Doch vor dem Zugriff staatlicher Stellen scheinen die

Wie können sich Unternehmen gegen den Zugriff von außen schützen?

Daten in der Cloud dennoch nicht besonders sicher zu sein. Rechtsanwalt Mike Rasch sagt dazu: „Jeder Staat hat hoheitliche Rechte, die sich mit keiner zivilrechtlichen Vereinbarung einschränken lassen. Dazu gehört auch das Zugriffsrecht auf Daten in bestimmten Fällen, z.B. wenn eine Straftat vorliegt. Dabei ist es ganz egal, ob die anvisierten Daten in der Cloud eines Dienstleisters oder auf einem Unternehmens-PC liegen. Doch was sich US-Behörden dank des Patriot Acts erlauben dürfen, schießt deutlich über unsere Auffassung von Datenschutz hinaus."

> „Hat die US-Regierung mehr Rechte als europäische Gesetzgeber? Im Prinzip ja, zumindest wenn amerikanische Unternehmen im Spiel sind."

„Die europäische Glocke"

Innerhalb des Europäischen Wirtschaftsraumes gelten einheitliche gesetzliche Regelungen, mit diesen lässt sich ein angemessenes Datenschutzsicherheitsniveau erreichen. Für außereuropäische Anbieter gelten diese Gesetze grundsätzlich nicht. Im Klartext: Cloud-Service-Anbieter mit Geschäftssitz in den USA unterliegen den Zugriffsrechten der amerikanischen Aufsichtsbehörden – übrigens auch dann, wenn das betreffende Rechenzentrum in Deutschland oder einem anderen EU-Land steht.

Safe Habor Principles

Aus diesem Grund entwickelte das US-Handelsministerium die Safe Habor Principles. US-Unternehmen, die sich diesen freiwilligen Regeln unterwerfen, sollen damit ihren europäischen Kunden strengere Datenschutzbemühungen garantieren. Ein guter Ansatz, befindet Mike Rasch, doch das Papier allein bringt keine Rechtssicherheit. Denn die Praxis der letzten Jahre hat gezeigt, dass das US-Handelsministerium keine ernsthaften Überprüfungen durchführt und Unternehmen das Zertifikat durch die Abgabe von Eigenerklärungen – also ohne echten Nachweis – erhalten.

Binding Corporate Rules

Noch eher hilfreich sind die sogenannten Binding Corporate Rules (BCR). Dahinter verbergen sich von der EU vorgegebene Standardvertragsklauseln, zu deren Einhaltung sich der Dienstleister verpflichtet. Sie wurden ursprünglich entwickelt, um es multinationalen Konzernen zu ermöglichen, unternehmensintern personenbezogene Daten über EU-Grenzen hinweg zu transferieren und dabei trotzdem europäisches Recht einzuhalten. Doch die Vereinbarung dieser Extraregeln ist nicht immer einfach und deren Überprüfung schon gar nicht. Die Ansprüche auf die Herausgabe von bestimmten Daten lassen sich so zwar einschränken, aber nicht ausschließen.

Das Risiko minimieren

Sollten Unternehmen also besser ganz die Finger von US-Anbietern lassen? Mike Rasch fasst es so zusammen: „Wenn man die Sache datenschutzrechtlich streng formal betrachtet, muss diese Frage mit Ja beantwortet werden." Für Achim Weiß, Geschäftsführer des Berliner IaaS-Anbieters Profitbricks, ist die Standortfrage ein wichtiges Argument: „Viele Unternehmen vertrauen ihre Daten überhaupt nur dann einer externen Cloud an, wenn sie diese als sicher einstufen können. Dabei genügt es nicht, wenn der Anbieter in Deutschland ansässig ist. Wir garantieren, dass die anvertrauten Daten nur in einem vom Kunden ausgewählten Rechenzentrum verarbeitet werden. Wählt der Kunde unsere Rechenzentren in Frankfurt oder in Karlsruhe, unterliegt die gesamte Geschäftsbeziehung dem deutschen BDSG."

Unternehmen können darüber hinaus einiges dafür tun, dass die Nutzung einer Cloud nicht in einem datenschutzrechtlichen Fiasko endet. Dazu gehört vor allem eine umfangreiche Gefahrenanalyse mit Risikobewertung im Vorfeld. Welche Daten und Prozesse eignen sich unter sicherheitstechnischen Gesichtspunkten überhaupt für die Verarbeitung bei einem Dienstleister? Und was muss ein Serviceprovider bieten? Achim Weiß empfiehlt Unternehmen, sich die Notfallmatrix des Dienstleisters für den Fall der Fälle erläutern zu lassen: „Auch wir als Anbieter haben Möglichkeiten, die Daten unserer Kunden zu schützen. Wir können z.B. die freiwillige Herausgabe von Daten verweigern. Unsere Notfallmatrix stellt sicher, dass jeder Mitarbeiter weiß, was das heißt und wie er reagieren muss, falls eine behördliche Anfrage kommt." <

GESA MÜLLER