Wolkige Mythen

Für Unternehmer gehört Überwindung dazu, Daten einem IT-Dienstleister anzuvertrauen. Wenn sich dann die Versprechungen des Cloud-Betreibers als unhaltbar erweisen, macht sich Frust breit. Denn oft wird verschwiegen, wo **Gefahrenherde für Kundendaten** liegen. Betreiber der Cloud-Dienste sprechen eben nicht gerne über Lücken im Sicherheitssystem, die sie zwar kennen, für die sie aber noch keine technische Lösung gefunden haben.

Dr. Hubert Jäger

Rechtsanwalt Matthias Schwarzer von der Sozietät Weber Schwarz & Schwarzer muss als Berufsgeheimnisträger eine „ungewollte Offenbarung von Mandantendaten“ vermeiden. Diese Tatsache hatte er im Auge, als er eine Cloud-Lösung suchte, um seinen Mandanten schnell und effizient helfen zu können. Praktisch wäre für ihn, „vom iPad aus auf die Daten und im Gerichtssaal auf die relevanten Dokumente zuzugreifen“. Trotzdem wollte er die iCloud nicht nutzen. Für Berufsgeheimnisträger gelten nämlich laut § 203 Strafgesetzbuch (StGB) zur Verletzung von Privatgeheimnissen strenge Regeln hinsichtlich des Datenschutzes.

Mythos 1: Die professionell betriebene Cloud ist sicher

„Problematisch sind die Angriffe von innen – also Gefahren, die von Mitarbeitern und Administratoren des Cloud-Anbieters ausgehen“, sagt Steffen Kroschwald, wissenschaftlicher Mitarbeiter der Projektgruppe „Verfassungsverträgliche Technikgestaltung“ (provet) im Forschungszentrum für Informationstechnik-Gestaltung (ITeG) an der Universität Kassel.

Anwälte und Ärzte könnten bei der Cloud-Nutzung rechtliche Probleme bekommen, wenn sie diese zur Datenverarbeitung, etwa im Rahmen des Software-as-a-Service-Modells (SaaS), nutzen. Systemadministratoren haben aus organisatorischen Gründen die Gelegenheit, auf unverschlüsselte Daten zuzugreifen und damit „die Möglichkeit zur Kenntnisnahme“. Und diese Tatsache genügt: Für eine Offenbarung von Geheimnissen im Sinne des § 203 StGB reiche, so Kroschwald, bei digitalen Geheimnissen allein schon der „potenzielle Zugang zu den Daten“.

Dass die Applikationsserver (APS) generell einen Gefahrenherd für den Datenschutz in einem Rechenzentrum darstellen, erwähnen Anbieter ungern. Dort werden die bereits verschlüsselten Daten wieder entschlüsselt, um sie überhaupt verarbeiten zu können. Deshalb können dort mit relativ einfachen Mitteln besonders viele Informationen abgezapft werden.

Cloud-Betreiber weisen selten darauf hin, dass in den APS die Daten für Mitarbeiter des Unternehmens – Systemadministratoren – zugänglich sind. Auch wenn verschlüsselt wird. Darin liegt eine der größten Sicherheitslücken, die IT-Sicherheitsexperten bekannt sind. Meist pochen die Betreiber jedoch darauf, dass das Rechenzentrum trotzdem „sicher“ sei, weil der Zugang zu den Daten mit organisatorischen Maßnahmen erschwert wird.

So zum Beispiel die Telekom: Wer illegal auf De-Mail zugreifen will, muss nach Aussage der Telekom drei verschiedene Administratoren bestechen. Doch die Erfahrung hat gezeigt, dass Insider meist Wege finden, die organisatorischen Maßnahmen zu umgehen – oder Mitarbeiter Fehler machen. Davon zeugen viele der in letzter Zeit bekannt gewordenen Datenpannen.

Philipp Dyckerhoff, Geschäftsführer des Finanzdienstleisters Pecunia Consult, berät bei speziellen Fragestellungen, „die sich aus einem Leben zwischen Spanien und Deutschland ergeben“. Darunter fallen Altersvorsorge, Immobilienfinanzierung und Vermögensaufbau – Themen also, die mit vertraulichen und personenbezogenen Daten verbunden sind. Deshalb kann Dyckerhoff sich nicht leisten, mit den Informationen nachlässig umzugehen.

Sein Hauptkritikpunkt an Cloud-Lösungen ist, „dass Datenschutz bei grenzüberschreitender Kommunikation – auch innerhalb der Europäischen Union – nur eingeschränkt gewahrt und von verschiedenen Seiten intensiv beobachtet wird“. Wie so viele hat er lange Zeit einfach per E-Mail, oft sogar unverschlüsselt, kommuniziert. Bis ihm klar geworden war, dass er eine sichere Lösung einsetzen musste. Aber welche?

Mythos 2: Wenn Daten nicht mehr sichtbar sind, wurden sie gelöscht

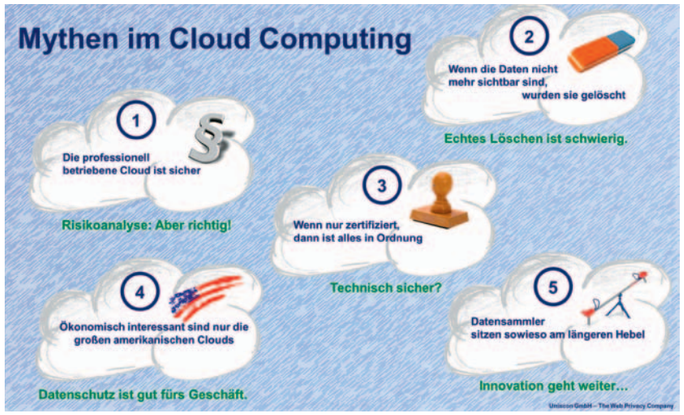
Elke Garreis, Steuer- und Fachberaterin für internationales Steuerrecht, stellt sich dieselbe Frage, aber aus einem anderen Grund: „Ich bin mir bei vielen Online-Anwendungen einfach nicht sicher, ob die Daten, die ich lösche, auch rückstandslos gelöscht werden“. Das fordern zwar Datenschützer, doch auch hierbei verschweigen Cloud-Anbieter die volle Wahrheit.

DER AUTOR

Dr. Hubert Jäger
Mitgeschäftsführer der Uniscon GmbH in München

Zertifikate sind keine Garantie dafür, dass die Daten in der Cloud wirklich umfassend geschützt sind.

Fünf Mythen bestimmen die gängige Einschätzung zur Cloud-Sicherheit. Doch was steckt dahinter?



Sie löschen im laufenden System, die Daten in den Backups allerdings löschen sie oft nicht. Das würde einen zu hohen Aufwand bedeuten. Dazu verschweigen sie, dass sie für die Daten im Backup Schlüssel besitzen. Das dafür verwendete Verschlüsselungsverfahren veraltet mit der Zeit, sodass die Backup-Datenbanken eine zusätzliche Sicherheitslücke darstellen können.

Mythos 3: Zertifikate garantieren Sicherheit

Manche Anwender denken, ein Online-Dienst, der nur diverse Zertifikate ausweist, würde bereits alle Sicherheitsaspekte abdecken. Tatsächlich kommt es darauf an, welche Maßstäbe bei der Zertifizierung wirklich angelegt werden. Werden nur ein paar Grundregeln eingehalten oder allein die Rechtskonformität zertifiziert?

Oder werden – basierend auf einer sorgfältigen Risikoanalyse – die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen geprüft und zertifiziert? Letzteres erfolgt beispielsweise, wenn das Bundesamt für Sicherheit in der Informationstechnik (BSI) das IT-Grundschutz-Zertifikat vergibt.

Oft zeigt die Risikoanalyse, dass es nicht reicht, die Vertraulichkeit der Kommunikation allein mit organisatorischen Maßnahmen abzusichern, sondern mit besonders wirksamen technischen Maßnahmen gearbeitet werden muss, um die Risiken der Industriespionage hinreichend zu minimieren. Dafür würde Dyckerhoff im Speziellen einen Kommunikationsdienst benötigen, der nicht nur die Inhalte, sondern dazu noch die Verbindungsdaten schützt.

In Gesprächen mit Detlef Eggert, Chief Information Security Officer (CISO) bei einer Wirtschaftsprüfungsgesellschaft, fällt oft das Wort „Mandantenfähigkeit“, wenn von einer Cloud-Anwendung die Rede ist. Er meint damit, dass sich auf demselben Server oder demselben Software-System die Daten mehrerer Mandanten – Kunden oder Auftraggeber – befinden und diese im System getrennt bleiben müssen.

Bei einer nicht ausreichend abgesicherten Mandantentrennung besteht die Gefahr, dass neben Datendieben auch harmlose Cloud-Nutzer unautorisiert Daten einsehen oder manipulieren können. In Wirtschaftsprüferkreisen sind starke Bedenken vorhanden, dass Daten in gemeinsam genutzten Datenbanken oft nicht logisch getrennt und verwaltet werden.

„In einer Public Cloud ist dieses Risiko eben höher“, sagt Dieter Spillmann, ehemaliger Direktor für Software-Entwicklung bei Fujitsu und Cloud-Sicherheitsexperte, „weil durch Virtualisierung keine kryptografische oder gar physikalische Trennung der Daten unterschiedlicher Mandanten mehr erfolgt.“

Die Sicherheitsrisiken beim Cloud Computing sind vielschichtig.

Mythos 4: Ökonomisch interessant sind nur die großen US-Clouds

Für jede Art der Verarbeitung personenbezogener Daten gilt, dass die Daten, die zu unterschiedlichen Zwecken erhoben wurden, nicht einfach gemischt und gemeinsam verarbeitet werden dürfen. Privatheit, so Spillmann, wird „wirkungsvoll und gleichzeitig kostengünstig geschützt, wenn sie bereits bei Design und Entwicklung mitgeplant wird“. Dazu sind viele technische Werkzeuge notwendig: von langfristig sicherer Kryptographie über Methoden für die anonyme Nutzung von Diensten bis zu physikalischen Maßnahmen. „Das kann besser gemacht werden als dies durch die großen amerikanischen Clouds gegenwärtig erfolgt,“ resümiert er.

Der Weg zu vertrauenswürdigem Cloud Computing muss über den Schutz der Inhalte und der Verbindungsdaten führen und zwar Angriffen gegenüber, die von außen und innen ausgeführt werden. Dabei gilt es, die Daten in der Datenbank, in den Anwendungsservern, beim Transfer und an allen Schnittstellen gleichwertig abzusichern.

Mancher Private-Cloud-Anbieter versucht die Fragen der Rechtskonformität (Compliance) zu lösen, indem alle, die zu dieser Cloud Zugang haben, Gehilfenstatus nach § 203 Abs. 3 Satz 2 StGB besitzen – rechtlich also dem Kanzleipersonal oder Arzthelfer gleichgestellt werden. Wer sich eine solche aber nicht leisten kann, musste bisher als sicherheitsbewusster Anwender Ende-zu-Ende verschlüsseln und sicherstellen, dass nur er im Besitz des Schlüssels ist.

Für die Datatree AG war diese Praxis schon seit Jahren selbstverständlich, aber zufrieden war man dort mit der Lösung bei Weitem nicht. „Das Problem, dass teilweise die Leute das Passwort vergessen oder Daten intern einfach weitergeleitet haben“, erklärt Vorstand Bernd Fuhlert, „führte zu einer Inflation von Passwörtern, die mit erheblichem Verwaltungsaufwand einherging“. Sein Fazit: „Sicherheitslösungen können ihre Wirkung nur entfalten, wenn sie von Anfang an bedienerfreundlich angelegt sind.“

Als Compliance-Dienstleister kümmert sich Datatree um die Sicherheitsstandards in Firmen. Die Mitarbeiter prüfen, analysieren und empfehlen Strategien oder Lösungen. Sie wissen: Diese in den Unternehmen tatsächlich umzusetzen, erweist sich oft als schwierig. Sicherheit muss mit Bedienerfreundlichkeit einhergehen – und die findet sich nur bei wenigen Sicherheitslösungen.

Mythos 5: Datensammler sitzen sowieso am längeren Hebel

Mit dem Trusted-Cloud-Programm startete das Bundesministerium für Wirtschaft und Technologie (BMWi) eine Initiative, um dieses Dilemma zu lösen. Forschungs- und Entwicklungsaktivitäten zu effizienten und innovativen Cloud-Strukturen sowie cloudbasierten Diensten werden gefördert. Das Sicherheitskonzept der Sealed-Cloud-Technologie des Münchner Unternehmens Uniscon setzte sich im Bereich „Basistechnologie“ gegen 116 Konsortien für eine Förderung durch.

Die Technologie versiegelt das Datenzentrum in erster Linie durch technische, für den Administrator unumgängliche Maßnahmen und schließt damit den Unsicherheitsfaktor „Mensch“ praktisch aus. Im Rahmen der Initiative wird die Sealed-Cloud-Technologie als Basistechnologie weiterentwickelt, die Cloud-Anbietern ermöglichen wird, ihren Kunden bedienerfreundliche und wirklich sichere Dienste anbieten zu können.

Mit der Technologie wird der Ansatz verfolgt, Ressourcen zu sparen und vorhandene technische Komponenten wie Schlüsselverteilung und vorsorgliche Datenlöschungen (Data Clean-Up) miteinander zu verbinden. Die Sealed Cloud ist aber nicht nur eine kryptografische Lösung, sondern kombiniert verschiedene technische Maßnahmen. Die Daten in der Cloud werden so rechtskonform und sicher verarbeitet und gespeichert. Sie ermöglicht damit Berufsgeheimnisträgern die Nutzung von Anwendungen als Cloud-Dienst, denn sie ist zurzeit als einzige Public-Cloud-Lösung rechtskonform nach § 203 StGB und Bundesdatenschutzgesetz (BDSG).

[rm]

STATEMENT

Matthias Kunisch
Geschäftsführer der forcont business technology gmbh

Kritische Fragen sind Pflicht

„Cloud Computing hat mittlerweile eine technologische Reife erlangt, die es Unternehmen in vielen Fällen ermöglicht, ihre Geschäftsprozesse sehr kosteneffizient zu optimieren und zu flexibilisieren. Die Nutzer müssen sich aber darüber im Klaren sein, dass es, ganz genauso wie bei lokalen Installationen, keine hundertprozentige Verfügbarkeit oder Sicherheit gibt.

Da man den Betrieb der Software sowie das Management von Daten an Dritte abgibt und eine fremde Software gemeinsam mit anderen teilt, sind kritische Fragen an den Cloud-Anbieter nicht nur berechtigt, sondern sogar nötig. Fragen über den Speicherort, die Zertifizierung des Rechenzentrums, die Einhaltung geltender Datenschutzgesetze, Aspekte wie Hochverfügbarkeit, Sicherheitsstandards und Schnittstellen sowie die Möglichkeit, eigene Daten aus der Cloud zu migrieren oder via Self-Services die Leistung individuell anzupassen.

Wie auch bei herkömmlichen IT-Projekten muss ein Nutzer Verantwortung übernehmen und von seinem Anbieter Antworten einfordern. In jedem Business gibt es Angebote und Anbieter unterschiedlicher Güte. Die richtige Wahl liegt letztlich beim Kunden. Das Thema Verfügbarkeit ist ein Sonderfall. Viele Rechenzentren bieten 99,9 Prozent. Das stimmt auch meist, ist aber nicht gleichbedeutend mit der Verfügbarkeit des Dienstes. Die hängt auch von der Softwarepflege, der Netzauslastung, der vorhandenen Bandbreite und anderen Dienstleistungen ab. Auch dessen muss man sich bewusst sein.“