Information des DIN-Verbraucherrates

DIGITALE SICHERHEIT – CLOUD COMPUTING

Dieses Papier soll aufzeigen, welche Aspekte des Themas Cloud Computing in der Normung betrachtet werden und welche weiteren Aspekte des Cloud Computing aus Verbrauchersicht relevant sind.

Cloud Dienstleistungen - Begriffsklärung

Die Cloud bezeichnet z.B. eine IT-Infrastruktur, die über das Internet verfügbar gemacht wird. Technisch ist es eine IT Infrastruktur, die über ein Rechnernetz zur Verfügung steht, ohne die Notwendigkeit einer lokalen Installation. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich durch technische Schnittstellen und Protokolle, etwa mittels eines Webbrowsers.

Um sicherzustellen, dass die Begriffe im Bereich Cloud Computing transparent verwendet werden können, wurde 2016 die Norm DIN ISO/IEC 17788 "Informationstechnik - Cloud Computing - Übersicht und Vokabular" veröffentlicht. Diese internationale Terminologienorm wird zur Zeit überarbeitet und aktualisiert. Auch die 2017 veröffentlichte Norm DIN ISO/IEC 17789 "Informationstechnik - Cloud Computing – Referenzarchitektur" dient der Transparenz.

Die Bandbreite der Dienstleistungen, die im Rahmen des Cloud Computing angeboten werden, geht über alle Bereiche der Informationstechnik hinweg. Dies umfasst unter anderem:

- IT-Infrastrukturdienstleistungen für virtualisierte Computerhardware-Ressourcen wie Rechner, Netze und Speicher (Infrastructure-as-a-service = IaaS),
- spezifische Plattformen, die Programmierungs- oder Laufzeitumgebungen mit flexiblen, dynamisch anpassbaren Rechen- und Datenkapazitäten bereitstellen (Platform-as-a Service = PaaS), oder
- Zugang zu unterschiedlichster Software als Anwendungssoftware (Software-as-a-Service = SaaS).

Es gibt unterschiedliche Cloud Liefermodelle. Besonders zu erwähnen sind die öffentliche (en: public), die private und die hybride Cloud.

Bei der „öffentlichen Cloud“ werden die angebotenen Dienste z.B. in Form einer IT-Infrastruktur gemietet und abhängig vom Nutzungsgrad bezahlt. Die „gemeinschaftliche (en: community) Cloud“ ist eine spezielle Ausprägung der „öffentlichen Cloud“.

Eine „private Cloud“ zeichnet sich durch ihre Ausschließlichkeit in der Nutzung aus. Sie wird ausschließlich für eine bestimmte Organisation betrieben - entweder durch das eigene Rechenzentrum oder auch durch Dritte.

Bei der „hybriden Cloud“ werden „öffentliche Cloud“ und „private Cloud“ Infrastrukturen den Nutzern zugänglich gemacht; in ihrer Weiterentwicklung

wird sie "Multi-Cloud" genannt. Bei ihr können dann mehrere Cloud Computing Dienste in einer heterogenen IT-Infrastruktur gleichzeitig genutzt werden.

Das bevorzugte Modell ist heute die dynamische "Multi-Cloud". Unternehmen, die Applikationen in der Cloud betreiben, und Technologieanbieter, die sie dabei mit Infrastruktur, Management und Security unterstützen, müssen ihre Produkte und Dienstleistungen so gestalten, dass sie sich problemlos verschieben lassen und in unterschiedlichen Umgebungen parallel laufen können.

Auch "Intercloud" und "Cloud Federation" sind weiterentwickelte Ausprägungen der "Hybriden Cloud". Als „Cloud Federation“ wird der Verbund verschiedener Private- und/oder Public-Cloud-Umgebungen bezeichnet, die miteinander vernetzt sind. Im Kern geht es um die Sicherstellung der Interoperabilität der verschiedenen Lösungen und Services untereinander, da aus architektonischer und funktionaler Sicht erst der Verbund selbst die Bereitstellung und Nutzbarkeit im Sinne eines Gesamt-Service sicherstellt.

Cloud Computing im Internet der Dinge (IoT)

Besonders gewinnt Cloud Computing im Internet der Dinge (IoT) an Bedeutung, sobald Geräte Daten in der Cloud speichern. In vielen Anwendungsfällen ist es aus Verbrauchersicht empfehlenswert, Daten lokal zu verarbeiten und nur da Cloud-Dienste zu nutzen, wo dies einen Funktionsvorteil bietet und eine lokale Verarbeitung nicht möglich ist. Z.B. sollten Sprachassistenten oder Glühbirnen entwickelt werden, die ohne die Übertragung von Daten ins Internet auskommen und die gesamte Verarbeitung auf dem Gerät selbst verwirklichen.

Edge Computing bereitet beispielsweise Sensordaten direkt im Sensorsystem auf, um sie dann an die Cloud weiterzuleiten. Die daraus resultierende Verkürzung von Wartezeiten bei der Nutzung von Edge Computing kann das Nutzungserlebnis für den Verbraucher verbessern, wenn z.B. die Daten einer Sprachsteuerung keinen großen Weg zurücklegen müssen, um verarbeitet zu werden.

Verbraucher und Cloud Services

Sind die Verbraucher selbst die Nutzer von Cloud Dienstleistungen, so ist die Schaffung von Transparenz über die Dienstleistung eine wichtige Grundlage für die Akzeptanz sowie Vergleichbarkeit von Angeboten. Der Verbraucher kann dann selbst entscheiden, ob die angebotenen Leistungen seinen Bedürfnissen entsprechen.

Verbraucher nutzen in vielen Fällen Cloud-Speicher. Verschiedene Veröffentlichungen der Stiftung Warentest klären über die Vor- und Nachteile von Cloud-Diensten bzw. Speichern generell und von einzelnen Produkten im Detail auf (z.B. Test 04/2019 "Cloud-Dienste" oder Test 05/2019 "Netzwerkfestplatten (NAS) im Test: Die besten Festplatten für die private Cloud").

Interoperabilität von Cloud-Speichern ist für Verbraucher insofern wichtig, dass sie einfach zwischen verschiedenen Diensten wechseln können und damit freie Wahl des Dienstleisters haben. Im Jahr 2017 wurde die internationale Norm ISO/IEC 19941 "Informationstechnik - Cloud Computing - Interoperabilität und Übertragbarkeit" veröffentlicht.

Hilfestellung für die Auswahl und Nutzung von Cloud-Dienstleistern durch Endverbraucher wird durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) auf dessen Webseite gegeben: https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/CloudComputing/cloudcomputing_node.html

In vielen Fällen trifft der Verbraucher die Entscheidung über die Verwendung von Cloud Dienstleistungen jedoch nicht selber und in manchen Fällen fehlt ihm sogar jegliches Bewusstsein dafür, dass Cloud Dienstleistungen genutzt werden; zum Beispiel wenn Kundendaten in einer Cloud gespeichert werden. Insbesondere dann sind Mindestanforderungen an die Sicherheit der Cloud, klar zugewiesene Verantwortlichkeiten und klare Anforderungen an den Datenschutz und die Datennutzung in der Cloud zwingend notwendig.

Aus Verbrauchersicht sind Anforderungen an Gebrauchstauglichkeit, Zugänglichkeit, Transparenz, Datenschutz und Datensicherheit zu setzen. Auch die Thematik der Interoperabilität bzw. der Portabilität spielt aus Verbrauchersicht eine große Rolle, falls der Verbraucher von einem Cloud Anbieter zu einem anderen wechseln möchte.

Daten in der Cloud

Zu klären ist, wie Datenflüsse über nationale Grenzen hinweg gestaltet werden und wie sicher gestellt werden kann, dass die für den Verbraucher in seinem Rechtsraum geltenden Gesetze eingehalten werden.

Das mit dem Thema Cloud Computing befasste internationale Gremium ISO/IEC JTC1 SC38 entwickelt zu diesen Fragestellungen verschiedene Dokumente wie ISO/IEC 22624: 2020 "Informationstechnik - Cloud Computing - Taxonomiebasiertes Datenhandling für Cloud-Services" oder ISO/IEC 19944:2017 "Informationstechnik - Cloud Computing - Datenfluss über Geräte und Cloud-Dienstleistungen".

Daten in der Cloud können verschiedenen Quellen unterschiedlicher Qualität entstammen. Zur Behandlung dieser Problematik wurde der technische Bericht ISO/IEC TR 23186: 2018 "Informationstechnik - Cloud Computing - Vertrauensrahmen für die Verarbeitung von Daten aus mehreren Quellen" entwickelt.

Generell gilt in der Cloud das Prinzip der geteilten Verantwortung: Der Cloud-Anbieter ist für die Absicherung der Cloud-Infrastruktur zuständig, der Kunde bzw. Nutzer der Cloud für die Sicherheit der Daten und Anwendungen, die er in dieser Infrastruktur betreibt. Nicht immer lassen sich diese Bereiche aber klar voneinander trennen, insbesondere im Bereich Platform-as-a-Service (PaaS) und Function-as-a-Service (FaaS).

Damit ist auch der Nutzer der Cloud für die Einhaltung der Datenschutzgrundverordnung (DSGVO) und sonstiger rechtlicher Anforderungen für Daten verantwortlich. Die 2017 erschienene Norm DIN ISO/IEC 27018 "Informationstechnik - Sicherheitsverfahren - Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung" gibt zu diesem Thema Hilfestellung.

Wenn Endverbraucher die Nutzer der Cloud-Dienstleistung sind, stellen sich die Fragen, ob diese immer in der Lage sind für die Absicherung der eigenen Daten zu sorgen und ob die Erwartung realitätsnah ist, dass er letztlich nur verschlüsselte Daten hochladen sollte.

Cloud Sicherheit

Die Sicherheit von Cloud Dienstleistungen ist wesentlich, um sie aus Verbrauchersicht nutzbar zu machen.

In den internationalen Normungsgremien wurde ISO/IEC 27017: 2015 "Information technology — Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services" hierzu erarbeitet.

Das BSI (Bundesamt für Sicherheit in der Informationstechnik) bietet eine IT-Sicherheitszertifizierung für Cloud-Dienstleistungen nach dem Cloud Computing Kriterienkatalog C5 (cloud computing compliance criteria catalogue) an: https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Kriterienkatalog/Kriterienkatalog_node.html.