Cloud Computing

Begriff

Cloud Computing bedeutet, IT-Ressourcen wie Rechenleistung, Speicherkapazität und Software nicht mehr selbst vorzuhalten, sondern flexibel und bedarfsabhängig von Dienstleistern über das Internet zu beziehen.

Zu den Cloud-Leistungen zählen die Bereitstellung von Anwendungsprogrammen (Software as a Service), von Speicher- oder Rechnerkapazitäten (Infrastructure as a Service) sowie von Entwicklungsumgebungen (Platform as a Service) über das Internet.

Vielen Unternehmen ist nicht bewusst, dass sie bereits Cloud-Dienste nutzen. Dabei sind unter den verwendeten Diensten durchaus datenkritische Anwendungen, wie zum Beispiel die Online-Speicherung von betrieblichen Dokumenten und → **E-Mails**.

Ein Unternehmen, das Cloud Computing nutzt und seine Daten extern speichern und verarbeiten lässt, bleibt in der Verantwortung für den Datenschutz **(→ Auftragsverarbeitung)**.

Gesetze, Vorschriften und Rechtsprechung

- Bei Cloud Computing handelt es sich in aller Regel um → **Auftragsverarbeitung** (Art. 28 DSGVO). Es muss insbesondere ein angemessenes Datenschutzniveau in der Cloud gewährleistet und nachgewiesen sein.

- Die Datenschutzbeauftragten des Bundes und der Länder bieten eine Orientierungshilfe Cloud Computing. Die Orientierungshilfe richtet sich an Entscheidungsträger, an betriebliche und behördliche Datenschutzbeauftragte sowie an IT-Verantwortliche. Sie soll den datenschutzgerechten Einsatz dieser Technologie fördern. http://www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OHCloudComputing.pdf

Risiken einer Cloud-Nutzung

Als Cloud-Risiken werden laut ENISA (European Network and Information Security Agency) gesehen:

- möglicher Kontrollverlust über die eigenen Daten
- Lokalisierung der Daten und entsprechende Zugriffskontrolle **(→ Zugangs- und Zugriffsschutz)** erschwert oder kaum möglich
- mangelnde Trennung zwischen den einzelnen Kundenbereichen
- Schwierigkeiten, die gesetzlichen Compliance-Vorgaben nachweisbar umzusetzen
- kaum oder keine Möglichkeit, selbst ein Audit **(→ Technik-Audit)** beim Cloud-Anbieter zu machen (wie bei → **Auftragsverarbeitung** nach Art. 28 Datenschutz-Grundverordnung (DSGVO) gefordert)
- Schwierigkeiten, eine sichere Datenlöschung **(→ Löschen)** zu gewährleisten
- möglicher Datenmissbrauch durch Cloud-Anbieter oder seine Subunternehmer

Anforderungen an Datensicherheit des Cloud-Anbieters

Der Schutzbedarf der Daten **(→ Schutzbedarfsfeststellung)** entscheidet über die Sicherheitsanforderungen, die an den Dienstleister zu stellen sind, aber auch über die Art der Cloud, die genutzt werden sollte. Besonders sensible Daten sollten nicht in einer Cloud verarbeitet werden, die für mehrere Unternehmen gemeinsam betrieben wird (Public Cloud), sondern in einer speziell für das eigene Unternehmen vorgehaltenen Cloud (Private Cloud).

Zu den notwendigen Vorgaben für Cloud-Anbieter gibt es mehrere Empfehlungen der Aufsichtsbehörden für den Datenschutz und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) **(→ BSI-Standard)**:

- Dazu gehört zum Beispiel, dass die Nutzer bei Cloud Computing darauf achten sollten, dass ihr Dienstleister über ein zertifiziertes Sicherheitsmanagement **(→ IT-Sicherheitsmanagement)** verfügt und dass das externe Rechenzentrum ausfallsicher und gegen Angriffe von Hackern und Industriespionen geschützt ist.
- Unerlaubte Zugriffe auf die Daten müssen ausgeschlossen werden können. Deshalb ist eine sichere → **Verschlüsselung** bei der Datenübertragung ins Internet und bei der externen Datenspeicherung besonders wichtig, ebenso die Verwendung von Passwörtern, die sich nicht ohne größere Anstrengungen knacken lassen.
- Nicht zuletzt benötigt der Anwender von Cloud Computing Transparenz über den Standort des Rechenzentrums, Berichte über die durchgeführten Leistungen und eine Möglichkeit, die Datenschutzmaßnahmen des Dienstleisters selbst zu prüfen.

- Das BSI hat einen Mindeststandard **(→ BSI-Standard)** zur Nutzung externer Cloud-Dienste veröffentlicht. Der Mindeststandard betrachtet neben der vorgelagerten Datenkategorisierung und Risikoanalyse den gesamten Lebenszyklus einer Cloud-Nutzung von der Beschaffungs- über die Einsatz- bis hin zur Beendigungsphase und stellt für jede dieser Phasen Sicherheitsanforderungen auf. Dabei wird ein Schwerpunkt insbesondere auf die Verknüpfung mit den Basisanforderungen des Anforderungskatalogs Cloud Computing des BSI (C5) gesetzt.
- Der Anforderungskatalog C5 adressiert vorrangig Cloud-Anbieter und definiert mit den dortigen Basisanforderungen bereits ein Niveau der Informationssicherheit von Cloud-Diensten, das aus Sicht des BSI nicht unterschritten werden sollte.

Die Aufsichtsbehörden für den Datenschutz haben zudem auf einige Punkte besonders hingewiesen, unter welchen Rahmenbedingungen der Einsatz von Cloud-Diensten aus den USA datenschutzkonform möglich ist. Danach muss neben der → **Verschlüsselung** der Daten und der Unterbindung von Telemetriedaten mit Bezug auf personenbezogene Daten auch ein Vertrag zur → **Auftragsverarbeitung** geschlossen werden.

Durch den U.S.-amerikanischen Cloud-Act versucht die USA, sich Zugriff auf Daten von Personen aus der EU zu verschaffen, in dem sie europäische Unternehmen verpflichtet, ihnen Daten zu übermitteln, so die Aufsichtsbehörden. Dieses Vorgehen wird von europäischen Datenschützer sehr kritisch beurteilt.