2.5.2 Cloud-Modelle der Bereitstellung und Dienstleistungen

Stichwörter: Community Cloud, Hybrid Cloud, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Private Cloud, Public Cloud, Software as a Service (SaaS)

› Warum ist das Thema wichtig?

Die Nutzung eines auf die betrieblichen Anforderungen zugeschnittenen Cloud-Modells verbessert die Effizienz und Effektivität von 4.0-Prozessen[1] und kann Kosten einsparen. Damit Betriebe die Möglichkeiten von Cloud Computing bewusst und systematisch nutzen können, sollten die unterschiedlichen Modelle der Bereitstellung und Dienstleistungen dieser 4.0-Technologie[2] bekannt sein.

› Worum geht es bei dem Thema?

Begriff: Cloud-Modelle

Cloud Computing ist eine Schlüsseltechnologie von cyber-physischen Systemen[3] (CPS)[4] und intelligenter Software[5] mit ihren Modellen der künstlichen Intelligenz (KI).

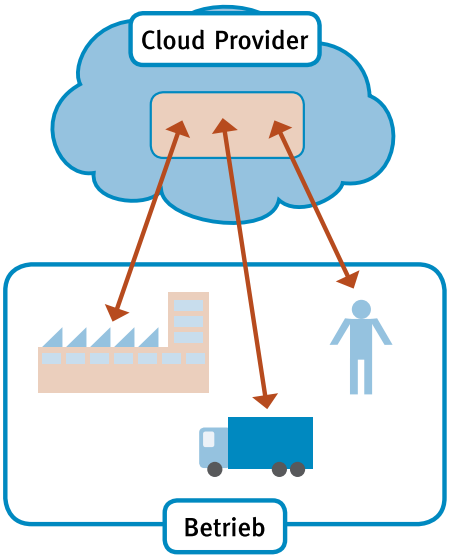
Bei der Nutzung von Clouds werden unterschiedliche Modelle verwendet. Sie werden unterschieden nach Formen der Bereitstellung für verschiedene Zielgruppen (öffentlich, firmenintern) und der angebotenen Dienstleistung (Leistungsumfang, Rechte, Interventionsmöglichkeiten).

Cloud-Modelle der Bereitstellung – Es werden vier Cloud-Modelle der Bereitstellung (Deployment Models) unterschieden[6]:

1. Cloud für eine Institution (Private Cloud)

In einer Private Cloud wird die Cloud-Infrastruktur nur für eine Institution betrieben. Sie kann von der Institution selbst oder einem Dritten organisiert und geführt werden und dabei im Rechenzentrum der eigenen oder einer fremden Institution stehen.

Beispiel: Daten über Gefährdungen bei der Arbeit eines Betriebes (wie Verschleiß von Maschinen, psychische Belastungen, Sicherheit der Ladung) werden in der Cloud gesammelt und es werden beinahe in Echtzeit Hilfen zur Verfügung gestellt, die ortsunabhängig von Beschäftigten genutzt werden können. In der Cloud liegt auch eine CPS-Verwaltungssoftware (System-Verwaltungsschale) für die Gestaltung von Prozessen im Unternehmen.



Diese Umsetzungshilfe gibt Experten und Interessierten Anregungen, wie Arbeit 4.0 zu gestalten ist. Die Empfehlungen sollten an die jeweilige konkrete betriebliche Situation angepasst werden.

[1] Unter 4.0-Prozessen werden hier alle Arbeitsprozesse verstanden, in denen cyber-physische Systeme (CPS) oder andere autonome technische Systeme (wie Plattformen, Messenger-Programme) beteiligt sind. 4.0-Prozesse sind in den Arbeitsprozessen bisher selten vollständig, aber in Ansätzen in allen Betrieben umgesetzt.

[2] 4.0-Technologie bezeichnet hier Hardware und technologische Produkte (wie Assistenzmittel/Smartphones, Sensoren/Aktoren in smarten Arbeitsmitteln, Fahrzeugen, Produkten, Räumen usw., smarte Dienstleistungen, Apps), die von intelligenter Software (inkl. KI) ganz oder teilweise gesteuert werden.

[3] Cyber-physische Systeme (CPS) verbinden und steuern als autonome technische Systeme Arbeitsmittel, Produkte, Räume, Prozesse und Menschen beinahe in Echtzeit. Die komplette oder teilweise Steuerung übernimmt intelligente Software auf Grundlage von Modellen der künstlichen Intelligenz. Genutzt werden dazu unter anderem auch Sensoren/Aktoren, Verwaltungsschalen, Plattformen/Clouds.

[4] Anwendungsbereiche von CPS können sein: **Insellösungen**, Teilkomponenten und Teilprozesse (zum Beispiel einzelne Arbeitsplätze, Arbeitsmittel, Teile von Anlagen, Räume, Produkte, Assistenzsysteme) und **verkettete Prozesse** und Gesamtsystemlösungen (zum Beispiel verkettete Arbeitsmittel, Wertschöpfungskette). Außerdem **geschlossene Betriebsanwendungen** (autark – zum Beispiel Edge Computing, betriebliche Cloud), **offene Anwendungen** (zum Beispiel Public Clouds, Hersteller-Plattformen).

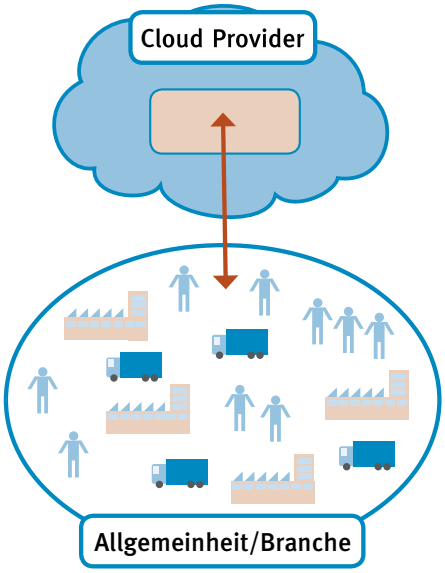
[5] Intelligente Software steuert cyber-physische Systeme (CPS) und andere autonome technische Systeme (wie Messenger-Programme). Intelligente Software nutzt Modelle künstlicher Intelligenz zusammen mit anderen Basistechnologien wie zum Beispiel Algorithmen, semantischen Technologien, Data-Mining. Intelligente Software ist autonom und selbstlernend.

[6] National Institute of Standards and Technology (NIST) – BSI 2012, S. 17

2. Cloud für eine große Gruppe/Allgemeinheit (Public Cloud)

Von einer Public Cloud wird gesprochen, wenn die Services von der Allgemeinheit oder einer großen Gruppe, wie beispielsweise einer ganzen Branche, genutzt werden können und die Services von einem Anbieter zur Verfügung gestellt werden.

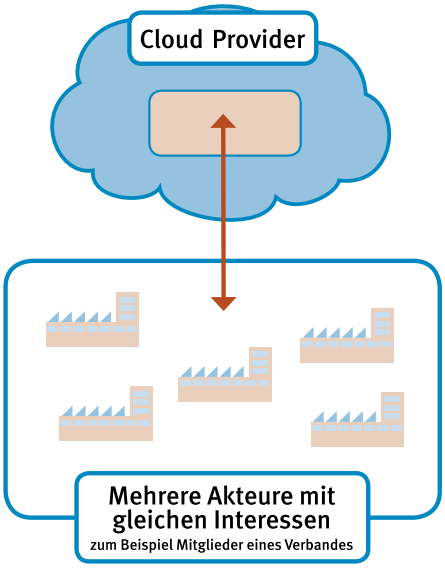
Beispiel: Ein Gefahrstoffsystem stellt Daten über Gefahrstoffe, Sicherheitsdatenblätter, Betriebsanweisungen in der Cloud zur Verfügung, die von Betrieben und Privatpersonen je nach Einsatz (zum Beispiel über Sensoren oder ID-Codes) beinahe in Echtzeit genutzt werden können.



3. Cloud für eine begrenzte Gruppe (Community Cloud)

In einer Community Cloud wird die Infrastruktur von mehreren Institutionen geteilt, die ähnliche Interessen haben. Eine solche Cloud kann von einer dieser Institutionen oder einem Dritten betrieben werden.

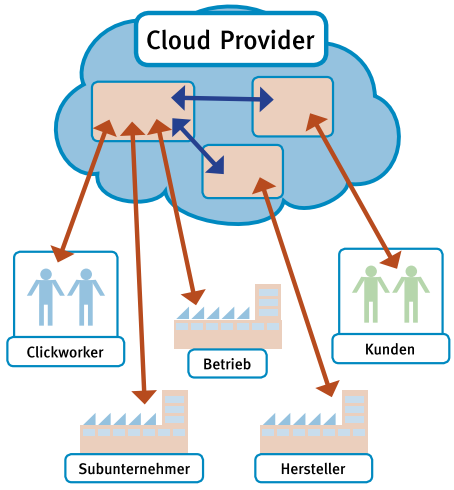
Beispiel: Ein Fachverband stellt seinen Mitgliedsbetrieben Gefährdungsbeurteilungen und Arbeitsanweisungen zur Verfügung, die je nach Bedarf (Impulse über Sensoren) den Führungskräften und Beschäftigten in den Mitgliedsbetrieben über Assistenzsysteme zur Verfügung gestellt werden.



4. Mehrere vernetzte Clouds (Hybrid Cloud)

In einer Hybrid Cloud werden mehrere Cloud-Infrastrukturen, die selbst eigenständig sind, über standardisierte Schnittstellen gemeinsam genutzt.

Beispiel: Das Prozess-CPS eines Betriebes liegt in einer Cloud-Plattform und ist mit Plattformen von Herstellern und Kunden verbunden.



Cloud-Modelle der Dienstleistungen

Auf der Grundlage der beschriebenen Cloud-Modelle der Bereitstellung werden drei Cloud-Modelle der Dienstleistungen (Kategorien von Servicemodellen) unterschieden[7]:

1. *Cloud als Datenspeicher und Infrastruktur (IaaS – Infrastructure as a Service)*
   Hier werden Rechenleistung, Datenspeicher oder Netze als Dienst angeboten (IT-Ressourcen). „Ein Cloud-Kunde kauft diese virtualisierten und in hohem Maß standardisierten Services und baut darauf eigene Services zum internen oder externen Gebrauch auf. So kann ein Cloud-Kunde zum Beispiel Rechenleistung, Arbeitsspeicher und Datenspeicher anmieten und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.“[8]
   Kontrolle des Kunden: Der Kunde hat die volle Kontrolle über das IT-System, da alles innerhalb seines Verantwortungsbereiches betrieben wird. Seine Verwaltung (zum Beispiel Wartung, Skalierung) obliegt dem Nutzer.
2. *Cloud als Plattform mit zusätzlichen Funktionen (PaaS – Platform as a Service)*
   Hierbei werden neben Rechenleistung und Infrastruktur zusätzliche Funktionen und Werkzeuge auf der Plattform mit standardisierten Schnittstellen angeboten – wie zum Beispiel für Entwicklung, Vertrieb, Marketing, Service oder Ausbildung im Unternehmen. Der Kunde hat keinen Zugriff auf die darunterliegenden Schichten (Betriebssystem, Hardware), er kann aber auf der Plattform eigene Anwendungen laufen lassen, für deren Entwicklung der Cloud-Anbieter in der Regel eigene Werkzeuge hat.
   Kontrolle des Kunden: Der Kunde hat nur Kontrolle über seine Anwendungen, die auf der Plattform laufen. Verwaltungs- und Wartungsarbeiten werden durch die Plattform übernommen (zum Beispiel Wartung, Skalierung).
3. *Cloud als Dienstleistung mit zusätzlichen Softwareprogrammen (SaaS – Software as a Service)*
   Über Clouds werden neben Rechenleistung, Infrastruktur und zusätzlichen Funktionen auch umfassende Anwendungsprogramme angeboten. Anwender nutzen diese Software-Anwendungen direkt über das Internet. Als Beispiele dafür seien Kontaktdatenmanagement, Finanzbuchhaltung, Gestaltungsprogramme oder Kollaborationsanwendungen genannt. In diesen Bereich fallen auch die Verwaltungsprogramme für Steuerungen von Prozessen in Betrieben oder zwischen Betrieben (Verwaltungssoftware/-schale von cyber-physischen Systemen).
   Kontrolle des Kunden: Der Provider hat die volle Kontrolle über das IT-System. Eine Installation der Software auf dem PC des Kunden beziehungsweise im Rechenzentrum des Unternehmens ist nicht erforderlich.

Welche Chancen und Gefahren gibt es?

Chancen: Betriebe, die die Modelle der Bereitstellung und der möglichen Dienstleistungen von Cloud-Anbietern kennen, können die Möglichkeiten sowie die Vor- und Nachteile der einzelnen Modelle besser einschätzen und somit verlässliche Entscheidungen zur Nutzung von geeigneten Cloud-Dienstleistungen treffen. › *Siehe Umsetzungshilfe 1.1.6 Vor- und Nachteile von CPS-Anwendungsbereichen*. Damit lassen sich die Akzeptanz der Beschäftigten und die betrieblichen Prozesse verbessern. Ein passendes Cloud-Modell ermöglicht

- eine bedarfsgerechte Auswahl von Leistungen,
- ausreichende Interventionsmöglichkeiten,
- die gezielte Entscheidung über Zugänge und Kontrolle der Zugriffsrechte,
- Möglichkeiten der unterschiedlichen Nutzung, zum Beispiel Firmen- und private Daten,
- Verbesserungsprozesse beinahe in Echtzeit,
- gleichzeitige Bearbeitung von Dokumenten,
- die Dokumentation der Datenflüsse und damit eine Nachvollziehbarkeit der Bearbeitung.

Gefahren: Wer ohne die Kenntnisse der Modelle, der Bereitstellung und der Dienstleistungen Cloud-Anbieter beauftragt, unterliegt unter anderem der Gefahr, dass er Leistungen einkauft, die

- nicht den Möglichkeiten der neuen Cloud-Technologien entsprechen,
- unnötige Kosten produzieren,
- zu Mehraufwand und Störungen im Arbeitsablauf führen,
- die Führungskräfte und Beschäftigten belasten und Unzufriedenheit bei ihnen erzeugt,
- von den Führungskräften und Beschäftigten nicht genutzt werden,
- dazu führen, dass er die Hoheit über seine Daten teilweise aufgibt oder verliert.

Ein grundsätzliches Risiko bei der Auswahl eines Cloud-Modells ist die Entstehung neuer Abhängigkeiten von Dritten. Dabei ist der Standort des Cloud-Anbieters besonders relevant, weil das Landesrecht den Zugriff auf die Cloud (zum Beispiel durch staatliche Behörden) und die Sicherheit der Daten regelt.

Über bestimmte Cloud-Modelle werden Datenflüsse verfolgbar. Dies ermöglicht die Dokumentation und Auswertung beispielsweise von Bearbeitungszeiten und könnte zum problematischen Umgang mit personenbezogenen Daten von Führungskräften und Beschäftigten führen.

Welche Maßnahmen sind zu empfehlen?

Negative Auswirkungen von Cloud-Dienstleistungen können durch präventive Überlegungen vermieden werden. Sowohl die unterschiedlichen Bereitstellungsmodelle als auch die Nutzungsmodelle der Cloud sowie die Qualität des Cloud-Dienstleisters haben Auswirkungen auf Prozesse im Betrieb.

Vor der Modellauswahl sollten unter anderem folgende Fragen reflektiert werden:

- Für welche Aufgaben benötigen wir die Cloud und welche Anforderungen muss die Cloud erfüllen?
- Welche Art der Cloud-Lösung ist sinnvoll beziehungsweise auf welche

[7] BSI 2016; Bernnat et al. 2015
[8] BSI 2012, S. 17

bestehenden Dienste können wir gegebenenfalls zurückgreifen? › *Siehe Umsetzungshilfe 1.1.6 Vor- und Nachteile von CPS-Anwendungsbereichen.*
- Welche sind die für den Betrieb wichtigsten Kriterien für die Auswahl des passenden Cloud-Modells?

Folgende Präventionskriterien helfen, die Qualität der Cloud-Dienstleistung zu beurteilen:
- Datensicherung (Sicherheits- und Notfallmanagement)
- Datenschutz (betriebssensibler und personenbezogenen Daten)
- Zugang zu den Daten
- Kontrolle über die Daten und Programme
- Interventions- und Eingriffsmöglichkeiten
- Zugriff auf die Daten durch Dritte
- Abhängigkeit von den Cloud-Anbietern

Quellen und weitere Informationsmöglichkeiten:

Appelrath, H.-J., Kagermann, H., & Krcmar, H. (Hrsg.). (2014). *Future Business Clouds – Ein Beitrag zum Zukunftsprojekt Internetbasierte Dienste für die Wirtschaft.* München: acatech STUDIE.

Bernnat, R., Zink, W., Bieber, N., Strach, J., Tai, S., & Fischer, R. (2015). *Das Normungs- und Standardisierungsumfeld von Cloud Computing.* München: Hansa Print.

BSI – Bundesamt für Sicherheit in der Informationstechnik. (2016). *Anforderungskatalog Cloud Computing Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten.* Frankfurt am Main: Zarbock.

BSI – Bundesamt für Sicherheit in der Informationstechnik. (2012). *Eckpunktepapier: Sicherheitsempfehlungen für Cloud Computing Anbieter – Mindestanforderungen in der Informationssicherheit.* Rheinbach: Moser.

Zu diesem Thema könnten Sie auch folgende weitere Umsetzungshilfen interessieren:

- 1.1.6 Vor- und Nachteile von CPS-Anwendungsbereichen
- 2.2.3 Risikobetrachtung und IT-Sicherheit
- 2.5.1 Anforderungen an eine Cloud

Herausgeber: „Offensive Mittelstand – Gut für Deutschland“ – Stiftung „Mittelstand – Gesellschaft – Verantwortung“ Kurfürsten-Anlage 62, 69115 Heidelberg, E-Mail: info@offensive-mittelstand.de; Heidelberg 2019