Datenschutz in der Cloud

Lassen sich Privatsphäre und Daten-Hosting miteinander in Einklang bringen?

Kai-Oliver Detken

Immer mehr Unternehmen überlegen, ihre Daten einem Cloud-Anbieter anzuvertrauen. Schließlich spart man dadurch Rechenzentrumskapazität, Klimaanlagen und Stromverbrauch ein. Auch der Mangel an IT-Fachpersonal kann durch Cloud-Dienste abgemildert werden. Warum also keine Auslagerung? Aber Vorsicht: Es lauern Datenschutzverletzungen, zu langsame Internetanbindungen und eine Erhöhung der Ausfallwahrscheinlichkeit. Dieser Artikel soll daher den Trend in die Cloud kritisch beleuchten.

Prof. Dr.-Ing. Kai-Oliver Detken ist Geschäftsführer der Decoit GmbH in Bremen

Deutschland hinkt in Sachen Cloud Computing dem internationalen Vergleich nach wie vor hinterher. Während man in anderen Ländern sehr viel offener mit diesem Thema umgeht, standen in Deutschland jahrelang die Risiken des Einsatzes im Vordergrund, die sich durch die Datenschutzgrundverordnung (DSGVO) seit Mai 2018 noch vergrößert haben dürften. Laut Statistik von Bitkom und KPMG hat sich die Nutzung von Cloud-Diensten aber inzwischen etabliert. So setzen zwei Drittel der Unternehmen in Deutschland inzwischen auf Rechenleistung aus der Cloud und jedes fünfte Unternehmen plant deren Einsatz. Bei Großunternehmen sind die Zahlen noch eindeutiger: Hier nutzen bereits über 80 % ihre Dienste aus der Wolke.

Doch wie sieht es mit der Einhaltung von Datenschutzrechten aus? Zuerst einmal muss die Frage nach der Art des Cloud-Computing gestellt werden.

Cloud-Varianten

Der Begriff Cloud Computing hat inzwischen viele Facetten und beinhaltet unterschiedliche Nutzungsvarianten. Dabei muss man sich immer vor Augen halten, dass es sich hierbei nicht um eine neue Technik handelt, sondern um eine spezielle Nutzung vorhandener IT-Services. Denn Cloud-Computing basiert in erster Linie darauf, eine IT-Infrastruktur, die Speicherplatz, Rechenleistung und Anwendungssoftware beinhaltet, als Dienstleistung verfügbar zu machen. Nichts anderes leistet das interne Rechenzentrum einer Firma, das von eigenen IT-Mitarbeitern verwaltet wird, für das anstellende Unternehmen. Bietet man dieses Rechenzentrum über das Internet auch noch anderen Firmen an, entsteht ein neues Geschäftsmodell. Dabei erfolgen Angebot und Nutzung der IT-Dienstleistung ausschließlich durch technische Schnittstellen und Protokolle, z.B. über einen Webbrowser. Die IT-Dienstleistung bzw. Servicemodelle lassen sich dabei unterscheiden zwischen Infrastruktur, Plattform und Software:

- Software as a Service (SaaS): Nutzungszugang von Softwaresammlungen und Anwendungsprogrammen; SaaS-Provider bieten spezielle Softwarevarianten an, die auf ihrer IT-Infrastruktur laufen;
- Platform as a Service (PaaS): Nutzungszugang von Programmierungs- oder Laufzeitumgebungen mit flexiblen, dynamisch anpassbaren Rechen- und Datenkapazitäten; PaaS ermöglicht die Nutzung oder Entwicklung eigener Softwareanwendungen innerhalb einer Softwareumgebung, die vom Provider bereitgestellt und unterhalten wird;
- Infrastructure as a Service (IaaS): Nutzungszugang zu virtualisierten Computerressourcen, wie Rechnern, Netzen und Speicher; mit IaaS kann der Nutzer eigene virtuelle Computer-Cluster aufbauen und ist selbst für Installation, Konfiguration und Betrieb verantwortlich.

Die dargestellten Cloud-Varianten können wiederum durch unterschiedliche Liefermodelle zum Kunden transportiert werden (*Bild*):

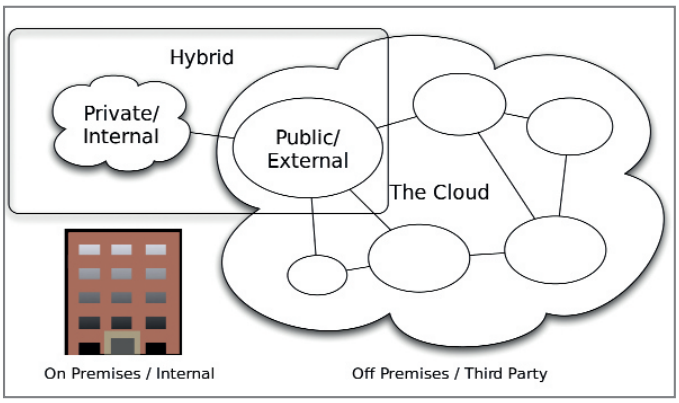
- Public Cloud: bietet Zugang zu einer abstrahierten IT-Infrastruktur für die Öffentlichkeit über das Internet; die Bezahlung erfolgt meist über die tatsächliche Nutzung, der Kunde muss kein Kapital in eigene Rechner- und IT-Infrastruktur investieren; der Zugang sollte abgesichert sein, damit kein anderes Unternehmen darauf zugreifen kann;
- Private Cloud: wird nur durch die eigene Organisation betrieben; das Hosting und Verwalten der Cloud-

Plattform kann durch interne Fachkräfte, aber auch externe IT-Dienstleister erfolgen; der Sicherheitsgrad ist hoch, da normalerweise kein unverschlüsselter Zugang von außen gewährt wird;
- Hybrid Cloud: bietet den kombinierten Zugang zur abstrahierten IT-Infrastruktur, der aus Public und Private Cloud besteht; je nach Anforderung des Unternehmens werden Dienste in der öffentlichen oder privaten Cloud gehalten; in der privaten Cloud werden meistens sensible Anwendungen (z.B. ERP-Systeme) betrieben;
- Community Cloud: bietet Zugang zu einer Public Cloud, allerdings nur für einen kleineren Nutzerkreis (z.B. Forschungsgemeinschaften, Kooperationspartner); sollte ausreichend gesichert werden, um keine Innovationen oder Patente an Dritte zu verlieren.

Von daher kann man im Grunde die Cloud-Nutzung heute jedem Unternehmen unterstellen, je nachdem wie man diese definiert.

Darstellung von Cloud-Liefermodellen

(Quelle: Sam Johnson: Diagram Showing Three Main Types of Cloud Computing (Public/External, Hybrid, Private/Internal). Creative Commons Attribution-Share Alike 3.0 Unported License, 4th of March 2009)



DSGVO in der Cloud

Durch die zunehmende Virtualisierung wird im ersten Schritt in den Unternehmen aufgrund der besseren Ressourcennutzung über eine private Cloud nachgedacht bzw. diese umgesetzt. Dadurch lassen sich bereits Kosten sparen, indem weniger Serverhardware angeschafft werden muss und die Stromkosten reduziert werden. Im zweiten Schritt wird oftmals der Ruf nach der Public Cloud größer, denn dadurch können weitere Einsparmaßnahmen, wie bei der IT-Administration/-Verwaltung, vorgenommen werden. Allerdings ist man dabei auch von einer leistungsstarken Internetanbindung abhängig. Fällt diese aus, kann das ganze Unternehmen nicht mehr arbeiten. Das wird oft besonders schmerzhaft, wenn man sich auf TK-Anlagen in der Cloud verlässt. In diesem Fehlerfall wäre man nicht nur von außen nicht mehr erreichbar, sondern könnte auch keine internen Gespräche führen.

Der Trend zur Public Cloud wird in Deutschland hauptsächlich von der Sicherheitsdiskussion bestimmt, denn zwei Drittel der Unternehmen fürchten den unberechtigten Zugriff auf sensible Unternehmensdaten. Mehr als die Hälfte haben die Befürchtung, dass ihre Daten verloren gehen oder sehen eine unklare Rechtslage. Dieser Umstand wurde durch die Einführung der DSGVO noch verstärkt. So ist momentan auch die Einhaltung der DSGVO das Hauptkriterium bei der Cloud-Nutzung.

Daher muss ein Cloud-Anbieter die folgenden beiden Kriterien in jedem Fall unterstützen:
- Datensicherheit: die technische Datensicherheit ist die Basis für eine Sicherstellung des Datenschutzes und kann nur durch die verwendeten Techniken und Anwendungen des Anbieters erreicht werden. Grundsätzlich bietet dabei ein internes IT-System eine höhere Sicherheit, da der Aufwand höher ist, um ein öffentliches Cloud-System abzusichern. Man kann aber ein öffentliches Cloud-System deshalb nicht grundsätzlich als unsicherer bezeichnen.
- Datenschutz: Nach dem Europäischen Gerichtshof dürfen nur eingeschränkt personenbezogene Daten in die USA gelangen. Daran ändert auch das Safe-Harbor-Abkommen nichts, da dies im Oktober 2015 vom Europäischen Gerichtshof für ungültig erklärt wurde. Dies wird bei der Planung oft nicht berücksichtigt, da derzeit ca. 90 % aller Cloud-Computing-Infrastrukturen sich in den USA befinden oder zumindest dessen Hoheit unterstehen.

Die DSGVO hat die Anforderungen an den Datenschutz weiter angehoben, da sie sich nicht nur mehr mit der Frage beschäftigt, ob eine Verarbeitung personenbezogener Daten zulässig ist, sondern eine umfassende Dokumentations-, Organisations- und Transparenzpflicht vorsieht. Aus Sicht des Cloud-Computing sind dies allerdings Pflichten des Unternehmens und nicht cloudspezifische Anforderungen. Das heißt, der Cloud-Provider muss für sein Unternehmen die DSGVO-Pflichten erfüllen, ist aber nicht für die Erfüllung dieser Pflichten für seine Auftraggeber zuständig. Das bedeutet aber auch, wenn er die DSGVO für seine eigene Organisation nicht ausreichend umgesetzt hat, kann ihm ein potenzieller Auftraggeber ebenfalls nicht beim Datenaustausch vertrauen. Es ist daher immer wichtiger für Cloud-Provider, dass sie sich als DSGVO-konform ausgeben können.

Für Cloud-Provider sind folgende DSGVO-Neuerungen zu beachten:
- Kein Bestandsschutz: Ab dem 25. Mai 2018 gilt die DSGVO bei der Verarbeitung personenbezogener Daten, auch für Altverträge.
- Auftragsverarbeitung: Die Auftragsdatenverarbeitung (ADV) heißt unter der DSGVO nun Auftragsverarbeitung (AV). Grundsätzlich bleibt es aber dabei, dass die Auftragsverarbeitung die datenschutzrechtliche Grundlage für die Nutzung von Cloud-Services ist. Auch die Kernkomponenten einer Auftragsverarbeitung bleiben: Weisungsgebundenheit gegenüber dem Auftraggeber, eine Vereinbarung mit Inhalten nach Maßgabe der datenschutzrechtlichen Regelungen über die Auftragsverarbeitung und Dokumentation der Vereinbarung.
- Datenschutz durch Technikgestaltung: Die Pflicht zum Datenschutz

durch Technikgestaltung und datenschutzrechtliche Voreinstellung trifft den Auftraggeber. Da die Umsetzung dieser Pflicht nicht durch die Servicenutzung allein sichergestellt werden kann, wird diese Anforderung an den Cloud-Provider weitergegeben.

- Verzeichnis von Verarbeitungskategorien: Für den Auftragsverarbeiter muss ein Verzeichnis zu seinen Kategorien von Verarbeitungstätigkeiten geführt werden. Dieses Verzeichnis ist einer Aufsichtsbehörde jederzeit auf Verlangen vorzulegen. Hierbei sollte die Geheimhaltungspflicht mitberücksichtigt werden.
- Meldung der DSGVO-Verletzung: Die Verletzung der Sicherheit zu Vernichtung, Verlust, Veränderung oder unbefugten Offenlegung von personenbezogenen Daten ist dem Auftraggeber und/oder einer Aufsichtsbehörde (je nach Auflage) zu melden. Davon sind besonders Kritis-Unternehmen betroffen.
- Ausweitung der Haftung: Bisher waren Ansprüche bei Haftungsfragen von Betroffenen gegen den Auftraggeber geltend zu machen. Nach DSGVO kann nun aber der Auftragsverarbeiter direkt verklagt werden. Er haftet also sowohl gegenüber der betroffenen Person auch als für einen Fehler des Auftraggebers. Dies gilt allerdings nicht ohne Einschränkungen.
- Sicherheit der Verarbeitung: Die Sicherheit der Verarbeitung geht in der DSGVO klar über das bisherige Datenschutzrecht hinaus. Sie ist dabei nicht unbedingt mit der IT-Sicherheit gleichzusetzen, denn die Schutzziele können sich sogar entgegenstehen. Die DSGVO besitzt einen eigenen Kriterienkatalog für den Schutz personenbezogener Daten, der dokumentiert und an dem der Service ausgerichtet werden muss.
- Mittelbare Erfüllung von Pflichten des Auftraggebers: Erhebliche Auswirkungen werden die Regelungen haben, die nicht direkt den Auftragsverarbeiter in die Pflicht nehmen, sondern seinen Auftraggeber. Denn den Auftraggeber als Verantwortlichen treffen die umfassenden Dokumentations-, Organisations- und Transparenzpflichten. In diese Pflichten wird der Auftraggeber den Cloud-Provider entweder einbinden oder gar diese Pflichten auslagern wollen.

Der Cloud-Provider muss daher für jeden Service spezifisch festlegen, wie er mit der Datenschutzsituation umgehen möchte und was bei ihm alles mit zum Service gehört. Zudem wurden mögliche Bußgelder bei Verstößen gegen die DSGVO stark angehoben (theoretisch bis zu 10 Mio. € oder bis zu 2 % des erzielten Jahresumsatzes). Diese Auflagen machen es daher nicht einfacher, als Cloud-Anbieter in Deutschland zu bestehen.

Privatsphäre in der Cloud

Ein Risiko ist die Absicherung der Anwendungsdaten beim Zugriff auf den Cloud-Speicher. Dies wird heute durch den Einsatz von SSL-/TLS-Verschlüsselung größtenteils behoben. Wesentlich größer wird allerdings das Risiko von Kunden eingeschätzt, dass andere Provider-Mandanten oder der Provider selbst auf die eigenen Daten zugreifen könnten.

Hier hat sich das Konzept der Sealed Cloud bewährt. Die Schlüssel für diesen Dienst werden dynamisch für jeden Datensatz generiert und lösen über ein Trusted Platform Module (TPM-Chip) eine sog. Chain of Trust aus. Erst nach mehreren Schritten ist es dann möglich, auf die eigenen Daten zuzugreifen. Neben den Inhalten sind in diesem patentierten Verfahren auch die Verbindungs- oder Metadaten vor dem Zugriff durch den Provider geschützt. Es kann dadurch eine geordnete Sicherung und ggf. Löschung unverschlüsselter Daten erfolgen, bevor ein Administrator einen Zugriff auf den Speicher erhält.

Die Sealed Cloud ist inzwischen eine patentierte Basistechnik, mit der Systeme in Rechenzentren so gesichert werden können, dass die über sie laufenden Daten auch für den Betreiber unzugänglich sind. Unter anderem hat das Fraunhofer AISEC in München diese Technik in einem Forschungskooperationsprojekt entwickelt. Seit Ende 2014 existieren Schnittstellen für Cloud-Anwendungen in diversen Bereichen. Ziel war es, die DSGVO-Prinzipien „Privacy by Design“ und „Privacy by Default“ zu unterstützen und eine versiegelte Infrastruktur für Cloud-Computing zu schaffen. Dies bedeutet letztendlich, dass der Betreiber der Infrastruktur grundsätzlich keine Möglichkeit hat, auf unverschlüsselte Daten (Inhalte, Metadaten) zuzugreifen – selbst während der Verarbeitung von Nutzerdaten. Die Deutsche Telekom nutzt u.a. diesen Ansatz bereits in ihrer eigenen „versiegelten Cloud“.

Fazit

Die gesetzlichen Anforderungen an Cloud-Provider haben sich gerade in Deutschland sichtlich erhöht. So verlangt die DSGVO den Providern einiges ab, was teilweise nicht alles eingehalten werden kann. Gerade Provider aus den USA tun sich hier schwer, weil sie mit anderen Vorgaben in Zielkonflikt geraten. Hinzu kommt, dass Cloud-Provider aus unterschiedlichen Beweggründen per se Daten über ihre Mandanten sammeln. Je nach Anbieter und Nutzungsbedingungen sowie Wichtigkeit und Sensibilität der eigenen Daten hat man daher die Wahl zwischen höheren Kosten für weniger Speicherplatz zugunsten eines Anbieters, der sich an deutsche Datenschutzbestimmungen gebunden fühlt, sowie geringere Kosten für viel Speicherplatz bei einem Unternehmen, dessen Firmensitz sich im außereuropäischen Ausland befindet und bei dem die Datensammelleidenschaft größer ist.

Um sich nicht auf den Cloud-Provider verlassen zu müssen und sich selbst hinsichtlich der DSGVO abzusichern, sind daher verschlüsselte Datencontainer in einer Cloud anzuraten. Denn für die Einhaltung der DSGVO und die eigenen Daten ist jedes Unternehmen noch immer selbst verantwortlich. Daher empfehlen sich Lösungen wie die Sealed Cloud, mit deren Hilfe das einstige Sicherheitsdilemma überwunden werden kann. Man sollte daher darauf achten, ob der gewählte Cloud Provider DSGVO-konform handelt und entsprechende technische Sicherheitsverfahren anbietet. *(bk)*