2.5.1 Anforderungen an eine Cloud

Stichwörter: Cloud-Dienstleistungen, Managed Security Services (MSS), Notfallmanagement, Qualitätsstandards, Security as a Service (SecS), Sicherheitsmanagement, Vertragsgestaltung, Zertifizierungen

› Warum ist das Thema wichtig?

Cloud Computing ist eine Basistechnologie[1] der 4.0-Prozesse[2], ohne die cyber-physische Systeme[3] mit ihrer intelligenten Software[4] nicht funktionieren würden.[5] Über Clouds können Unternehmensprozesse effizienter und flexibler gestaltet sowie technische und personelle Ressourcen eingespart werden. Da diese 4.0-Technologie[6] in der Regel von externen Anbietern zur Verfügung gestellt wird, müssen die betrieblichen Anforderungen mit den Leistungen der Cloud abgeglichen und vereinbart werden, um zum Beispiel die Datensicherheit gewährleisten, den „Besitz" der Daten sicherstellen und die Verfügbarkeit garantieren zu können.

› Worum geht es bei dem Thema?

Begriff: Cloud
Clouds ermöglichen eine zentrale Speicherung und Bearbeitung umfangreicher Datenmengen im Internet, die für den ortsunabhängigen und geräteübergreifenden Zugriff eines großen definierten Teilnehmerkreises zur Verfügung gestellt werden sollen. Dabei werden Daten in der Regel auf den Servern des Anbieters gespeichert und unterliegen damit dessen rechtlichen Rahmenbedingungen (zum Beispiel Allgemeine Geschäftsbedingungen [AGB], Gesetze zum Datenschutz und weitere Länderrechtsprechungen).

Für Clouds stehen verschiedene Modelle zur Verfügung, zwischen denen die Nutzer je nach Anforderungen wählen können. › *Siehe Umsetzungshilfe 2.5.2 Cloud-Modelle der Bereitstellung und Dienstleistungen.* Die jeweiligen Vorteile der Cloud können dann genutzt werden, wenn nicht ausschließlich auf die technische Lösung und den wirtschaftlichsten Cloud-Anbieter geschaut wird, sondern wenn auch die Effektivität, Sicherheit und Wirkung der Arbeits- und Betriebsprozesse, die von dem Cloud-Angebot abhängen, beachtet werden. Hier spielt die präventive Gestaltung der Cloud-Prozesse eine wichtige Rolle, um störungsfreie und gesundheitsgerechte Arbeitsprozesse zu haben, die die Motivation der Beschäftigten fördern und gleichzeitig effizient und produktiv sind. › *Siehe Umsetzungshilfe 1.1.6 Vor- und Nachteile von CPS-Anwendungsbereichen.*

› Welche Chancen und Gefahren gibt es?

Chancen: Wer Cloud Computing gezielt und systematisch sowie unter Berücksichtigung aller Sicherheitsaspekte nutzt, kann alle Vorteile der Cloud-Dienstleistungen ausschöpfen und die Effektivität und Effizienz der Prozesse verbessern:

- Arbeits- und Unternehmensprozesse können unternehmensintern und entlang der Wertschöpfungskette besser vernetzt werden.
- Es werden Zeit- und Kostengewinne erzielt, zum Beispiel durch die Reduzierung von personellen, finanziellen und zeitlichen Aufwänden für Serverwartung und -bereitstellung. Clouds sind sofort verfügbar.
- Prozesse lassen sich durch schnelle und flexible Zugriffsmöglichkeiten auf benötigte Daten beschleunigen.
- Es entstehen Unterstützungs- und Entlastungsmöglichkeiten, weil beispielsweise den Nutzern eine größere Flexibilität ermöglicht wird.

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] Appelrath et al. 2014

[2] 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.

[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] 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.

[5] 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).

[6] 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.

- Die Speicherkapazität kann dem Bedarf flexibel angepasst werden und steht geräteübergreifend zur Verfügung.
- Der Anbieter ist technisch auf dem neuesten Stand, sodass der Nutzer vom Modernisierungsdruck entlastet wird und dahingehend Investitionen einspart.
- Die Datensicherung wird durch Zuverlässigkeit der Technik verbessert. Der Aufwand für Back-ups verringert sich und erfolgt geräteunabhängig.

Gefahren: Fehlende präventive Überlegungen bei der Beauftragung und Nutzung von Cloud-Dienstleistungen können negative Auswirkungen auf den Betrieb, die Beschäftigten und andere Nutzer haben.[7] Störungen der Betriebsprozesse und Belastungen der Beschäftigten sowie Nutzer entstehen zum Beispiel durch:

- Ungenügendes Sicherheits- und Notfallmanagement des Cloud-Anbieters – zum Beispiel Datenverlust beziehungsweise Störung des Informationsflusses, Ausfall der Internet- oder Netzverbindung, Fehler in der Cloud-Administration
- Nicht gebrauchtstaugliche Software (Usability) des Cloud-Anbieters, fehlende Interventionsmöglichkeiten oder Fehler in Cloud-Programmen beziehungsweise nicht auf den Arbeitsprozess abgestimmte Programme
- Nutzung von Cloud-Software, die nicht zu den Prozessen im Betrieb passt und ihre Umsetzung erschwer
- Fehlende Aspekte der Sicherheit und Gesundheit in dem Anwendungsprogramm des Cloud-Anbieters
- Verletzung des rechtlichen Rahmens (Compliance) inklusive der Vorschriften zum Datenschutz, Arbeitsschutz und zur Gesundheit im Betrieb
- Verlust der Kontrolle über die Daten und Anwendungen, zum Beispiel durch organisatorische Mängel beim Cloud-Anbieter – etwa durch unzureichendes Informationssicherheits-Management, Fehlen von Sicherheitsrichtlinien, ungenügende Sicherheitsüberprüfung und ungenügende Schulung der Beschäftigten in Sicherheitsfragen, unzureichende Kontrolle des Zugriffs
- Ausfall von Zugriffsmöglichkeiten auf die betrieblichen Daten durch fehlendes Notfallmanagement beim Cloud-Anbieter oder ungenügendes Schnittstellenmanagement zwischen Anbieter und Betrieb, das von den Beschäftigten kurzfristig ausgeglichen werden muss beziehungsweise das die Prozesse im Betrieb zum Erliegen bringt
- Verlust von Daten durch Fehlfunktion oder Versagen technischer Systeme und Infrastrukturen beim Cloud-Anbieter – zum Beispiel durch Störung interner Versorgungs- und Kommunikationsnetze, fehlerhafte Implementierung von Standards und Standardlösungen, die zu Inkompatibilitäten oder zu neuen Schwachstellen (Hard- oder Softwareschwachstellen) und -fehlern führen, oder durch Ausfall oder Störung vorhandener Sicherheitseinrichtungen bei fehlendem Sicherheitsmanagement oder auch durch vorsätzliche Handlungen – zum Beispiel durch Manipulation von Geräten und Zubehör, Missbrauch von Zugriffsrechten, Datenmanipulation gespeicherter Daten, Hackerangriffe
- Standortferne des Cloud-Anbieters, die den schnellen persönlichen Notfallservice erschwert beziehungsweise Betriebsdaten unter ausländisches Recht stellt und somit die Sicherheit von Prozessabläufen im Betrieb einschränkt
- Anteilige Bereitstellung von Cloud-Dienstleistungen für verschiedene Kunden oder Bereitstellung verschiedener Programme für einen Kunden bergen die Gefahr unzureichender Trennung von Anwendungen (isolation failure) oder Ausfall von Schnittstellenfunktionalitäten

› Welche Maßnahmen sind zu empfehlen?

Für die Qualität der Cloud-Dienstleistungen gibt es umfassende Qualitätsstandards und Zertifizierungen, die einen detaillierten Rahmen für die Cloud-Anbieter beschreiben.[8] Diese Standards enthalten eine Vielzahl von präventiven Aspekten, wie sorgfältige Planungen nach Qualitätsprozessen (ISO 9001), ein umfassendes Sicherheits- und Notfallmanagement sowie Informationspflichten gegenüber dem Kunden und Interventionsmöglichkeiten für den Kunden. Diese Qualitätsstandards und Zertifizierungen richten sich jedoch an Cloud-Anbieter und können für Cloud-Nutzer, darunter auch kleine und mittlere Betriebe, schwer verständlich sein. Im Folgenden werden deswegen einige wesentliche Kriterien für die Cloud-Nutzung für kleine und mittlere Betriebe aus Perspektive der Prävention zusammengefasst.

Vorüberlegungen und Planung des Betriebes

- Welche Leistung des Cloud-Anbieters benötigen wir im Detail (Funktionen, Datenvolumen, Programme, Schnittstellen, Zugriffsmöglichkeiten, Kommunikationswege)?
- Welche Art der Cloud-Lösung ist sinnvoll beziehungsweise auf welche bestehenden Dienste können wir gegebenenfalls zurückgreifen? Welches Bereitstellungsmodell (Private Cloud/Public Cloud/Hybrid Cloud) und welches Dienstleistungsmodell (Speicherplatz/Funktionen/Softwareprogramme) werden gewählt? › *Siehe Umsetzungshilfe 2.5.2 Cloud-Modelle der Bereitstellung und Dienstleistungen.*
- Welchen Schutzbedarf haben wir für unsere Aufgaben in der Cloud (Informationen, Anwendungen, Systeme und Cloud-Services in Schutzbedarfskategorien einteilen)?
- Welche rechtlichen Rahmenbedingungen sind zu beachten (Compliance) (zum Beispiel Datenschutz, Arbeits- und Gesundheitsschutz)?
- Welche Risiken gibt es und wie schätzen wir sie ein (Risikoanalyse/Gefährdungsbeurteilung)?
- Welche spezifischen Sicherheitsanforderungen müssen die Cloud und die über die Cloud geregelten Prozesse erfüllen?

[7] BSI 2014a, S. 27ff.
[8] BSI 2012; BSI 2014a; BSI 2016a; BSI 2016b; Kompetenzzentrum Trusted Cloud 2015; Überblicksstudien: Bernnat et al. 2015; Kompetenzzentrum Trusted Cloud 2016

- Können zusätzliche Sicherheitsdienstleister beauftragt werden, die beispielsweise den Weg der Daten verfolgen und/oder Datenverschlüsselungen vornehmen? Dabei stehen zwei Modelle zur Verfügung:
  - Security as a Service (SecS) = standardisierte Leistung eines Dienstleisters/Providers. Der Dienstleister hält dabei die benötigte Sicherheitstechnik als Service zentral auf seiner Cloud zur Verfügung.
  - Managed Security Services (MSS) = Dienstleister, der vom Unternehmen vorgegebene Leistungsanforderungen umsetzt und maßgeschneiderte Lösungen anbietet.
- Wurde auf Grundlage der Vorüberlegung und Planung eine Kosten-Nutzen-Abschätzung vorgenommen (zum Beispiel Kosten für Cloud-Nutzung, interner Administrationsaufwand, Qualifizierung der Beschäftigten, neue IT und Netzanbindungen, Kosten für Einführung, Einsparungen)?
- Wie kann die Cloud-Nutzung in den Arbeitsprozess integriert werden?
- Sind die angebotenen Cloud-Dienstleistungen (Programme) kompatibel mit der Software im Betrieb? Welche weiteren Anforderungen bestehen an die Software des Cloud-Anbieters?
- Ist der Einsatz der Cloud von uns ausreichend softwaretechnisch vorbereitet beziehungsweise besitzen wir die erforderlichen Voraussetzungen, damit die Umsetzung in eine Cloud gelingen kann (zum Beispiel Datenformate, Einhaltung von Standards)?
- Wie können die Beschäftigten auf die Cloud-Lösung vorbereitet werden (zum Beispiel Erfahrungen einbinden, an Lösungen beteiligen, Akzeptanz herstellen/motivieren, Kompetenzen erweitern/qualifizieren)?
- Welche Vor- und Nachteile haben geschlossene Betriebsanwendungen und offene Anwendungen? › *Siehe Umsetzungshilfe 1.1.6 Vor- und Nachteile von CPS-Anwendungsbereichen.*

Kriterien für die Wahl des geeigneten Cloud-Anbieters[9]

Zur Überprüfung der Eignung eines Anbieters sollten unter anderem folgende Kriterien berücksichtigt werden:[10]

- Standorte, an denen die Informationen verarbeitet und gespeichert werden (möglichst regionale Anbieter mit direktem persönlichen Support)
- Rechtliche Rahmenbedingungen (zum Beispiel geltendes Landesrecht)
- Empfehlungen, Rankings, überprüfbare Referenzen oder Bewertungsmatrizen von (möglichst unabhängigen) Organisationen und Kunden
- Klärung, ob Cloud-Computing das Kerngeschäft des Anbieters ist. Falls nicht, könnte es sein, dass der Cloud-Dienst rasch eingestellt oder von einem anderen Anbieter übernommen wird
- Möglichkeiten und Erlaubnis auf Zugriffe durch den Dienstanbieter oder durch Dritte
- Angaben zu Subunternehmen und zur Service-Erbringung, um Abhängigkeiten des Cloud-Anbieters beurteilen zu können
- Nachweis von Zertifikaten und Nachweis, ob der Zertifizierungsgegenstand den gesamten angebotenen Cloud-Service enthält und was die wesentliche Aussage des Zertifikats ist

Spezielle **Kriterien zum Sicherheitsmanagement,** die gesondert nachgewiesen werden sollten, sind unter anderem › *siehe Umsetzungshilfe 2.2.3 Risikobetrachtung und IT-Sicherheit*:

- Hat der Cloud-Anbieter ein definiertes Vorgehensmodell für alle IT-Prozesse[11] (zum Beispiel nach bestehenden Standards wie ITIL, COBIT, das Trusted Cloud Label)?
- Besitzt der Cloud-Anbieter ein anerkanntes Informationssicherheits-Managementsystem (zum Beispiel nach BSI-Standard 100-2 [IT Grundschutz], ISO 27001)?
- Wird das Informationssicherheitskonzept für die Cloud nachhaltig umgesetzt?
- Ist die Informationssicherheit ausreichend nachgewiesen (zum Beispiel Zertifizierung)?
- Besitzt der Cloud-Anbieter eine angemessene Organisationsstruktur für Informationssicherheit (inklusive Benennung von Ansprechpartnern für Kunden zu Sicherheitsfragen)?
- Sind im Angebot des Cloud-Anbieters die angebotenen Services ausreichend klar und verständlich beschrieben oder lassen sie sich anderweitig klären?
- Liegen Informationen zu Subunternehmen des Cloud-Anbieters und den vom Subunternehmer geforderten Sicherheitsstandards vor, um Abhängigkeiten des Cloud-Anbieters beurteilen zu können?

Vertragsgestaltung

In den Angeboten der Cloud-Anbieter sind immer auch vertragliche Bestandteile (AGB) enthalten. Diese sollten überprüft werden, ob sie für den Betrieb, der die Cloud-Dienste nutzen will, tragbar sind.[12] Wie ein Vertrag zur Auftragsvergabe von Datenverarbeitung auszusehen hat, ist rechtlich geregelt (Datenschutz-Grundverordnung – DSVGO).

Folgende Punkte sollten mindestens im Vertrag über die Cloud-Dienste enthalten sein[13]:

- Standorte des Cloud-Anbieters (Land, Region), an denen die Kundendaten gespeichert und verarbeitet werden
- Subunternehmer des Cloud-Anbieters, die für die Erbringung der Cloud-Dienstleistungen wesentlich sind
- Verantwortlichkeiten, Aufgaben und Schnittstellen zwischen Kundenbetrieb und Cloud-Anbieter (zum Beispiel geteilte Verantwortlichkeiten, Mitwirkungspflichten, Schnittstellen zum Melden von Sicherheitsvorfällen und Störungen); ebenfalls eventuelle Weisungsbefugnisse des Auftraggebers (Auftragskontrolle)
- Regelungen zu Prozessen, Arbeitsabläufen
- Regelungen zum Sicherheitsmanagement und zum Datenschutz

[9] BSI 2012, S. 26f.
[10] BSI 2012b, S. 18
[11] Trusted Cloud Angebote (www.trusted-cloud.de): Trusted Cloud hat das Ziel, die Nutzenpotenziale von Cloud Services, insbesondere für kleinere und mittlere Unternehmen (KMU), aufzuzeigen und das Vertrauen in Cloud Services zu steigern. Die Trusted-Cloud-Plattform führt Anwender (insbesondere KMU) und Anbieter von Cloud Services, Anbieter von Cloud-Gütesiegeln sowie Anbieter von Cloud-bezogenen Dienstleistungen zusammen. Hier sind vertrauenswürdige Cloud-Angebote gelistet. Das Trusted Cloud Label zeichnet vertrauenswürdige Cloud Services und Cloud-bezogene Dienstleistungen aus, die Mindestanforderungen im Hinblick auf Transparenz, Sicherheit, Qualität und Rechtskonformität erfüllen. Trusted Cloud bietet Informationen für KMU und Qualifizierungsangebote.
[12] BSI 2014b, S. 19
[13] BSI 2012, S. 69ff.; BSI 2014b, S. 19; Schröter et al. 2015

- Kommunikationswege und Ansprechpartner
- Kontrolle von Zutritt, Zugang, Zugriff, Eingabe und Weitergabe
- Zeitnahe und regelmäßige Unterrichtung über Änderungen (zum Beispiel neue, geänderte oder gestrichene Funktionen, neue Subunternehmer)
- Information, welche Software durch den Cloud-Anbieter aufseiten des Kundenbetriebes installiert wird sowie über die daraus resultierenden Sicherheitserfordernisse/-risiken
- Notfallvorsorge
- Haftungsfragen
- Weg aus der Cloud heraus; Beendigung, Übergabe der Daten und Datenlöschung beim Cloud-Anbieter
- Bereitstellung der Daten im Falle einer Insolvenz des Cloud-Service-Anbieters

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. (2016a). *Anforderungskatalog Cloud Computing Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten*. Frankfurt am Main: Zarbock.

BSI – Bundesamt für Sicherheit in der Informationstechnik. (2016b). *Referenzierung des Anforderungskatalogs Cloud Computing auf internationale Standards*. Bonn.

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

BSI – Bundesamt für Sicherheit in der Informationstechnik. (2014a). *Sicherheitsprofil für ein SaaS Archivierungssystem*. Bonn.

BSI – Bundesamt für Sicherheit in der Informationstechnik. (2014b). *Sichere Nutzung von Cloud-Diensten*. Frankfurt am Main: Zarbock.

Hoffmann, F.J. (2014). Antropomatik schafft revolutionäre Logistik-Lösungen. In Bauernhansl, T., ten Hompel, M., & Vogel-Heuser, B. (Hrsg.), *Industrie 4.0 in Produktion, Automatisierung und Logistik* (S. 207–220). Wiesbaden: Springer Vieweg.

Kompetenzzentrum Trusted Cloud. (2016). *Cloud-Standards und Zertifizierungen im Überblick*. Berlin.

Kompetenzzentrum Trusted Cloud. (2015). *Trusted Cloud-Datenschutzprofil für Cloud-Dienste (TCDP) – Version 0.9*. Berlin.

Schröter, W., & Scherer, I. (2015). *E10 Entscheidungshilfe: Arbeit 4.0 – Rechtliche Aspekte der Nutzung von Cloud-Lösungen*. Abgerufen von http://www.offensive-mittelstand.de/fileadmin/user_upload/pdf/mittelstand_40/Entscheidungshilfe_10_0604.pdf . Zugegriffen: 14.12.2018.

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
- 2.2.4 Notfallorganisation und 4.0-Prozesse
- 2.5.2 Cloud-Modelle der Bereitstellung und Dienstleistungen

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