Bundesamt
für Sicherheit in der
Informationstechnik

Eckpunktepapier

Sicherheitsempfehlungen für Cloud Computing Anbieter

– Mindestanforderungen in der Informationssicherheit –

Inhaltsverzeichnis

Vorwort

Minimierte Risiken beim Cloud Computing

Cloud Computing hat das Potential, die Bereitstellung und Nutzung von Informationstechnologie nachhaltig zu verändern. Damit IT-Dienstleistungen aus der Cloud jedoch zuverlässig genutzt werden können, ist die Informationssicherheit einer der Schlüsselfaktoren. Um im Hinblick auf Sicherheit beim Cloud Computing eine tragfähige Basis zu schaffen, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) im September 2010 einen praxisnahen Austausch angeregt. Sowohl Anbieter entsprechender Lösungen als auch deren Anwender sowie Sicherheitsexperten waren aufgerufen, das vom BSI veröffentlichte Eckpunktepapier mit Mindestanforderungen an die Informationssicherheit beim Cloud Computing zu diskutieren.

Nicht nur die klassischen Angriffsszenarien sind für Cloud-Systeme relevant. Hinzu kommen spezielle Charakteristika wie etwa die Tatsache, dass sich mehrere Nutzer eine gemeinsame IT-Infrastruktur teilen. Zudem stellt die dynamische Verteilung der IT-Leistung über mehrere Standorte hinweg eine besondere Herausforderung dar.

Die zahlreichen Rückmeldungen der Branche auf diese BSI-Initiative haben gezeigt, dass sich der Ansatz einer gemeinsamen, praxisorientierten Diskussion von Anbietern und Anwendern bewährt hat: Das Eckpunktepapier wurde von den Marktteilnehmern weitgehend positiv aufgenommen. Das belegen die zahlreichen Anfragen genauso wie die vielen konstruktiven Kommentare. Die Ergebnisse dieser Diskussion sind nun in dem vorliegenden Band dokumentiert.

Ziel des BSI ist es, gemeinsam mit den Beteiligten sinnvolle und angemessene Sicherheitsanforderungen an das Cloud Computing zu entwickeln, die einen Schutz von Informationen, Anwendungen und Systemen gewährleisten. Diesem Ziel sind wir ein gutes Stück näher gekommen. Die im Folgenden beschriebenen Mindestanforderungen sind skalierbar in Richtung Verfügbarkeit und Vertraulichkeit. Sie bieten eine methodische Grundlage, um

einerseits weitere Aspekte integrieren zu können und um sie kontinuierlich an sich verändernde Gegebenheiten anzupassen. Andererseits bilden sie eine gute Basis in den Diskussionen auf internationaler Ebene. Internationale Standards bilden die Zertifizierungsgrundlage für die Aspekte Interoperabilität und Informationssicherheit. Erst auf dieser Basis wird sich für Anwender die Möglichkeit eröffnen, sich von den unterschiedlichen Cloud-Angeboten ein umfassendes, verlässliches Bild zu machen. Als nächsten Schritt planen wir, Cloud Computing in die IT-Grundschutz-Vorgehensweise des BSI einzuarbeiten.

Denn nur, wenn die entsprechenden Dienstleistungen auf hohem Sicherheitsniveau bereitgestellt werden, lassen sich die Potentiale von Cloud-Lösungen – wie hohe Flexibilität und Effizienz, aber auch sinkende Kosten bei der Bereitstellung und Nutzung von Informationstechnologie – wirklich nutzen.

Ich wünsche Ihnen eine aufschlussreiche Lektüre.

Michael Hange
Präsident des Bundesamtes für Sicherheit in der Informationstechnik

Das BSI im Dienst der Öffentlichkeit

Das Bundesamt für Sicherheit in der Informationstechnik wurde am 1. Januar 1991 mit Sitz in Bonn gegründet und gehört zum Geschäftsbereich des Bundesministeriums des Innern.

Mit seinen derzeit rund 550 Mitarbeiterinnen und Mitarbeitern und 62 Mio. Euro Haushaltsvolumen ist das BSI eine unabhängige und neutrale Stelle für alle Fragen zur IT-Sicherheit in der Informationsgesellschaft.

Als zentraler IT-Sicherheitsdienstleister des Bundes ist das BSI operativ für den Bund, kooperativ mit der Wirtschaft und informativ für den Bürger tätig.

Durch die Grundlagenarbeit im Bereich der IT-Sicherheit übernimmt das BSI als nationale IT-Sicherheitsbehörde Verantwortung für unsere Gesellschaft und ist dadurch eine tragende Säule der Inneren Sicherheit in Deutschland.

Ziel des BSI ist der sichere Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft. IT-Sicherheit soll als wichtiges Thema wahrgenommen und eigenverantwortlich umgesetzt werden. Sicherheitsaspekte sollen schon bei der Entwicklung von IT-Systemen und -Anwendungen berücksichtigt werden.

Das BSI wendet sich mit seinem Angebot an die Anwender und Hersteller von Informationstechnik. Zielgruppe sind die öffentlichen Verwaltungen in Bund, Ländern und Kommunen sowie Privatanwender und Unternehmen.

Das Eckpunktepapier zum Cloud Computing gibt einen kompakten Überblick über die wichtigsten organisatorischen, personellen, infrastrukturellen und technischen Informationssicherheitsmaßnahmen für Cloud Computing Anbieter.

1 Einleitung

1 Einleitung

1.1 Motivation

Das Thema Cloud Computing ist derzeit eines der am meisten diskutierten Themen in der Informationstechnik (IT). Hinter dem Begriff Cloud Computing stehen aber weniger neue Technologien, sondern deren Kombination und konsequente Weiterentwicklung ermöglichen neue IT-Services und neue Geschäftsmodelle.

Wie bei vielen neuen Techniken und Dienstleistungen werden auch beim Cloud Computing die Aspekte Informationssicherheit und Datenschutz intensiv diskutiert und durchaus kritischer beleuchtet als bei schon länger vorhandenen Angeboten. Viele Umfragen und Studien zeigen, dass potentielle Kunden Bedenken bezüglich Informationssicherheit und Datenschutz beim Cloud Computing haben, die einem verstärkten Einsatz entgegen stehen. Bei den Nutzern von Cloud-Angeboten muss noch das notwendige Vertrauen aufgebaut werden.

Das BSI hat daher Empfehlungen für sicheres Cloud Computing erstellt, die sich zunächst an Cloud Service Provider (CSP) richten. CSPs haben die Möglichkeiten und die Pflicht, Informationssicherheit in einem angemessenen Umfang umzusetzen. Das vorliegende Eckpunktepapier kann von CSPs als Richtschnur für die Umsetzung von Sicherheitsmaßnahmen genutzt werden. Andererseits können Cloud-Nutzer, die sich mit den vorliegenden Empfehlungen beschäftigen, die CSPs nach deren Umsetzung fragen. Der erste Schritt für einen Cloud-Kunden sollte es jedoch immer sein, sich über die Schutzbedürftigkeit der eigenen Daten und Anwendungen klar zu werden. Davon hängt im Wesentlichen ab, ob und unter welchen Rahmenbedingungen geschäftsrelevante Daten und Anwendungen in die Cloud verlagert werden können.

Das Eckpunktepapier stellt einen Überblick über die wesentlichen Felder von Cloud Computing dar, in denen Sicherheit umgesetzt werden sollte. Nicht für alle Cloud Services sind alle aufgeführten Punkte gleich relevant. Da sich beispielsweise die Gefährdungslage für Private und Public Clouds in manchen Bereichen unterscheidet, müssen zum Teil auch andere Sicherheitsmaßnahmen umgesetzt werden.

Das vorliegende Dokument betrachtet nicht nur Cloud-spezifische Aspekte, sondern richtet den Blick auch auf grundlegende Anforderungen der Informationssicherheit, da diese die Basis bilden, auf der alle Cloud-Dienste aufsetzen sollten. Die Empfehlungen wurden weitgehend abstrakt gehalten, ohne detaillierte Anweisungen für deren Umsetzung zu geben. Dies würde zum einen den Umfang des Dokuments sprengen und zum anderen lässt dies die Vielfältigkeit der Cloud-Angebote nicht zu. Die Bewertung der Sicherheit eines bestimmten Angebots muss daher immer auch individuell erfolgen.

1.2 Zielsetzung

Obwohl weltweit IT-Dienstleistungen aus der „Wolke“ immer stärker in Anspruch genommen werden, zeigen fast alle Umfragen und Studien, dass es auch eine Vielzahl von Bedenken gibt, die Anwender vor der Nutzung von Cloud Computing Diensten zurückschrecken lassen. Als eines der größten Hindernisse wird immer wieder mangelndes Vertrauen in die Sicherheit der bereitgestellten Services genannt. Als zentrale Stelle des Bundes für die Informationssicherheit ist es dem BSI wichtig, die Aufbauphase von Cloud Services aktiv mitzugestalten.

Primäres Ziel des vorliegenden Eckpunktepapiers ist es, eine Grundlage für die Diskussion zwischen CSPs und Cloud-Kunden zu bieten. Als weitergehendes Ziel soll dieses Papier die Grundlage bilden, um darauf aufbauend konkrete Empfehlungen für Unternehmen und Behörden zur Absicherung von Cloud Services zu erarbeiten. Das Eckpunktepapier ist ein erster Schritt in Richtung zur Schaffung von Standards, auf deren Basis die Sicherheit von Cloud Computing Plattformen überprüft werden kann. Die im vorliegenden Papier formulierten Anforderungen werden auch künftig weiter diskutiert und, wo erforderlich, überarbeitet und auch weitergehende Details ausgearbeitet werden. Ziel ist es aber nicht, die Eckpunkte weiter zu konkretisieren. Diese sollen die jetzige Tiefe beibehalten, weitergehende Ausarbeitungen und Detaillierungen zum Themenbereich Cloud Computing werden allerdings im IT-Grundschutz einfließen, beispielsweise in Form von IT-Grundschutz-Bausteinen oder Kurzstudien. Geplant ist die Entwicklung von IT-Grundschutz-Bausteinen

sowohl für die sichere Nutzung als auch für die sichere Bereitstellung von Cloud-Diensten. Außerdem muss der BSI-Standard 100-2 zur Integration von Cloud-Aspekten in die IT-Grundschutz-Vorgehensweise angepasst werden, insbesondere im Bereich der Modellierung komplexer, virtualisierter Informationsverbünde.

1.3 Adressatenkreis

Das Eckpunktepapier wendet sich an IT-affine Personen, die mit der Bereitstellung bzw. Nutzung von Cloud Services befasst sind. Die Themen der Informationssicherheit werden angerissen und setzen ein Grundverständnis von Informationssicherheit auf technischer, infrastruktureller, personeller und organisatorischer Ebene voraus.

Die Empfehlungen wenden sich dabei in erster Linie an CSPs, die diese Dienste für Unternehmen und Behörden zur Verfügung stellen, sowie an professionelle Anwender. Sie richten sich nicht unmittelbar an Privatanwender, die einzelne Cloud Services nutzen, können aber von diesen als Anregung in Sicherheitsfragen mit genutzt werden.

1.4 Anwendungsweise

Die im Folgenden aufgeführten Punkte zeigen auf einem abstrakten Niveau auf, welche Sicherheitsmaßnahmen von einem CSP umzusetzen sind. Eine strukturierte Vorgehensweise und ein effektives Management der Informationssicherheit sind unabdingbare Voraussetzungen, um ein angemessenes Sicherheitsniveau in einem Unternehmen oder einer Behörde erfolgreich zu erzielen und aufrechtzuerhalten. Wie ein funktionierendes Managementsystem für Informationssicherheit aufgebaut werden kann und was dies umfassen sollte, ist in einschlägigen Normen wie ISO 27001 oder dem BSI-Standard 100-2 zur IT-Grundschutz-Vorgehensweise beschrieben. Zum Schutz von Cloud Computing Diensten müssen außerdem die für Cloud Computing spezifischen Gefährdungen analysiert und passende Sicherheitsmaßnahmen dagegen identifiziert und umgesetzt werden.

Jeder CSP muss daher in einer Risikoanalyse ermitteln, welche Gefährdungen für die von ihm betriebenen Dienste aktuell und relevant sind, welche Auswirkungen diese haben können und wie die erkannten Risiken behandelt werden sollen, beispielsweise durch spezifische Sicherheitsmaßnahmen. In abgespeckter Form müssen auch Cloud-Nutzer die Risiken bewerten, die für sie durch eine Verlagerung von Daten oder Anwendungen in die Cloud entstehen können. Die in diesem Eckpunktepapier vorgelegten Sicherheitsempfehlungen bilden ein Rahmenwerk, um die aus Sicht des BSI kritischen Bereiche beim Cloud Computing zu adressieren.

Bei der Risikobetrachtung steht ein CSP vor der Herausforderung, dass er den Wert bzw. den Schutzbedarf der Kundendaten meist im Vorfeld nicht kennt. Ein Ausweg wäre, für alle Kunden und ihre Daten ein hohes oder sehr hohes Schutzniveau anzubieten. Dies ist aber erfahrungsgemäß für Daten mit einem normalen Schutzbedarf zu teuer. CSPs sollten das Thema Informationssicherheit frühzeitig gegenüber ihren Kunden ansprechen. Informationssicherheit gehört mit zu den wesentlichen Entscheidungsgründen von Kunden, wenn es um die Auswahl von Cloud Service Anbietern und konkreter Cloud-Dienstleistungen geht. Daher sollten CSPs ihren Kunden darlegen, wie gut sie in puncto Informationssicherheit aufgestellt sind. Dazu gehört, dass sie den Kunden aufzeigen, welche Sicherheitsmaßnahmen bei ihren Angeboten zum Standardumfang gehören und welche optional erhältlich sind, aber sie sollten die Kunden auch darauf hinweisen, welche Sicherheitsmaßnahmen diese selber ergreifen müssen.

1.5 Thematische Abgrenzung der BSI-Sicherheitsempfehlungen

In diesem Dokument liegt der Schwerpunkt auf Sicherheitsbetrachtungen der Cloud-basierten Verarbeitung von Informationen, die einen normalen bis hohen Schutzbedarf haben, wie z. B. firmenvertrauliche Informationen, schützenswerte personenbezogene Daten. Die Festlegung des Schutzbedarfs von Informationen, Anwendungen und IT-Systemen orientiert sich an den Schutzbedarfskategorien nach IT-Grundschutz (siehe BSI-Standard 100-2 [1]). Der Schutz von Informationen, die als staatliche Verschlusssache eingestuft wurden, wird in diesem Dokument nicht explizit betrachtet.

Bei der Erstellung der Eckpunkte standen Vertraulichkeit und Verfügbarkeit als die zu schützenden Grundwerte der Informationssicherheit im Vordergrund. Die Sicherheitsempfehlungen sind daher nach Vertraulichkeit und Verfügbarkeit unterteilt, während eine dezidierte Betrachtung nach dem Grundwert Integrität nicht vorgenommen wurde.

Die aufgeführten Sicherheitsempfehlungen sind drei Kategorien zugeordnet:

» Die **Kategorie B** (=Basisanforderung) umfasst die Basisanforderungen, die an jeden Cloud Service Anbieter gestellt werden.

» Die **Kategorie C+** (=Vertraulichkeit hoch, Confidentiality) umfasst zusätzliche Anforderungen, wenn Daten mit einem hohen Schutzbedarf bezüglich Vertraulichkeit verarbeitet werden sollen.

» Die **Kategorie A+** (=Verfügbarkeit hoch, Availability) umfasst zusätzliche Anforderungen, wenn Dienstleistungen mit einem hohen Schutzbedarf bezüglich Verfügbarkeitsbedarf in Anspruch genommen werden sollen.

In den Tabellen zur Übersicht über die Sicherheitsempfehlungen in den einzelnen Bereichen wird außerdem noch mit Pfeilen aufgezeigt, wie das BSI das Gefährdungspotential in diesem Bereich für Private bzw. Public Clouds einschätzt. Ein Pfeil nach rechts (⇨) symbolisiert ein durchschnittliches Gefährdungspotential, ein Pfeil nach oben (⇗) bedeutet erhöhtes Gefährdungspotential.

Alle genannten Anforderungen gelten für IaaS, PaaS und SaaS, soweit nicht anders vermerkt.

Aufgrund der dynamischen Entwicklungen im Bereich Cloud Computing wird es auch weiterhin erforderlich sein, die nachfolgend dargestellten Sicherheitsempfehlungen regelmäßig zu überprüfen und anzupassen sowie unter Umständen auch zusätzliche Anforderungen hinzuzunehmen. Aktualisierte Versionen dieses Eckpunktepapiers werden auf dem BSI-Webserver www.bsi.bund.de veröffentlicht.

2 Cloud Computing Grundlagen

2 Cloud Computing Grundlagen

2.1 Was ist Cloud Computing?

Bisher konnte sich für den Begriff Cloud Computing keine Definition als allgemeingültig durchsetzen. In Publikationen oder Vorträgen werden häufig Definitionen verwendet, die sich zwar meist ähneln, aber die doch immer wieder variieren. Eine Definition, die in Fachkreisen meist herangezogen wird, ist die Definition der US-amerikanischen Standardisierungsstelle NIST (National Institute of Standards and Technology) [2], die auch von der ENISA genutzt wird [3]:

„Cloud Computing ist ein Modell, das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können."

Folgende fünf Eigenschaften charakterisieren gemäß der NIST-Definition einen Cloud Service:

» On-demand Self Service: Die Provisionierung der Ressourcen (z. B. Rechenleistung, Storage) läuft automatisch ohne Interaktion mit dem Service Provider ab.

» Broad Network Access: Die Services sind mit Standard-Mechanismen über das Netz verfügbar und nicht an einen bestimmten Client gebunden.

» Resource Pooling: Die Ressourcen des Anbieters liegen in einem Pool vor, aus dem sich viele Anwender bedienen können (Multi-Tenant Modell). Dabei wissen die Anwender nicht, wo die Ressourcen sich befinden, sie können aber vertraglich den Speicherort, also z. B. Region, Land oder Rechenzentrum, festlegen.

» Rapid Elasticity: Die Services können schnell und elastisch zur Verfügung gestellt werden, in manchen Fällen auch automatisch. Aus Anwendersicht scheinen die Ressourcen daher unendlich zu sein.

» Measured Services: Die Ressourcennutzung kann gemessen und überwacht werden und entsprechend bemessen auch den Cloud-Anwendern zur Verfügung gestellt werden.

Diese Definition gibt die Vision von Cloud Computing wieder, wobei davon abgesehen werden sollte, die einzelnen Punkte zu dogmatisch zu sehen. So wird z. B. eine ubiquitäre Verfügbarkeit bei Private Clouds eventuell gar nicht angestrebt.

Nach der Cloud Security Alliance (CSA) hat Cloud Computing neben der oben erwähnten Elastizität und dem Self Service noch folgende Eigenschaften [4]:

» Service orientierte Architektur (SOA) ist eine der Grundvoraussetzungen für Cloud Computing. Die Cloud-Dienste werden in der Regel über ein sogenanntes REST-API angeboten.

» In einer Cloud-Umgebung teilen sich viele Anwender gemeinsame Ressourcen, die deshalb mandantenfähig sein muss.

» Es werden nur die Ressourcen bezahlt, die auch tatsächlich in Anspruch genommen wurden (Pay per Use Model), wobei es auch Flatrate-Modelle geben kann.

Begriffsdefinition

Um für alle künftigen Arbeiten rund um Cloud Computing eine einheitliche Grundlage zu haben, hat das BSI folgende Definition für den Begriff „Cloud Computing“ festgelegt:

Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das

komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

In diesem Dokument wird der Begriff „Cloud Computing" entsprechend benutzt, wobei die von NIST und CSA aufgestellten Charakteristika stets im Hinterkopf zu halten sind. So ist eine einfache Webanwendung in der Regel kein Cloud Computing, obwohl dies von den Marketingabteilungen der Hersteller oft so bezeichnet wird.

2.2 Was unterscheidet eine Public Cloud von einer Private Cloud?

NIST unterscheidet vier Bereitstellungsmodelle (Deployment Models):

» 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 kann dabei im Rechenzentrum der eigenen Institution oder einer fremden Institution stehen.

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

» 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.

» Werden mehrere Cloud Infrastrukturen, die für sich selbst eigenständig sind, über standardisierte Schnittstellen gemeinsam genutzt, wird dies **Hybrid Cloud** genannt.

Die oben genannten Definitionen decken aber nicht alle Varianten von Cloud Angeboten ab, was zu weiteren Definitionen wie „Virtual Private Cloud", etc. führt. Während bei einer Private Cloud, bei der im Prinzip Anbieter und Nutzer identisch sind, der Nutzer die komplette Kontrolle über

die genutzten Services hat, überträgt der Nutzer bei einer Public Cloud die Kontrolle an den Cloud Computing Anbieter.

Im Weiteren wird in diesem Dokument nur zwischen Private Cloud und Public Cloud unterschieden, die gemäß der obigen Definition die ganze Spannbreite der Cloud-Bereitstellungsmodellen darstellen. Bei allen Modellen, die „zwischen" diesen beiden Extremen liegen, muss hinterfragt werden, ob die Gefährdungen z. B. durch gemeinsam genutzte Infrastrukturen eher denen einer Private Cloud oder einer Public Cloud ähneln.

2.3 Welche verschiedenen Servicemodelle werden im Cloud Computing angeboten?

Grundsätzlich können drei verschiedene Kategorien von Servicemodellen unterschieden werden:

1. **Infrastructure as a Service (IaaS)**
   Bei IaaS werden IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netze als Dienst angeboten. 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 z. B. Rechenleistung, Arbeitsspeicher und Datenspeicher anmieten und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.

2. **Platform as a Service (PaaS)**
   Ein PaaS-Provider stellt eine komplette Infrastruktur bereit und bietet dem Kunden auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. So kann die Plattform z. B. Mandantenfähigkeit, Skalierbarkeit, Zugriffskontrolle, Datenbankzugriffe, etc. als Service zur Verfügung stellen. 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 CSP in der Regel eigene Werkzeuge anbietet.

3. **Software as a Service (SaaS)**
   Sämtliche Angebote von Anwendungen, die den Kriterien des Cloud Computing entsprechen, fallen in diese Kategorie. Dem Angebotsspektrum sind hierbei keine Grenzen gesetzt. Als Beispiele seien Kontaktdatenmanagement, Finanzbuchhaltung, Textverarbeitung oder Kollaborationsanwendungen genannt.

Der Begriff „as a Service" wird noch für eine Vielzahl weiterer Angebote benutzt, wie z. B. für Security as a Service, BP as a Service (Business Process), Storage as a Service, so dass häufig auch von „XaaS" geredet wird, also „irgendwas als Dienstleistung". Dabei lassen sich die meisten dieser Angebote zumindest grob einer der obigen Kategorien zuordnen.

Die Servicemodelle unterscheiden sich auch im Einfluss des Kunden auf die Sicherheit der angebotenen Dienste. Bei IaaS hat der Kunde die volle Kontrolle über das IT-System vom Betriebssystem aufwärts, da alles innerhalb seines Verantwortungsbereichs betrieben wird, bei PaaS hat er nur noch Kontrolle über seine Anwendungen, die auf der Plattform laufen, und bei SaaS übergibt er praktisch die ganze Kontrolle an den CSP.

2.4 Was unterscheidet Cloud Computing vom klassischen IT-Outsourcing?

Beim Outsourcing werden Arbeits-, Produktions- oder Geschäftsprozesse einer Institution ganz oder teilweise zu externen Dienstleistern ausgelagert. Dies ist ein etablierter Bestandteil heutiger Organisationsstrategien. Das klassische IT-Outsourcing ist meist so gestaltet, dass die komplette gemietete Infrastruktur exklusiv von einem Kunden genutzt wird (Single Tenant Architektur), auch wenn Outsourcing-Anbieter normalerweise mehrere Kunden haben. Zudem werden Outsourcing-Verträge meistens über längere Laufzeiten abgeschlossen.

Die Nutzung von Cloud Services gleicht in vielem dem klassischen Outsourcing, aber es kommen noch einige Unterschiede hinzu, die zu berücksichtigen sind:

» Aus wirtschaftlichen Gründen teilen sich in einer Cloud mehrere Nutzer eine gemeinsame Infrastruktur.

» Cloud Services sind dynamisch und dadurch innerhalb viel kürzerer Zeiträume nach oben und unten skalierbar. So können Cloud-basierte Angebote rascher an den tatsächlichen Bedarf des Kunden angepasst werden.

» Die Steuerung der in Anspruch genommenen Cloud-Dienste erfolgt in der Regel mittels einer Webschnittstelle durch den Cloud-Nutzer selbst. So kann der Nutzer automatisiert die genutzten Dienste auf seine Bedürfnisse zuschneiden.

» Durch die beim Cloud Computing genutzten Techniken ist es möglich, die IT-Leistung dynamisch über mehrere Standorte zu verteilen, die geographisch weit verstreut sein können (Inland ebenso wie Ausland).

» Der Kunde kann die genutzten Dienste und seine Ressourcen einfach über Web-Oberflächen oder passende Schnittstellen administrieren, wobei wenig Interaktion mit dem Provider erforderlich ist.

2.5 Strategische Planung der Cloud Computing Services durch den Nutzer

Bevor geschäftskritische Informationen oder Anwendungen in die Cloud ausgelagert werden, muss vorher eine Cloud-Strategie festgelegt werden, in der die wesentlichen Rahmenbedingungen geklärt werden. Dazu muss immer eine individuelle Sicherheitsanalyse für die auszulagernden Informationen oder Anwendungen durchgeführt werden. In der Cloud-Strategie ist unter anderem festzuhalten, wie die IT-Struktur aussieht (z. B. bei IaaS), wie bestehende IT-Systeme oder Geschäftsprozesse abgegrenzt und getrennt werden können, wie alle betrieblichen und rechtlichen Rahmenbedingungen aussehen und wie der Schutzbedarf der auszulagernden Informationen oder Anwendungen ist.

Typischerweise haben CSPs zwar ihre Angebote auf bestimmte Arten von Informationen oder Anwendungen zugeschnitten. Dabei stehen sie aber vor der Herausforderung, dass sie den spezifischen Schutzbedarf der Kundendaten nicht kennen. Sie könnten für alle Kundendaten ein hohes oder sehr hohes Schutzniveau anbieten, aber das dürfte für Daten mit einem normalen Schutzbedarf zu teuer sein.

Um jedem Cloud-Kunden einen Service anbieten zu können, der Kunden aus verschiedenen Bereichen sowohl funktional als auch finanziell überzeugt, sollten CSPs frühzeitig Informationssicherheit gegenüber den Cloud-Kunden thematisieren. CSPs sollten ihren Kunden darlegen, welche Sicherheitsmaßnahmen bei ihren Angeboten zum Standardumfang gehören, welche zusätzlich zugekauft werden können und für welche Sicherheitsmaßnahmen die Kunden selbst verantwortlich sind. Dies hilft auch, Missverständnissen vorzubeugen. So werden hohe Schäden, die von Zwischenfällen wie Datenverlusten verursacht werden, oft dem CSP angelastet, obwohl es der Cloud-Kunde war, der nicht für ausreichende Sicherheit seiner Daten gesorgt hatte, weil er ein zu niedriges Schutzniveau gewählt hat bzw. ein zu hohes Risiko eingegangen ist.

Deshalb ist es auch für den CSP essentiell, dass der Cloud-Kunde den Schutzbedarf der ausgelagerten Informationen oder Anwendungen kennt bzw. sich im Klaren über das gebotene Schutzniveau ist. So kann der CSP dem Kunden auch mögliche Sicherheitsvorteile deutlich machen, die sich durch die Nutzung von Cloud-Diensten ergeben können.

Schon im Rahmen der strategischen Entscheidung, ob und in welcher Form ein Cloud Service eingesetzt wird, müssen daher die sicherheitsrelevanten Rahmenbedingungen vom Nutzer vorher herausgearbeitet werden. Dies gilt ebenso für Public wie für Private Clouds, und dort genauso jeweils für IaaS, PaaS und SaaS. Hierzu gehören u. a. folgende Schritte:

» Strukturanalyse von IT-Systemen (z. B. bei IaaS) und Anwendungen, um eine Abgrenzung zu ermöglichen und alle Schnittstellen zu identifizieren

» Durchführung einer Schutzbedarfsfeststellung für Informationen, Anwendungen und IT-Systeme

» Eingliederung der Informationen, Anwendungen, Systeme und Cloud Services in Schutzbedarfskategorien

» Klärung der betrieblichen und rechtlichen Rahmenbedingungen

» Festlegung der spezifischen Sicherheitsanforderungen an CSPs

So kann der Cloud-Kunde entscheiden, welches Sicherheitsniveau er bei Cloud-Diensten benötigt und einfordern muss.

3 Sicherheitsmanagement beim Anbieter

3 Sicherheitsmanagement beim Anbieter

Abbildung 1 zeigt eine Referenzarchitektur, die grob die Komponenten darstellt, die vielen Cloud Computing Plattformen gemeinsam sind. Diese Referenzarchitektur dient als Diskussionsgrundlage für die nachfolgenden Eckpunkte. Die vorgestellte Referenzarchitektur berücksichtigt die Anregungen ähnlicher Referenzarchitekturen, wie sie z. B. von NIST [5], IBM [6] und der Cloud Computing Use Cases Group [7] verwendet werden.

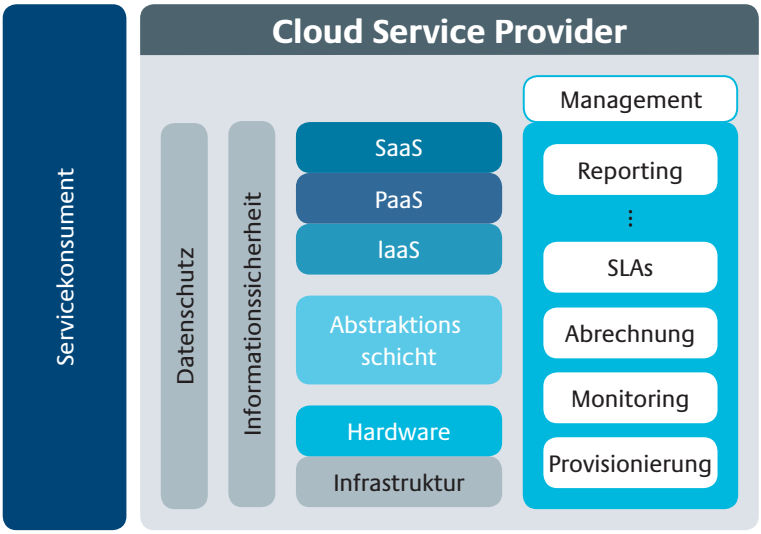

Abbildung 1: Referenzarchitektur für Cloud Computing Plattformen

Eine genaue Betrachtung der zugrunde gelegten Referenzarchitektur zeigt, dass ein Provider zur Erbringung von Cloud Services eine Vielzahl von Aufgaben erledigen muss. Zu den typischen Aufgaben eines Public CSP zählen u. a.:

» die Bereitstellung eines Service-Katalogs zur Beschreibung der angebotenen Dienste,

» die Provisionierung bzw. De-Provisionierung von Ressourcen wie z. B. virtuellen Maschinen, Load Balancern, virtuellen Datenspeichern, IP- und MAC-Adressen und

» die für den Kunden nachvollziehbare Abrechnung der in Anspruch genommenen Services.

Eine andere wichtige Aufgabe ist die Überwachung der bereitgestellten Dienste, um die garantierte Dienstgüte einhalten zu können. Diese Überwachung läuft permanent. Etwaige Störungen oder Ausfälle von Ressourcen z. B. Virtualisierungsserver, virtuelle Maschine, Load-Balancer, etc. müssen zeitnah erkannt werden, so dass entsprechende Gegenmaßnahmen schnellstmöglich eingeleitet werden können. Weitere Aufgaben neben dem Sicherheitsmanagement, die üblicherweise zum Repertoire eines CSP gehören, sind:

» Patch- und Änderungsmanagement

» Konfigurationsmanagement

» Netzmanagement

» System Management

» Application Management

» Reporting

Die Komplexität und Vielzahl der oben beschriebenen Aufgaben erfordert eine strukturierte Herangehensweise. Insofern sollte jeder CSP standardisierte Vorgehensmodelle wie ITIL oder COBIT einsetzen, die als Orientierung bei der Umsetzung von IT-Prozessen dienen können.

Vertrauen in den CSP und seine Angebote wird derzeit als wesentliche Motivation genannt, wenn nach den Gründen gefragt wird, warum sich Anwender für oder gegen Cloud-Angebote entscheiden. Vertrauen basiert auf der Einschätzung, ob ein Anbieter alle Risiken ausreichend, angemessen und nachhaltig abgedeckt hat, sowohl diejenigen aus dem Bereich der Informationssicherheit als auch aus Bereichen wie Datenschutz, Technik und Recht.

Für ein zuverlässiges und sicheres Cloud Computing ist als Grundlage ein effizientes Management der Informationssicherheit (Information Security Management System, ISMS) auf Seiten des CSP unerlässlich. Das BSI empfiehlt, sich für Aufbau und Betrieb eines ISMS an ISO 27001/2 oder bevorzugt am BSI-Standard 100-2 zur IT-Grundschutz-Vorgehensweise (der ISO 27001/2 abdeckt) zu orientieren.

Wesentliche Bestandteile eines ISMS sind eine funktionierende Sicherheitsorganisation und ein Informationssicherheitskonzept als Werkzeuge des Managements zur Umsetzung der Sicherheitsstrategie. Ein CSP sollte die Sicherheitsorganisation nutzen, um hierüber geeignete Ansprechpartner für seine Kunden zu benennen, die Sicherheitsfragen der Kunden beantworten können. Informationssicherheit ist ein Prozess und sollte daher im Sinne eines PDCA-Zyklus (Plan-Do-Check-Act) fortlaufend weiterentwickelt werden.

Damit CSPs nachweisen können, dass sie auch bei hohem Schutzbedarf bezüglich Vertraulichkeit und Verfügbarkeit ausreichend Sicherheit gewährleisten, ist eine Zertifizierung des Informationssicherheitsmanagements sinnvoll. Vorzugsweise sollten CSPs nach ISO 27001 auf Basis von IT-Grundschutz, ISO 27001 oder einem anderen etablierten Standard zertifiziert sein.

Hinweis:
Hier und im Folgenden sind die aufgeführten Sicherheitsempfehlungen danach unterteilt, ob sie sich an Private oder Public Clouds richten und sind jeweils drei Kategorien zugeordnet. Dabei steht:

» **B** für Basisanforderung (richtet sich an jeden Cloud Service Anbieter),

» **C+** (=Vertraulichkeit hoch, Confidentiality high) umfasst zusätzliche Anforderungen für Bereiche mit hohem Schutzbedarf bei Vertraulichkeit,

» **A+** (=Verfügbarkeit hoch, Availability high) umfasst zusätzliche Anforderungen für Bereiche mit hohem Verfügbarkeitsbedarf.

Ein Pfeil nach rechts (⇨) symbolisiert ein durchschnittliches Gefährdungspotential, ein Pfeil nach oben (⇗) erhöhtes Gefährdungspotential bei Private oder Public Clouds.

Sicherheitsmanagement beim Anbieter	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
Definiertes Vorgehensmodell für alle IT-Prozesse (z. B. nach ITIL, COBIT)	✓			✓		
Implementation eines anerkannten Informationssicherheits-Managementsystems (z. B. nach BSI Standard 100-2 (IT-Grundschutz), ISO 27001)	✓			✓		
Nachhaltige Umsetzung eines Informationssicherheitskonzepts für die Cloud	✓			✓		
Nachweis einer ausreichenden Informationssicherheit (Zertifizierung)		✓	✓		✓	✓
Angemessene Organisationsstruktur für Informationssicherheit beim CSP (inklusive Benennung von Ansprechpartnern für Kunden zu Sicherheitsfragen)	✓			✓		

4 Sicherheitsarchitektur

4 Sicherheitsarchitektur

Soll eine Cloud Computing Plattform wirksam abgesichert werden, müssen alle Aspekte betrachtet werden, die die Vertraulichkeit, Integrität und Verfügbarkeit der dort gespeicherten Informationen gefährden können. Neben einem gut strukturierten Vorgehensmodell für alle IT-Prozesse sind insbesondere der Aufbau einer Sicherheitsarchitektur zum Schutz der Ressourcen (Mitarbeiter, Gebäude, Netze, IT-Systeme, Anwendungen, Daten, etc.) und eine sichere Isolierung der Mandanten wichtig. Eine robuste Trennung der Kunden auf allen Ebenen des Cloud Computing Stacks (Anwendung, Server, Netze, Storage, etc.) ist eine der grundlegenden Anforderungen, die jede Cloud Computing Plattform erfüllen sollte. Diese Anforderung gilt gleichermaßen für Public Clouds wie auch für Private Clouds. Beim Aufbau einer soliden Sicherheitsarchitektur für Cloud Computing sollten die im Folgenden beschriebenen Aspekte betrachtet werden.

4.1 Rechenzentrumssicherheit

Rechenzentren sind die technische Basis von Cloud Computing. Insofern ist es wichtig, dass jeder CSP die Sicherheit seiner Anlagen nach dem aktuellen Stand der Technik gewährleistet. Dazu zählen eine permanente Überwachung der Zugänge, etwa durch Videoüberwachungssysteme, Bewegungssensoren, Alarmsysteme und geschultes Sicherheitspersonal. Versorgungskomponenten, die für den Betrieb unverzichtbar sind, sollten redundant ausgelegt sein, so zum Beispiel die Stromversorgung, Klimatisierung und Internet-Anbindung. Auch zeitgemäße Vorkehrungen für den Brandschutz müssen umgesetzt sein und regelmäßig getestet werden. Ein Rechenzentrum sollte insgesamt einen Sicherheitsbereich bilden, der sowohl ausreichend vor Elementarschäden, z. B. durch Gewitter oder Hochwasser, als auch vor unbefugtem Eindringen schützt. Fordert ein Kunde eine besonders hohe Verfügbarkeit seiner Dienste, sollte der CSP außerdem Kapazitäten in Ausweich- bzw. Redundanz-Rechenzentren vorhalten, so dass diese den Ausfall eines anderen Rechenzentrums kompensieren können. Die Rechenzentren sollten geografisch so weit voneinander entfernt liegen, dass ein beherrschbares Schadensereignis wie z. B. Feuer, Explosion, Unfälle im Straßen-, Schienen-, Wasser- oder Luftverkehr oder Naturkatastrophen mit

begrenzter Breitenwirkung wie ein Flusshochwasser nicht gleichzeitig das ursprünglich genutzte Rechenzentrum und das, in dem die Ausweichkapazitäten genutzt werden, beeinträchtigen.

Im Bereich SaaS betreiben viele Anbieter keine eigene Infrastruktur. Ist dies der Fall, müssen die hier gestellten Anforderungen von den Subunternehmen, auf die der SaaS-Anbieter zugreift, hier also den Rechenzentrums-Betreibern, erfüllt werden.

Rechenzentrumssicherheit	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
Redundante Auslegung aller wichtigen Versorgungskomponenten (Strom, Klimatisierung der RZ, Internetanbindung, Verkabelung, etc.)	✓			✓		
Überwachung des Zutritts: Zutrittskontrollsystem, Videoüberwachungssysteme, Bewegungssensoren, Sicherheitspersonal, Alarmsysteme, etc.	✓			✓		
Zwei-Faktor-Authentisierung für den Zutritt ins Rechenzentrum	✓			✓		
Brandschutz: Brandmeldeanlage, Brandfrüherkennung, geeignete Löschtechnik, regelmäßige Brandschutzübungen	✓			✓		
Robuste Infrastruktur, die ausreichenden Widerstand gegen Elementarschäden und unbefugtes Eindringen bietet	✓			✓		
Redundante Rechenzentren, die mindestens so weit voneinander entfernt sind, dass ein beherrschbares Schadensereignis nicht gleichzeitig das ursprünglich genutzte Rechenzentrum und das, in dem die Ausweichkapazitäten genutzt werden, beeinträchtigen			✓			✓

4.2 Server-Sicherheit

Die Server stellen die Umgebung dar, auf der die Prozesse und deren Berechnungen zur Ausführung kommen. Daher sollten die auf den Servern eingesetzten Betriebssysteme so gehärtet sein, dass sie möglichst wenig Angriffsflächen bieten. Dazu sollten schon bei der Grundinstallation nur die notwendigen Software-Pakete eingespielt und nicht benötigte Programme und Dienste abgeschaltet oder besser deinstalliert werden. Darüber hinaus sollten Standardmaßnahmen zum Schutz von IT-Systemen, wie etwa Host Firewalls, Host-based Intrusion Detection Systems, etc. umgesetzt und regelmäßig Integritätsüberprüfungen wichtiger Systemdateien durchgeführt werden. Host-based Intrusion Detection Systems sind dadurch gekennzeichnet, dass sie auf dem zu überwachenden IT-System betrieben werden. Sie werden typischerweise eingesetzt, um Angriffe zu erkennen, die auf Anwendungs- oder Betriebssystemebene durchgeführt werden. Beispiele für derartige Angriffe sind Rechteüberschreitungen von Nutzern, Login-Fehlversuche oder Schadsoftware wie Trojanische Pferde.

Die technischen Grundlagen für eine zuverlässige und sichere Bereitstellung sowie Nutzung von Cloud-Diensten bilden eine Breitbandanbindung, standardisierte und weitverbreitete Übertragungsprotokolle, eine serviceorientierte Architektur und vor allem Virtualisierung.

Für die Servervirtualisierung setzen die Anbieter unterschiedliche Hypervisoren ein. Der Hypervisor ist die zentrale Komponente der Servervirtualisierung, die den Zugriff auf die gemeinsam genutzten Ressourcen steuert. Angriffe auf den Hypervisor sind bisher bis auf wenige Ausnahmen nicht in der freien Wildbahn aufgetaucht [8], sondern wurden nur theoretisch oder als Proof-of-Concept beschrieben. Sollte aber ein Angriff gelingen, so sind die Auswirkungen verheerend. Ein Angriff auf den Hypervisor kann beispielsweise durch die Manipulation von CPU-Registern, die die Virtualisierungsfunktionen steuern, durchgeführt werden. Fehler in der Implementierung der Ressourcen, die den virtuellen Maschinen (VMs) durch den Hypervisor zur Verfügung gestellt werden, können ebenfalls zu einer Kompromittierung des Hypervisors führen. Insofern sollten CSPs, die Servervirtualisierung einsetzen, auf zertifizierte und

gehärtete Hypervisoren zurückgreifen. Zur Härtung der Hypervisoren sollten die Empfehlungen zur sicheren Konfiguration von Virtualisierungsservern, die von den Herstellern veröffentlicht werden, herangezogen werden. Grundlage der Zertifizierung sollten die weltweit abgestimmten „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ oder kurz Common Criteria sein. Als Prüftiefe sollte bei der Zertifizierung mindestens Vertrauenswürdigkeitsstufe EAL 4 erreicht worden sein.

Bei Angeboten der Form „IaaS-Compute“ werden den Kunden virtuelle Maschinen zur Verfügung gestellt, z. B. über eine Webschnittstelle. Zur Absicherung der virtuellen Maschinen ist es hilfreich, wenn der Iaas-Anbieter seinen Kunden Richtlinien zur Härtung der virtuellen Maschinen an die Hand gibt. Außerdem sollte es den Kunden möglich sein, eigene Images für die virtuellen Maschinen hochzuladen oder qualitätsgesicherte Images vom Provider zu beziehen.

Server-Sicherheit	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Technische Maßnahmen zum Schutz des Hosts (Host Firewalls, regelmäßige Integritätsüberprüfungen, Host-based Intrusion Detection Systems)	✓			✓		
Sichere Grund-Konfiguration des Hosts (z. B. Einsatz gehärteter Betriebssysteme, Deaktivierung unnötiger Dienste, etc.)	✓			✓		
Möglichkeit, für Kunden eigene Images für virtuelle Maschinen einzusetzen oder qualitätsgesicherte Images des Providers zu nutzen (nur bei IaaS)	✓			✓		
Sichere Default-Konfiguration des Gastbetriebssystems durch den Einsatz gehärteter Betriebssysteme, Deaktivierung unnötiger Dienste, etc. (nur bei PaaS/SaaS)	✓			✓		
Einsatz zertifizierter Hypervisoren (Common Criteria mindestens EAL 4)		✓	✓		✓	✓

PaaS- oder SaaS-Anbieter, die auf Servervirtualisierung zurückgreifen, wie z. B. Microsoft mit der Windows Azure Plattform, sollten auch die Sicherheit der Gastbetriebssysteme gewährleisten.

4.3 Netzsicherheit

In der Vergangenheit sind Cloud Computing Plattformen vielfach missbraucht worden, um dort Schadprogramme abzulegen, um über diese Spam zu versenden, um deren Rechenleistung zu nutzen, um Passwörter durch Brute-Force-Angriffe zu knacken oder um auf diesen Command and Control Server (C&C Server) zur Steuerung von Bots zu verstecken. Um solche und ähnliche Angriffe bzw. den Missbrauch der Ressourcen zu verhindern, sollte jeder CSP wirksame Sicherheitsmaßnahmen zur Abwehr netzbasierter Angriffe umsetzen. Zusätzlich zu gängigen IT-Sicherheitsmaßnahmen wie Virenschutz, Trojaner-Detektion, Spam-Schutz, Firewalls, Application Layer Gateway, IDS/IPS-Systeme, sollte insbesondere auch darauf geachtet werden, dass jegliche Kommunikation zwischen CSP und Kunden sowie zwischen den Standorten des Anbieters verschlüsselt ist. Sind zur Erbringung der Services Drittdienstleister notwendig, dann ist die Kommunikation mit ihnen auch zu verschlüsseln.

Aufgrund der Konzentration der Ressourcen in zentralisierten Rechenzentren ist ein besonders für Public Cloud Computing Plattformen gefährlicher Angriff die Ausführung von Distributed Denial of Service-Angriffen (DDoS-Angriffen). Nach einem Bericht von Arbor Networks, einem Anbieter von Sicherheitslösungen, erreichen DDoS-Angriffe (wie beispielsweise die DNS Amplification/Reflection Attack) mittlerweile enorme Bitraten (über 100 Gbps) [9]. Ein Standard-Backbone ist für eine weit geringere Datenrate ausgelegt. Folglich können viele CSPs DDoS-Angriffe mit hohen Datenraten kaum abwehren. Dies kann gravierende Folgen sowohl für das eigentliche Opfer als auch andere angeschlossene Kunden haben. Vor diesem Hintergrund sollte jeder Public CSP über geeignete Maßnahmen zur Abwehr von DDoS (DDoS-Mitigation) verfügen. Aufgrund der Tatsache, dass viele CSPs DDoS-Angriffe mit hohen Datenraten selbst kaum abwehren können, bietet es sich an, solche Mitigation-Dienste über größere Internet Service Provider (ISPs)

einzukaufen und deren Nutzung in Verträgen zu regeln. Darüber hinaus sollten auch Maßnahmen implementiert werden, um interne DDoS-Angriffe von Cloud-Kunden auf andere Cloud-Kunden erkennen zu können.

Die Fehlkonfiguration eines Systems ist häufig die Ursache für erfolgreiche Angriffe. Da Cloud Computing Plattformen aus vielen verschiedenen Komponenten bestehen, ergibt sich eine hohe Komplexität der Gesamtkonfiguration. Das Ändern eines Konfigurationsparameters bei einer Komponente (z. B. Virtualisierungsserver) kann im Zusammenspiel mit den anderen Komponenten (z. B. Netz oder Storage) zu Sicherheitslücken, Fehlfunktionen und/oder Ausfällen führen. Daher müssen die eingesetzten Komponenten sicher und sorgfältig konfiguriert werden. Auch sollte jeder CSP auf eine geeignete Netzsegmentierung achten, damit Fehler sich nicht beliebig ausbreiten können. Hier bietet es sich an, abhängig vom Schutzbedarf unterschiedliche Sicherheitszonen innerhalb des Provider-Netzes zu definieren und einzurichten. Beispiele hierfür sind:

» Sicherheitszone für das Management der Cloud

» Sicherheitszone für die Live Migration, falls Servervirtualisierung eingesetzt wird

» Sicherheitszone für das Storage-Netz

» Eigene Sicherheitszonen für die virtuellen Maschinen eines Kunden bei IaaS

Das Management-Netz des CSP sollte vom Datennetz isoliert sein.

Wird die Cloud-Infrastruktur bzw. werden die Cloud Services fernadministriert, so muss dies über einen sicheren Kommunikationskanal (z. B. SSH, IPSec, TLS/SSL, VPN) erfolgen.

Hat ein Servicekonsument besonders hohe Anforderungen an die Verfügbarkeit der in Anspruch genommenen Dienste, sollten die Standorte des CSP redundant untereinander vernetzt sein.

Netzsicherheit	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Sicherheitsmaßnahmen gegen Malware (Virenschutz, Trojaner-Detektion, Spam-Schutz, etc.)	✓			✓		
Sicherheitsmaßnahmen gegen netzbasierte Angriffe (IPS/IDS-Systeme, Firewall, Application Layer Gateway, etc.)		✓	✓	✓		
DDoS-Mitigation (Abwehr von DDoS-Angriffen)			✓	✓		
Geeignete Netzsegmentierung (Isolierung des Management-Netzs vom Datennetz)	✓			✓		
Sichere Konfiguration aller Komponenten der Cloud-Architektur	✓			✓		
Fernadministration durch einen sicheren Kommunikationskanal (z. B. SSH, IPSec, TLS/SSL, VPN)	✓			✓		
Verschlüsselte Kommunikation zwischen Cloud Computing Anbieter und Cloud Computing Nutzer (z. B. TLS/SSL)	✓			✓		
Verschlüsselte Kommunikation zwischen Cloud Computing Standorten	✓			✓		
Verschlüsselte Kommunikation mit Drittdienstleistern, falls diese für das eigene Angebot notwendig sind	✓			✓		
Redundante Vernetzung der Cloud-Rechenzentren			✓			✓

4.4 Anwendungs- und Plattformsicherheit

Bei Angeboten im Bereich PaaS müssen sich die Kunden nicht mehr explizit um Datenbankzugriffe, Skalierbarkeit, Zugriffskontrolle, etc. kümmern, sondern diese Funktionalitäten werden von der Plattform bereitgestellt. Aufgrund der Tatsache, dass die Kunden zur Entwicklung eigener Software auf Kernfunktionalitäten der Plattform zurückgreifen, kann eine sichere Software-Entwicklung auf Seiten der Kunden allerdings nur

gelingen, wenn der gesamte Software-Stack der Plattform professionell und sicher entwickelt bzw. weiterentwickelt wird. Typischerweise setzen CSPs nicht nur eine Vielzahl verschiedener Software-Komponenten ein, sondern entwickeln diese auch weiter, um die Dienste der Laufzeit-Umgebung ihren Kunden optimal bereitstellen zu können. Bei der Software-Entwicklung muss jeder CSP Sicherheit als festen Bestandteil des Software Development Life Cycle Prozess (SDLC-Prozess) etabliert haben. Sicherheitsaspekte müssen in allen Phasen des Software-Entwicklungsprozesses berücksichtigt werden und es dürfen nur Programme bzw. Module zum Einsatz kommen, die ordnungsgemäß getestet und auch seitens der Sicherheitsverantwortlichen des CSP freigegeben wurden.

Software, die von den Kunden entwickelt wird, benötigt nicht nur eine sichere Basis (die vom CSP zu stellen ist), sondern auch dabei müssen Sicherheitsaspekte beachtet werden. Es ist zu empfehlen, dass der CSP entsprechende Anwenderrichtlinien für Kunden zur Erstellung von sicheren Anwendungen bereitstellt, damit durch die von Kunden selbstentwickelten Programme gewisse Mindestanforderungen an Sicherheit, Dokumentation und Qualität erfüllt werden. Dies ist nicht nur hilfreich für die Kunden, sondern unterstreicht auch die Kompetenz des Providers und reduziert die Gefahr, dass Sicherheitslücken in Kundensoftware andere Kunden beeinträchtigen.

Wenn der CSP zur Bereitstellung der Plattform-Dienste auch Drittdienstleister hinzuzieht, so gelten diese Anforderungen gleichermaßen auch für sie. Neben Code Reviews sollten zusätzlich auch automatische Review-Tools eingesetzt sowie Vulnerability Tests durchgeführt werden. Automatische Review-Tools können beispielsweise häufig vorkommende Programmierfehler, wie Endlosschleifen oder Null-Pointer-Exceptions, erkennen. Bei höherem Schutzbedarf sollte der CSP auch den von den Kunden selbstentwickelten Code automatisch auf Schwachstellen überprüfen.

Bei PaaS teilen sich mehrere Kunden eine gemeinsame Plattform, um Software auszuführen. Eine sichere Isolierung der Kunden-Anwendungen sollte gewährleistet werden, beispielsweise unter Anwendung von Sandboxing Technologien. Eine strikte Isolierung der Kundenbereiche trägt

unter anderem dazu bei, dass von einer Anwendung nicht unberechtigt auf die Daten einer anderen Anwendung zugegriffen werden kann.

Da die Cloud-Kommunikation im Kern ausschließlich auf Web-Technologien beruht, z. B. Webinterfaces für Cloud-Nutzer und Anwendungs-Administrationen, Application Frameworks wie Java und .NET, Kommunikation über HTTP(S), kommt der Sicherheit der Cloud-Anwendungen gegen Angriffe auf Applikationsebene eine noch höhere Bedeutung zu als bei traditionellen Web-Anwendungen. Daher sollte jeder CSP sicherstellen können, dass bei ihm die Prinzipien zur sicheren Software-Entwicklung des Open Web Application Security Project bei der Erstellung der Anwendungen eingehalten werden, die gegen die wichtigsten Sicherheitsrisiken bei Webanwendungen (OWASP Top 10) wirken [10].

Anwendungs- und Plattformsicherheit	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Sicherheit muss Bestandteil des Software Development Life Cycle-Prozesses sein (Reviews, Automatisierte Tests, Vulnerability Tests, etc.)	✓			✓		
Sichere Isolierung der Anwendungen (PaaS)	✓			✓		
Einhaltung von Sicherheits-Mindeststandards der zur Verfügung gestellten Webanwendungen (z. B. Prinzipien zur sicheren Software-Entwicklung nach OWASP)	✓			✓		
Richtlinien für Kunden zur Erstellung von sicheren Anwendungen (PaaS)	✓			✓		
Automatische Überprüfung von Kunden-Anwendungen auf Anwendungs-Schwachstellen, insbesondere vor Inbetriebnahme (PaaS)		✓	✓		✓	✓
Patch- und Änderungsmanagement (zügiges Einspielen von Patches, Updates, Service Packs) sowie Release Management	✓			✓		
Sicherstellung der Patchverträglichkeit auf Testsystemen vor Einspielen in Wirkbetrieb	✓			✓		

Wichtig ist weiterhin ein gut eingespieltes und effektives Patch- und Änderungsmanagement, damit Störungen im Betrieb vermieden sowie Sicherheitslücken minimiert und zeitnah beseitigt werden können. Zur Qualitätssicherung und um Fehler erkennen beziehungsweise zukünftigen Fehlern vorbeugen zu können, sollte jeder Patch und jede Änderung, bevor sie aufgespielt werden, ausreichend getestet und ihre Wirksamkeit bewertet werden.

4.5 Datensicherheit

Der Lebenszyklus von Daten umfasst ihre Erzeugung, die Datenspeicherung, die Datennutzung und -weitergabe und die Zerstörung der Daten. Alle diese Phasen im Daten-Lebenszyklus sollte jeder CSP mit entsprechenden Sicherheitsmechanismen unterstützen.

Zur Speicherung der Daten werden eine Vielzahl von Speichertechniken wie z. B. NAS, SAN, Object Storage, etc. eingesetzt. Allen Speichertechniken ist gemeinsam, dass sich viele Kunden einen gemeinsamen Datenspeicher teilen. In einer solchen Konstellation ist eine sichere Trennung von Kundendaten essentiell und sollte daher gewährleistet sein.

Bei SaaS beispielsweise werden Kundendaten meist in einer gemeinsamen Tabelle gespeichert. Die Unterscheidung der Kunden untereinander erfolgt dann anhand einer sogenannten Tenant-ID. Ist die Webanwendung (geteilte Applikation) unsicher programmiert, dann könnte ein Kunde z. B. über eine SQL-Injection unerlaubt auf die Daten eines anderen Kunden zugreifen, diese löschen oder manipulieren. Um dies zu verhindern, müssen entsprechende Sicherheitsmechanismen umgesetzt werden.

Ähnlich wie bei der traditionellen IT sind Datenverluste auch beim Cloud Computing eine ernst zu nehmende Gefahr. Zur Vermeidung von Datenverlusten sollte jeder CSP regelmäßige Datensicherungen basierend auf einem Datensicherungskonzept durchführen. Durch technische Defekte, falsche Parametrisierung, einer Überalterung der Medien, einer unzureichenden Datenträgerverwaltung oder der Nichteinhaltung von Regeln, die in einem

Datensicherungskonzept gefordert werden, kann es vorkommen, dass sich Backups nicht wieder einspielen lassen und eine Rekonstruktion des Datenbestandes nicht möglich ist. Daher ist es notwendig, dass sporadisch überprüft wird, ob die erzeugten Datensicherungen zur Wiederherstellung verlorener Daten genutzt werden können. Je nachdem, wie lange der Zeitraum zwischen Datensicherung und Wiedereinspielen der Daten aufgrund von Datenverlusten oder anderer Zwischenfälle war, können die letzten Änderungen an den Daten verloren sein. Daher muss ein CSP seine Kunden sofort informieren, wenn Datensicherungen wieder eingespielt werden müssen, insbesondere über deren Stand. Die Datensicherung (Umfang, Speicherintervalle, Speicherzeitpunkte, Speicherdauer, etc.) muss transparent und nachvollziehbar für den Kunden erfolgen.

Hilfreich für die Kunden kann es außerdem sein, wenn Cloud-Anbieter ihnen die Möglichkeit bieten, selbst Datensicherungen anzufertigen.

Aufgrund der zugrunde liegenden Multi-Tenant-Architektur ist eine dauerhafte, also vollständige und zuverlässige Löschung von Kundendaten auf Wunsch eines Servicekonsumenten, beispielsweise nach Beendigung eines Vertragsverhältnisses, oft nur nach einer gewissen Zeitspanne möglich. Dieser Wert sollte in den SLAs kenntlich gemacht werden. Nach Ablauf der definierten Zeitspanne müssen alle Kundendaten dann von allen Speichermedien vollständig und zuverlässig gelöscht worden sein. Um Daten selektiv zu löschen, muss darauf geachtet werden, dass nicht nur die aktuelle Version, sondern auch alle Vorgängerversionen, temporäre Dateien und Dateifragmente gelöscht werden.

Daher muss jeder CSP eine effektive Vorgehensweise zum sicheren Löschen bzw. Vernichten von Daten und Datenträgern haben. Kunden sollten darauf achten, dass vertraglich geregelt ist, zu welchem Zeitpunkt und in welcher Weise der CSP Daten bzw. Datenträger vollständig löschen oder vernichten muss.

Datensicherheit	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Datensicherheit im Lebenszyklus der Kundendaten definieren und umsetzen	✓			✓		
Sichere Isolierung der Kundendaten (z. B. virtuelle Speicherbereiche, Tagging, etc.)	✓			✓		
Regelmäßige Datensicherungen, deren Rahmenbedingungen (Umfang, Speicherintervalle, Speicherzeitpunkte und Speicherdauer) für die Kunden nachvollziehbar sind	✓			✓		
Daten müssen auf Wunsch des Kunden vollständig und zuverlässig gelöscht werden	✓			✓		

4.6 Verschlüsselung und Schlüsselmanagement

Um sensible Informationen sicher speichern, verarbeiten und transportieren zu können, sollten geeignete kryptographische Verfahren und Produkte eingesetzt werden. Die Verwaltung der kryptographischen Schlüssel in Cloud Computing Umgebungen ist komplex und derzeit fehlen entsprechende Werkzeuge zur Schlüsselverwaltung. Deswegen werden ruhende Daten von den meisten Anbietern nicht verschlüsselt. Bei Angeboten der Form „IaaS-Storage“ hat der Kunde jedoch die Möglichkeit, seine Daten vor der Speicherung selbst zu verschlüsseln. Somit behält er die vollständige Kontrolle über die kryptographischen Schlüssel und muss sich naturgemäß auch um die Schlüsselverwaltung kümmern.

Wird seitens des Anbieters verschlüsselt, dann müssen in jeder Lebenszyklus-Phase eines kryptographischen Schlüssels geeignete Sicherheitsmaßnahmen umgesetzt werden, damit Schlüssel vertraulich, integer und authentisch erzeugt, gespeichert, ausgetauscht, genutzt und vernichtet werden. Da beim Einsatz kryptographischer Verfahren sehr viele komplexe Einflussfaktoren zu betrachten sind, sollte jeder CSP hierfür ein Kryptokonzept erstellen. Damit die Kunden wissen, welche Aufgaben im Bereich der

Kryptographie der CSP übernimmt und welche Aspekte sie selbst beachten sollten, ist es sinnvoll, wenn Provider den Kunden eine Übersicht über die eingesetzten kryptographischen Mechanismen und Verfahren zur Verfügung stellen.

Die folgenden Best-Practices der Schlüsselverwaltung sollten umgesetzt werden:

» Die Schlüsselerzeugung sollte in sicherer Umgebung und unter Einsatz geeigneter Schlüsselgeneratoren erfolgen.

» Kryptographische Schlüssel sollten möglichst nur für einen Einsatzzweck dienen.

» Generell sollten Schlüssel nie in klarer Form, sondern grundsätzlich verschlüsselt im System gespeichert werden. Darüber hinaus muss die Speicherung stets redundant gesichert und wiederherstellbar sein, um einen Verlust eines Schlüssels zu vermeiden.

» Die Schlüssel müssen sicher (vertraulich, integer und authentisch) verteilt werden.

» Administratoren der Cloud dürfen keinen Zugriff auf Kundenschlüssel haben.

» Es müssen regelmäßig Schlüsselwechsel durchgeführt werden. Die verwendeten Schlüssel sollten regelmäßig auf ihre Aktualität überprüft werden.

» Der Zugang zu Schlüsselverwaltungsfunktionen sollte eine separate Authentisierung erfordern.

» Die Schlüssel sollten sicher archiviert werden.

» Nicht mehr benötigte Schlüssel (z. B. Schlüssel, deren Gültigkeitsdauer abgelaufen sind) sind auf sichere Art zu löschen bzw. zu vernichten.

Für ein verlässliches Schlüsselmanagement sind ausreichende Kryptographie-Kenntnisse erforderlich. Daher müssen beim CSP Verantwortliche für das Schlüsselmanagement benannt und geschult sein.

Schlüsselmanagement	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Best-Practices der Schlüsselverwaltung umsetzen	✓			✓		
Krypto-Übersicht für Kunden zugänglich machen		✓			✓	

5 ID- und Rechtemanagement

5 ID- und Rechtemanagement

Die Identitäts- und Berechtigungsverwaltung ist ein wichtiger Bestandteil der Zugriffskontrolle. Ein CSP muss diese mit geeigneten organisatorischen, personellen und technischen Maßnahmen absichern. Daher sollte die Identitätsverwaltung von jeder Cloud Computing Plattform unterstützt werden. Die Unterstützung kann darauf basieren, dass ein Serviceanbieter selbst dem Kunden ein ID-Management anbietet oder Schnittstellen zu externen Identitätsanbietern bereitstellt. Für beide Modelle, Serviceanbieter mit oder ohne integriertem ID-Management, werden im Folgenden die Themen Authentisierung und Autorisierung näher betrachtet, die in Cloud Computing Plattformen abgebildet werden müssen.

Authentisierung

Hardware, Software und Services werden beim Cloud Computing von vielen Nutzern in Anspruch genommen. Aufgabe des Identitäts- und Berechtigungs-Managements ist es, dafür zu sorgen, dass nur befugte Personen die IT-Ressourcen nutzen können. Der Zugriff auf alle IT-Systeme oder Dienste muss durch Identifikation und Authentikation der zugreifenden Benutzer oder IT-Systeme abgesichert werden. Für sicherheitskritische Anwendungsbereiche sollte starke Authentisierung verwendet werden, also Zwei-Faktor-Authentisierung, wie es zum Beispiel beim Online-Banking üblich ist. Netzzugriffe sollten grundsätzlich über eine starke Authentisierung abgesichert werden. Diese hohen Anforderungen gelten insbesondere für die Mitarbeiter des CSP: Sie sollten ebenfalls nur über eine starke Authentisierung Zugriff auf die zu administrierenden IT-Ressourcen erhalten, also z. B. über eine Hardware-basierte Authentisierung mit Chipkarten oder USB-Sticks oder über Einmal-Passwörter, die auch von Hardwaregeräten generiert werden können. Dies ist für Zugriffe über das Internet absolut unumgänglich. Greift ein CSP-Administrator aus einem gesicherten Firmennetz über ein VPN, für das er sich bereits mit zwei Faktoren authentisieren musste, auf die Systeme beim CSP zu, dann kann in diesem Fall auf eine erneute Zwei-Faktor-Authentisierung verzichtet werden.

Auch Servicekonsumenten sollten bei hohen Anforderungen an die Sicherheit der bereitgestellten Services nur nach einer starken Authentisierung

(z. B. Zwei-Faktor-Authentisierung) auf die Dienste zugreifen können, wenn der Zugang zum genutzten Dienst direkt über das Internet erfolgt. Greift ein Kunde über ein VPN aus dem abgesicherten Kundennetz auf die Cloud-Dienste zu, für das er sich mit zwei Faktoren authentisieren muss, ist eine zusätzliche Zwei-Faktor-Authentisierung zur Nutzung der Cloud Services nicht zwingend erforderlich.

Bei verschlüsselter Kommunikation zwischen CSP und Servicekonsumenten, wie im Abschnitt 4.3 gefordert, kann zur Erhöhung der Sicherheit der Zugriff auf die Services auf bestimmte IP-Adressen oder Domains beschränkt werden.

Ein weiteres Thema, das beim Cloud Computing eine Schlüsselrolle spielt, ist die Föderation von Identitäten bei der Authentisierung von Unternehmenskunden, bei der Bereitstellung von Single-Sign-On-Lösungen (SSO) und dem Austausch von Identitätsattributen zwischen dem Serviceanbieter und den Identitätsanbietern. Im Unternehmensumfeld sind SAML oder WS-Federation weit verbreitet, wobei SAML deutlich häufiger eingesetzt wird. Die Alternative zu SAML und WS-Federation ist eine SSO-Lösung, die über einen gesicherten VPN-Tunnel eingesetzt wird. Der weitverbreitete SAML-Standard wird häufig in den Versionen 1.1 und 2.0 eingesetzt. Nach Möglichkeit sollte SAML 2.0 unterstützt werden, da in diesem Standard verschiedene proprietäre Erweiterungen integriert wurden und damit eine breite Basis an Einsatzszenarien adressiert werden kann.

Autorisierung

Das Rechtemanagement muss gewährleisten, dass jede Rolle nur die Daten (auch Metadaten) sehen darf, die zur Erfüllung der Aufgabe notwendig sind. Die Zugriffskontrolle sollte rollenbasiert erfolgen und die eingerichteten Rollen und Berechtigungen sollten regelmäßig überprüft werden. Generell sollte das Least Privilege Model genutzt werden, Benutzer und CSP-Administratoren sollten nur die Rechte besitzen, die sie zur Erfüllung ihrer Aufgaben benötigen. Besonderes Augenmerk sollte dabei auf privilegierte Benutzer gerichtet werden. Handelt es sich bei einer

Rolle um einen CSP-Administrator, dann sollte es möglich sein, nachzuweisen, dass tatsächlich nur die für die Aufgabe notwendigen Daten eingesehen wurden. Darüber hinaus sollte das Rechtemanagement in der Lage sein, Datenexporte und -importe von und zum CSP vollständig zu dokumentieren und zu kontrollieren. Und schließlich sollten besonders kritische Administrationstätigkeiten wie z. B. das Einspielen von Patches nur im Vier-Augen-Prinzip durchführbar sein.

ID- und Rechtemanagement	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Starke Authentisierung (Zwei-Faktor-Authentisierung) für Administratoren des CSP	✓			✓		
Rollenbasierte Zugriffskontrolle und regelmäßige Überprüfung der Rollen und Rechte	✓			✓		
Least Privilege Model (Nutzer bzw. CSP-Administratoren sollen nur die Rechte besitzen, die sie zur Erfüllung ihrer Aufgabe benötigen)	✓			✓		
Vier-Augen-Prinzip für kritische Administrationstätigkeiten		✓	✓		✓	✓
Starke Authentisierung (z. B. Zwei-Faktor-Authentisierung) für Cloud-Kunden		✓			✓	

6 Kontrollmöglichkeiten für Nutzer

6 Kontrollmöglichkeiten für Nutzer

Beim Public Cloud Computing begibt sich der Kunde in eine starke Abhängigkeit von seinem Cloud-Dienstleister – er hat schließlich keinen direkten Zugriff mehr auf Hard- und Software und ist auf die Verfügbarkeit der Dienste, die in der „Cloud" laufen, angewiesen. Insofern sollte es dem Kunden möglich sein, die Verfügbarkeit der genutzten Services zu überwachen, z. B. über eine Webschnittstelle oder per API. Dies wird bereits von vielen CSPs praktiziert. In vielen Fällen können sich die Kunden über eine Webseite des CSP den Status der in Anspruch genommenen Dienste anzeigen lassen. Über zusätzlich beim CSP buchbare Dienste oder Tools von Drittanbietern haben die Kunden auch die Möglichkeit, umfassende Monitoring-Informationen über die Performance der genutzten Dienste wie z. B. CPU-Auslastung, Netzauslastung, Durchsatz, Latenz sowie durchschnittliche Transaktionszeit abzufragen.

Kunden sollten darauf achten, dass es ihnen möglich ist, die vertraglich festgehaltene Dienstgüte auch zu überwachen. Der CSP sollte hierfür geeignete Schnittstellen zur Verfügung stellen.

Kontrollmöglichkeiten für Nutzer	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
Kunden müssen die Möglichkeit haben, messbare Größen, wie im SLA vereinbart, zu überwachen	✓			✓		

7 Monitoring und Security Incident Management

7 Monitoring und Security Incident Management

Die Beurteilung der operationellen Sicherheit einer Cloud Computing Plattform setzt ein umfassendes Monitoring voraus. Neben der Überwachung der Performance zur Einhaltung der SLAs und für Abrechnungszwecke ist insbesondere auch das Sicherheitsmonitoring in einer Cloud-Umgebung wichtig. Um die Informationssicherheit im laufenden Betrieb aufrecht zu erhalten, ist es notwendig, die Behandlung von Angriffen bzw. Sicherheitsvorfällen im Vorfeld zu konzipieren und einzuüben. Cloud-Dienste sollten rund um die Uhr (24/7) umfassend überwacht werden und Personal für zeitnahe Reaktionen bei Angriffen bzw. Sicherheitsvorfällen vorgehalten werden. Falls im SLA so geregelt (z. B. bei hohen Anforderungen an die Verfügbarkeit der Cloud Services), sollte das Team beim CSP für Security Incident Handling und Trouble-Shooting für die Kunden ebenfalls rund um die Uhr erreichbar sein.

Zur Nachvollziehbarkeit der Administration sollten alle administrativen Handlungen protokolliert werden. So kann der CSP gegenüber seinem Kunden nachvollziehbar darstellen, wann, wer, welche Änderungen am Service vorgenommen hat.

Zur Erkennung von Angriffen sollten Protokolldateien (z. B. über Systemstatus, fehlgeschlagene Authentisierungsversuche, etc.) und weitere sicherheitsrelevante Datenquellen wie z. B. Auswertungen von Tools zur Netz- und Systemüberwachung (IDS, IPS, Integritätschecker, etc., siehe Abschnitt 4.3) herangezogen und korreliert werden. Hat ein Kunde einen höheren Schutzbedarf an die Vertraulichkeit seiner Information, können bei Bedarf weitere Tools (z. B. zur Data Leakage Prevention) eingesetzt werden, die den Datenfluss im Netz und/oder auf Endgeräten kontrollieren. Sie sollen erkennen oder sogar einschreiten, wenn vertrauliche Informationen über unsichere Wege übertragen werden oder in falsche Hände geraten. Solche Tools überprüfen beispielsweise, ob per E-Mail, Datenaustausch oder bei der Internet-Nutzung bestimmte Informationen übermittelt werden sollen oder ob diese auf CD gebrannt oder auf einen USB-Stick kopiert werden sollen. Da über solche Tools unter Umständen auch Einsicht in vertrauliche oder persönliche Daten genommen werden kann, muss deren Einsatz sorgfältig geplant und zwischen CSP und Kunden abgestimmt werden.

Erkennt der CSP Angriffe gegen die Cloud Computing Plattform, sollte er zeitnah und angemessen reagieren und entsprechende Gegenmaßnahmen einleiten. Aufgrund der Multi-Tenant-Architektur sollte bei der Planung der Detektionsmaßnahmen von Angriffen ein besonderes Augenmerk auch auf interne Angriffe von Cloud-Nutzern auf andere Cloud-Nutzer gerichtet werden. Weiterhin ist es wichtig, Meldungen über neue Schwachstellen in den eingesetzten IT-Komponenten auszuwerten und nachzuprüfen, ob offene Schwachstellen ausgenutzt werden können.

Beim Public Cloud Computing hat der Kunde a priori nur eingeschränkte Einsicht in die Protokolldateien. Dabei sollten die Kunden über eine externe Schnittstelle einen Teil der Protokolldateien abrufen können, z. B. über fehlgeschlagene Authentisierungsversuche. Insofern ist es wichtig, dass der CSP bei Sicherheitsvorfällen zeitnah reagiert und den Kunden über mögliche Auswirkungen informiert, die seine Services betreffen könnten.

Ein weiterer wichtiger Punkt ist eine revisionssichere Speicherung der relevanten Protokolldaten, die der CSP auf Kundenwunsch anbieten sollte.

Neben einer schnellen Information muss der CSP dem Kunden auch alle für ihn relevanten Protokolldaten in einem geeigneten Format zur Verfügung stellen. Hier bietet es sich an, sie in einem für die maschinelle Verarbeitung geeigneten Format zur Verfügung zu stellen, damit der Kunde diese Information bei Bedarf in ein vorhandenes Tool zum Security Incident and Event Management (SIEM) integrieren kann.

Monitoring und Security Incident Management	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
24/7 umfassende Überwachung der Cloud Dienste sowie zeitnahe Reaktion bei Angriffen bzw. Sicherheitsvorfällen	✓			✓		
Erfassung und Auswertung von Datenquellen (z. B. Systemstatus, fehlgeschlagene Authentisierungsversuche, etc.)	✓			✓		
24/7-erreichbares, handlungsfähiges Team für Security Incident Handling und Trouble-Shooting			✓			✓
Mitteilungspflichten des CSP gegenüber dem Kunden über Sicherheitsvorfälle oder Hinweise auf Sicherheitsvorfälle, die den Kunden betreffen könnten	n/a			✓		
Geeignete Bereitstellung relevanter Logdaten durch den CSP	✓			✓		
Logging und Monitoring der Aktivitäten von Administratoren	✓			✓		

8 Notfallmanagement

8 Notfallmanagement

Der vorbeugende Schutz gegen mögliche Gefährdungen ist eine wichtige Aufgabe bei den Bemühungen um Sicherheit. Die Erfahrung zeigt aber, dass gravierende Störungen und Unglücke auch bei bester Vorsorge nicht vollständig verhindert werden können. Und oftmals sind es unverhoffte Ereignisse, welche die größten Risiken mit sich bringen, wie z. B.:

» Im Oktober 2008 konnten, aufgrund des Ausfalls eines Umspannwerks in Hannover, bundesweit in rund 150 Geldinstituten Geldautomaten, Kontoauszugsdrucker und das Online-Banking nicht mehr benutzt werden.

» Im Januar 2009 führten fehlerhaft durchgeführte Wartungsarbeiten in einem Rechenzentrum dazu, dass in ganz Deutschland über Stunden hinweg keine Bahnfahrkarten mehr verkauft werden konnten, die Züge erhebliche Verspätungen aufwiesen oder teilweise sogar ganz ausfielen, und sich zudem vielerorts die Kunden über aus ihrer Sicht unzureichende Informationen durch das betroffene Verkehrsunternehmen beklagten.

» Im April 2010 brachte ein Ausbruch des Vulkans Gletschervulkans Eyjafjalla in Island den Flugverkehr in Europa tagelang nahezu vollständig zum Erliegen, was beispielsweise bei nicht wenigen Unternehmen Produktionsunterbrechungen aufgrund verzögerter Zulieferungen befürchteten ließ.

All diesen Beispielen ist gemeinsam, dass scheinbar lokal begrenzte Ereignisse unerwartete Breitenwirkungen und erhebliche Schäden in anderen Branchen nach sich gezogen haben. Bei näherer Betrachtung dieser und vergleichbarer Vorfälle zeigt sich aber auch immer wieder, dass es bei den betroffenen Institutionen Mängel in der Vorbereitung auf solche Ereignisse gab: Zuständigkeiten sind nicht geregelt, Ausweichkapazitäten fehlen, die Krisenkommunikation ist unzureichend, Notfallpläne sind veraltet oder fehlen vollkommen – die Liste möglicher Mängel ließe sich beliebig verlängern.

Um gegen solche Vorfälle gewappnet zu sein und um angemessen auf Notfallsituationen reagieren zu können, sollte daher jeder CSP über ein funktionierendes Notfallmanagement (Business Continuity Management) verfügen, basierend auf etablierten Standards wie beispielsweise BS 25999

oder BSI-Standard 100-4 [11]. Dazu gehört es, entsprechende organisatorische Strukturen aufzubauen sowie Konzepte zu entwickeln, die eine rasche Reaktion bei auftretenden Notfällen und die rasche Wiederaufnahme zumindest der wichtigsten Geschäftsprozesse ermöglichen.

Eine der wichtigsten Aufgaben im Vorfeld ist es, die betriebenen Dienste und Geschäftsprozesse für den Wiederanlauf zu priorisieren. Dafür muss der CSP deren Verfügbarkeitsanforderungen ermitteln und die Konsequenzen seinen Kunden deutlich machen, da die gesetzten Prioritäten und Wiederanlaufzeiten auf beiden Seiten wirtschaftliche Auswirkungen haben. Hierfür kann eine Einteilung der angebotenen Cloud-Dienste in Wiederanlaufklassen sinnvoll sein.

Darauf aufbauend müssen Notfallpläne und Maßnahmen entwickelt und umgesetzt werden, die eine effektive Notfallbewältigung und eine schnelle Wiederaufnahme der kritischen Geschäftsprozesse entsprechend der vorgenommenen Priorisierung ermöglichen.

Um die Wirksamkeit von Maßnahmen im Bereich des Notfallmanagements zu überprüfen, sollte jeder CSP regelmäßig Tests und Notfallübungen durchführen. Dadurch wird nicht nur überprüft, dass die Strategien und Pläne für die Notfallbewältigung funktionieren, nachvollziehbar und umsetzbar sind, sondern die Mitarbeiter gewinnen auch die notwendige Routine im Umgang mit Ausnahmesituationen. Da Tests und Übungen sehr aufwändig sein können, muss genau abgewogen werden, welche Arten von Überprüfungen für welchen Zweck sinnvoll sind. In einem zu entwickelnden Konzept wird beschrieben, welche Tests und Übungen vorgesehen sind. Die wesentlichen Ziele bei Übungen sind, Inkonsistenzen in den Notfallplänen oder Mängel in der Planung und Umsetzung von Notfallmaßnahmen aufzudecken sowie effektive und reibungslose Abläufe in einem Notfall zu trainieren. Typische Übungen sind beispielsweise:

» Funktionstests (z. B. von Stromaggregaten, Klimaanlagen, zentralen Servern),

» Durchführung von Brandschutzübungen,

» Wiederanlauf nach Ausfall von einzelnen Ressourcen oder Geschäftsprozessen,

» Räumung eines Bürogebäudes und Bezug einer Ausweichlokation und

» Ausfall eines Rechenzentrums und Inbetriebnahme des Ausweichrechenzentrums.

Bei hohem Schutzbedarf bzgl. der Verfügbarkeit der Prozesse sollte der CSP nachweisen, dass sein Notfallmanagement auf einem anerkannten Standard wie z. B. BS 25999 oder BSI-Standard 100-4 basiert und Notfallorganisation und Notfallkonzeption (bestehend aus den zwei wesentlichen Komponenten Notfallvorsorgekonzept und Notfallhandbuch) effektiv und effizient sind.

Notfallmanagement	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
Der Cloud-Anbieter muss ein Notfallmanagement aufsetzen und betreiben	✓			✓		
Der CSP muss seinen Kunden die Priorisierung des Wiederanlaufs für die angebotenen Cloud-Dienste transparent machen			✓			✓
Regelmäßige Notfall-Übungen (z. B. zu Ausfall eines Cloud Computing Standorts)			✓			✓
Der CSP sollte nachweisen, dass sein Notfallmanagement auf einem international anerkannten Standard wie z. B. BS 25999 oder BSI-Standard 100-4 basiert (z. B. anhand Notfallvorsorgekonzept und Notfallhandbuch)			✓			✓

9 Portabilität und Interoperabilität

9 Portabilität und Interoperabilität

Mit Interoperabilität von Cloud Computing Plattformen wird die Fähigkeit bezeichnet, zwei oder mehr unabhängige Cloud Computing Plattformen zusammenarbeiten zu lassen, ohne dass gesonderte Absprachen zwischen den Plattformen notwendig sind. Hierzu ist die Nutzung gemeinsamer Standards die Grundlage.

Mit Portabilität bzw. Plattformunabhängigkeit wird hingegen die Eigenschaft eines Cloud-Dienstes bezeichnet, auf unterschiedlichen Cloud Computing Plattformen lauffähig zu sein.

Im Falle von Daten bedeutet Portabilität, dass sie aus einem Cloud Service exportiert und in einen anderen Service importiert werden können. Bei SaaS-Angeboten erwirbt der Kunde das Nutzungsrecht an einem Software-Service. Da er sich normalerweise darauf verlässt, dass dieser Dienst auf Grundlage des geschlossenen Vertrags erbracht wird, entsteht dadurch eine Bindung an den Cloud Service Anbieter. Um ein sogenanntes Vendor Lock-In, also eine nicht einfach auflösbare Abhängigkeit von einem Anbieter, zu vermeiden, ist es wichtig, dass die Daten des Kunden portierbar bleiben. Die Portabilität der Daten muss dafür im Rahmen einer Exit-Vereinbarung mit zugesicherten Formaten unter Beibehalten aller logischen Relationen gewährleistet sein. Bei einer Migration der Daten beispielsweise zu einem anderen CSP können auch Kosten entstehen, die der Cloud Service Anbieter seinen Kunden offen legen sollte.

Eine Plattformunabhängigkeit zwischen verschiedenen CSPs kann derzeit nicht zugesichert werden. Plattformen wie Force.com von Salesforce (verwendet die Programmiersprache APEX, ein Java-Subset), SAP Business byDesign, Microsoft Azure (.NET, PHP; Ruby, Python oder Java), Google App Engine (Python, Java) stellen Kunden eine Reihe von Funktionalitäten zur Entwicklung von SaaS-Anwendungen zur Verfügung. Erstellt ein Servicekonsument eigene Dienste auf Basis eines PaaS-Dienstes, so muss er sich für eine der angebotenen Plattformen entscheiden. Die Nutzung beispielsweise eines Microsoft Azure Datenbank-Dienstes durch einen auf Google App Engine entwickelten Cloud-Dienst ist derzeit nicht möglich. Ein einmal auf einer Plattform entwickelter Dienst kann gegenwärtig in

der Regel nicht ohne erheblichen Aufwand portiert werden. Häufig ist in einem solchen Fall sogar die Neuentwicklung eines Cloud-Dienstes nötig.

Bei Angeboten der Form IaaS-Compute kann die Portabilität von VMs durch den Einsatz von OVF (Open Virtualization Format) erreicht werden. OVF ist ein plattformunabhängiger Standard zur Verpackung und Verteilung von virtuellen Appliances [12]. Derzeit nutzen allerdings fast alle Anbieter von virtuellen Maschinen eigene Formate, was den Servicekonsumenten den Wechsel des Anbieters erschwert. Beispielsweise sind bei Amazon sowohl die API zur Steuerung der Cloud-Dienste als auch das Format der virtuellen Images proprietär. Generell wäre die Unterstützung von OVF durch die Service-Anbieter zu begrüßen.

Mittlerweile existieren bereits eine Reihe von Industrie-Standards zur Senkung von Interoperabilitäts- und Portabilitätsproblemen, die im Bereich des Cloud Computings verwendet werden können und auch teilweise bereits verwendet werden. Zu nennen wären z. B. das Open Cloud Computing Interface (OCCI) des Open Grid Forums [13], die vCloud API von VMware [14] oder das bereits erwähnte OVF-Format. Eine andere Möglichkeit für Serviceanbieter, um die Interoperabilität und Portabilität zu verbessern, ist der Nachbau von bereits existierenden herstellerspezifischen Schnittstellen, wie es z. B. bei der Open Source Software Eucalyptus mit dem Amazon Web Services Interface gemacht wurde. Um Interoperabilität zu gewährleisten, sollten Cloud Computing Anbieter standardisierte oder offen gelegte Schnittstellen (API und Protokolle) verwenden.

Portabilität und Interoperabilität	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Exit-Vereinbarung mit zugesicherten Formaten unter Beibehalten aller logischen Relationen und ggf. Offenlegung der damit verbundenen Kosten (SaaS)	✓			✓		
Standardisierte oder offen gelegte Schnittstellen (API und Protokolle)	✓			✓		

10 Sicherheitsprüfung und -nachweis

10 Sicherheitsprüfung und -nachweis

Ein Bestandteil jedes erfolgreichen Informationssicherheitsmanagements ist die regelmäßige Überprüfung der etablierten Sicherheitsmaßnahmen und des Informationssicherheits-Prozesses. Cloud Service Anbieter müssen regelmäßig den IT-Sicherheitszustand ihrer Geschäftsprozesse, Dienste und ihrer Plattformen überprüfen und kontinuierlich verbessern und weiterentwickeln. Es bietet sich an, regelmäßig Reviews und Prüfungen durch unabhängige Dritte durchführen zu lassen, um Betriebsblindheit zu vermeiden und entsprechende Prüfnachweise den Cloud-Nutzern zur Verfügung stellen.

Auf der Basis einer Informationssicherheitsrevision (IS-Revision) können Aussagen über die wirksame Umsetzung von Sicherheitsmaßnahmen sowie deren Aktualität, Vollständigkeit und Angemessenheit und damit über den aktuellen Zustand der Informationssicherheit getroffen werden. Die IS-Revision ist somit ein Werkzeug zum Feststellen, Erreichen und Aufrechterhalten eines angemessenen Sicherheitsniveaus in einer Institution.

Die Kernforderung an die CSPs nach Sicherheitsprüfung und -nachweis hat verschiedene Facetten:

» Ergebnisse der von CSPs selbst durchgeführten Sicherheitstests sollten in geeigneter Form veröffentlicht werden.

» Die Kunden haben ein berechtigtes Interesse daran, eigene Sicherheitsprüfungen durchzuführen oder Dritte in ihrem Auftrag durchführen zu lassen.

Nutzt ein CSP Subunternehmen zur Erbringung seiner Services, so entlässt ihn dies nicht von der Verpflichtung, die Sicherheit dieser Dienste zu überprüfen, da der CSP gegenüber seinen Kunden für die Gesamtsicherheit seines Angebots verantwortlich und dies nicht auf Subunternehmer übertragen kann. In einem solchen Fall muss der CSP die erforderlichen Nachweise aller notwendigen Sicherheitsprüfungen von seinen Subunternehmern einfordern. Generell sollten durchgeführte Sicherheitsprüfungen so dokumentiert werden, dass es möglich ist, diese bei Bedarf an seine Kunden weitergeben zu können, sowohl die Nachweise beim CSP selber als auch bei dessen Subunternehmen.

Regelmäßige Sicherheitsüberprüfungen müssen sowohl bei Public als auch bei Private Cloud Diensten durchgeführt werden. Bei Private Clouds können allerdings typischerweise von den Betreibern die Ergebnisse von Sicherheitsprüfungen wie z. B. Penetrationstests einfacher an die Anwender weitergegeben werden, da diese sich innerhalb einer gemeinsamen Institution befinden.

Um die Wirksamkeit vorhandener technischer Sicherheitsmaßnahmen zu überprüfen, sind Penetrationstests ein erprobtes und geeignetes Vorgehen. Sie dienen dazu, die Erfolgsaussichten eines vorsätzlichen Angriffs auf einen Informationsverbund oder ein einzelnes IT-System vorab einzuschätzen und daraus notwendige ergänzende Sicherheitsmaßnahmen abzuleiten, bzw. die Wirksamkeit von bereits umgesetzten Sicherheitsmaßnahmen zu überprüfen. CSPs sollten für die von ihnen betriebenen Netze und Systeme, Anwendungen regelmäßig Penetrationstests durchführen.

Generell müssen alle Formen von Sicherheitsprüfungen von Personen mit geeigneten Qualifikationen durchgeführt werden. Diese dürfen jedoch nicht an der Erstellung der geprüften Strategien und Konzepte beteiligt gewesen sein, um Betriebsblindheit und Konflikte zu vermeiden. Die Prüfer bzw. Auditoren müssen möglichst unabhängig und neutral sein.

Sicherheitsprüfung und -nachweis	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Cloud Service Anbieter müssen den Cloud-Nutzern regelmäßig über Sicherheitsmaßnahmen, Änderungen im IT-Sicherheitsmanagement, Sicherheitsvorfälle, die Ergebnisse durchgeführter IS-Revisionen und Penetrationstests berichten	✓			✓		
Regelmäßige Penetrationstests	✓			✓		
Regelmäßige Penetrationstests bei Subunternehmen	✓			✓		
Regelmäßige und unabhängige Sicherheitsrevisionen		✓	✓		✓	✓
Regelmäßige und unabhängige Sicherheitsrevisionen bei Subunternehmern		✓	✓		✓	✓

11 Anforderungen an das Personal

11 Anforderungen an das Personal

Informationssicherheit wird unmittelbar von den Personen getragen, die mit den jeweiligen Informationen umgehen. Daher ist es essentiell, dass das bei CSPs tätige Personal ausreichend eingearbeitet und zu allen eingesetzten Techniken ebenso geschult wird wie zu Informationssicherheit und Datenschutz. Personen, die sicherheitsrelevante Aufgaben ausüben wie Administratoren und Mitarbeiter mit Zugang zu finanzwirksamen oder vertraulichen Informationen, müssen vertrauenswürdig und zuverlässig sein.

Vertrauenswürdiges Personal

Die Möglichkeiten, die Vertrauenswürdigkeit von neuem oder fremdem Personal überprüfen zu lassen, sind in Deutschland, aber auch in vielen anderen Ländern, rechtlich sehr eingeschränkt. Dazu kommt, dass die Ergebnisse meist wenig aussagekräftig sind, wie z. B. bei polizeilichen Führungszeugnissen. Grundsätzlich sollte aber vor der Übernahme von neuen oder externen Mitarbeitern beim CSP überprüft werden, ob

» diese hinreichende Referenzen haben, z. B. aus anderen, ähnlichen Arbeitsbereichen, und

» der vorgelegte Lebenslauf des Bewerbers aussagekräftig und vollständig ist.

Darüber hinaus kann es sinnvoll sein, sich akademische und berufliche Qualifikationen bestätigen zu lassen, beispielsweise durch Nachfragen an der Universität oder früheren Arbeitgebern oder Kunden. Die Datenschutzgesetze sind bei der Überprüfung der Person aber in jedem Fall einzuhalten.

Wenn ein CSP externes Personal einsetzt, das auf interne Anwendungen und Daten zugreifen kann, sollten vergleichbare Überprüfungen wie für eigene Mitarbeiter durchgeführt werden. Bei der Vertragsgestaltung mit externen Dienstleistern sollte vertraglich festgehalten werden, welche Seite solche Überprüfungen durchzuführen hat und in welcher Tiefe diese erfolgen.

Die Aufgabenverteilung und die hierfür erforderlichen Rollen sind so zu strukturieren, dass operative und kontrollierende Funktionen auf verschiedene Personen verteilt werden, um Interessenkonflikte bei den handelnden Personen zu minimieren oder ganz auszuschalten. Zu achten ist auch auf Interessenkonflikte, die auftreten können, wenn ein Mitarbeiter gleichzeitig verschiedene Rollen inne hat, die ihm zu weitreichende Rechte geben oder sich ausschließen. Zudem sollten die Aufgaben von Mitarbeitern nicht von Interessenkonflikten außerhalb der Behörde oder des Unternehmens beeinträchtigt werden, beispielsweise durch frühere Stellen oder durch anderweitige Verpflichtungen. Ein rollenbasiertes Rechtemanagement, das nur Zugriff auf diejenigen Daten und Systeme zulässt, die zur Erfüllung der jeweiligen Aufgaben notwendig sind, bietet hier die notwendige organisatorische und technische Unterstützung.

Alle Personen, die Zugang zu Kundendaten haben, sind in besonderem Maße über ihre Pflichten im Umgang mit diesen hinzuweisen. Auch bei Subunternehmen sollte auf die Auswahl und den Wissensstand des Personals geachtet werden.

Das Personal ist über die bestehenden Regelungen und Handlungsanweisungen zur Informationssicherheit, zum Datenschutz sowie zum Umgang mit Kundendaten zu unterrichten und auf deren Einhaltung zu verpflichten.

Schulungen

Beim Cloud Computing werden viele neue Techniken und IT-Komponenten eingesetzt. Die Innovations- und Updatezyklen sind daher in diesem Bereich sehr kurz. Deshalb müssen CSPs ihre Mitarbeiter regelmäßig so schulen, dass sie alle eingesetzten Techniken, Komponenten und Funktionalitäten beherrschen. Die Mitarbeiter müssen aber auch alle Sicherheitsimplikationen rund um diese Techniken kennen und im Griff haben. Dies gilt insbesondere für den Personenkreis, der mit der Entwicklung und dem Betrieb von Cloud Services befasst ist.

Da Fehlkonfigurationen in einer Cloud Computing Umgebung gravierende Folgen für die darauf bereitgestellten Ressourcen haben können, erhöhen sich die Anforderungen an die Administratoren. Daher ist es wichtig, dass die Administratoren ausreichende Kenntnisse über die eingesetzten Produkte und zugrunde liegenden Techniken besitzen, damit sie Probleme aus eigenem Handeln heraus vermeiden, technische Probleme rechtzeitig erkennen und beseitigen sowie die Funktionen und Sicherheitsmerkmale der dem Cloud Computing zugrunde liegenden Technologien optimal nutzen können. Sie müssen insbesondere in der Lage sein, die Folgen von Konfigurationsänderungen abschätzen zu können.

Damit sichergestellt ist, dass die Administratoren auch über aktuelle Sicherheitsrisiken im Zusammenhang mit Cloud Computing und über aktuelle Entwicklungen im Bereich Dynamic Data Center informiert sind, sollte der CSP dafür sorgen, dass sie sich regelmäßig weiterbilden können.

Alle Mitarbeiter des CSP müssen außerdem kontinuierlich für generelle Informationssicherheits- und Datenschutzbelange sensibilisiert werden.

Anforderungen an das Personal	Private ⇨			Public ⇨		
	B	C+	A+	B	C+	A+
Vertrauenswürdiges Personal	✓			✓		
Ausbildung der Mitarbeiter des Cloud Service Anbieters (Regelmäßige Schulungen)	✓			✓		
Sensibilisierung der Mitarbeiter des Cloud Service Anbieters für Informationssicherheit und Datenschutz	✓			✓		
Verpflichtung der Mitarbeiter auf Informations sicherheit, Datenschutz, angemessenen Umgang mit Kundendaten	✓			✓		

12 Vertragsgestaltung

12 Vertragsgestaltung

Die genauen Modalitäten der Nutzung von Cloud Services sollten klar geregelt werden. Dazu gehören neben der Beschreibung der gewünschten Leistungen inklusive Dienstgütevereinbarungen unter anderem die Klärung von Punkten wie Ansprechpartnern, Reaktionszeiten, IT-Anbindung, Kontrolle der Leistungen, Ausgestaltung der Sicherheitsvorkehrungen, Umgang mit Kundendaten und Weitergabe von Informationen an Dritte.

12.1 Transparenz

Nur wenn der CSP seinen Kunden überzeugend darlegen kann, wie und unter welchen Rahmenbedingungen er arbeitet, können die Kunde das notwendige Vertrauen in den CSP aufbauen, jenseits der technischen Maßnahmen, die der CSP ergreift. Insbesondere Public Cloud Provider stehen hier in der Pflicht, dem Kunden die notwendigen Informationen zu liefern.

Zunächst müssen Cloud Service Anbieter ihre Vertrags- und Geschäftsbedingungen nachvollziehbar offenlegen. Vor allem sollte transparent sein, welche Eingriffe der Cloud Service Anbieter oder Dritte in Daten und Verfahren der Kunden vornehmen dürfen. Zu den Vertragsgrundlagen gehören auch Service Level Agreements (SLAs), in denen unter anderem der Umfang der angebotenen Dienste, Verfügbarkeitsanforderungen, Reaktionszeiten, Rechenleistung, zur Verfügung stehender Speicherplatz und Support geregelt sind.

Cloud Service Anbieter müssen ihren Kunden offen legen, an welchen Standorten (also in welchen Ländern und welchen Regionen) die Daten gespeichert und verarbeitet werden. Hierbei spielt weniger die geographische Entfernung eine Rolle, als die Frage, was für Auswirkungen die Standortwahl auf die angebotenen Dienste und die gespeicherten Daten haben kann. Sehr wichtig ist auch, wie die jeweiligen Standorte abgesichert sind und wie der Zugriff auf die Kundendaten durch Dritte geregelt ist.

Je nach Standort der CSP-Rechenzentren sind diverse gesetzliche Rahmenbedingungen zu beachten. In einigen Ländern dürfen beispielsweise kryptographische Verfahren nicht ohne Genehmigung eingesetzt werden. Dies kann dazu führen, dass der CSP zwar Verschlüsselung einsetzen kann, aber unter Umständen staatlichen Stellen den Zugriff ermöglichen muss.

CSPs sollten daher die Kunden darüber informieren, welche lokalen rechtlichen Regelungen Auswirkungen auf die Vertraulichkeit, Integrität oder Verfügbarkeit der Kundendaten haben können.

Ebenso sollten CSPs offenlegen, in welchen Rechts- und Besitzverhältnissen sie sich befinden. Nur so können Kunden beurteilen, ob ein CSP ein geeigneter Geschäftspartner ist.

Gehört ein CSP beispielsweise zu einem Unternehmen, das in Konkurrenz zu einem Cloud-Kunden steht, könnte dies zu Interessenkonflikten führen und letztendlich dazu, dass der Kunde oder der CSP die bestehenden Verträge kündigt. Deshalb kann es wichtig sein, zu wissen, wem der CSP gehört und wie die Entscheidungsstrukturen beim CSP sind. Nicht alle Geschäftsformen lassen aber solche Aussagen zu, da sich die Besitzverhältnisse bei aktiennotierten Unternehmen ändern können und nur größere Aktionäre ihren Aktienbesitz veröffentlichen müssen.

Auf jeden Fall sollte der Kunde vom CSP eine Freistellung von Rechtsstreitigkeiten um Lizenzabgaben oder Patent-Auseinandersetzungen bei der Nutzung des Dienstes erhalten.

Viele Anbieter von SaaS betreiben keine eigene Infrastruktur, sondern nutzen wiederum PaaS- oder IaaS-Angebote anderer CSPs. In solchen Fällen sind die für die Erbringung der Cloud Services wichtigen Subunternehmer gegenüber den Kunden offenzulegen und diesen die erforderlichen Informationen zur Verfügung zu stellen.

Bei wesentlichen Änderungen einer der oben genannten Punkte hat der CSP seine Kunden in geeigneter Weise zu unterrichten.

Können bestimmte Cloud-Dienste nur genutzt werden, wenn die Kunden hierfür vorab vom CSP bereitgestellte Programme installieren (z. B. Browser-Plugins bei SaaS), so ist dies den Kunden vor Vertragsschluss mitzuteilen. Darüber hinaus sollte der CSP die Kunden auch auf Sicherheitsrisiken hinweisen, die aus deren Nutzung entstehen können, sowie auf erforderliche Sicherheitsmaßnahmen seitens des Kunden.

Transparenz	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Offenlegung der Standorte des Cloud Service Anbieters (Land, Region), an denen die Kundendaten gespeichert und verarbeitet werden	✓			✓		
Offenlegung der Subunternehmer des Cloud Service Anbieters, die für die Erbringung der Cloud Services wesentlich sind	✓			✓		
Transparenz, welche Eingriffe der Cloud Service Anbieter oder Dritte in Daten und Verfahren der Kunden vornehmen dürfen	✓			✓		
Regelmäßige Unterrichtung über Änderungen (z. B. neue oder abgekündigte Funktionen, neue Subunternehmer, andere Punkte, die für das SLA relevant sind)	✓			✓		
Transparenz, welche Software durch den Cloud Service Anbieter aufseiten des Kunden installiert wird sowie über die daraus resultierenden Sicherheitserfordernisse /-risiken	✓			✓		
Transparenz bezüglich staatlicher Eingriffs- und Einsichtrechte, über gerichtlich festlegbare Einsichtrechte Dritter und über Prüfpflichten zu gespeicherten Daten durch den Cloud Service Anbieter an allen potenziellen Standorten	n/a				✓	✓
Darlegung der Rechts- und Besitzverhältnisse des Cloud Service Anbieters sowie der Entscheidungsbefugnisse	n/a				✓	✓

12.2 Service Level Agreement (SLA)

In einem SLA (Service Level Agreement) werden die Leistungen, die der CSP erbringt, vertraglich festgehalten. Im Fokus stehen in der Regel funktionale und juristische Gesichtspunkte. SLAs bestehen meistens aus allgemeinen sowie quantitativen Leistungsbeschreibungen. Der CSP muss nur die Funktionalitäten liefern, die in den SLAs vereinbart sind. Wer-

den zu einzelnen Punkten konkrete Werte angegeben, so müssen diese auch messbar sein, beispielsweise bei den Verfügbarkeitsanforderungen. Der CSP muss seinen Kunden die Möglichkeit geben, die Einhaltung der vereinbarten Werte zu überprüfen oder überprüfen zu lassen. Dazu kann der CSP diese Leistungsparameter seinen Kunden beispielsweise über spezielle Schnittstellen zugänglich machen.

Wichtig sind auch Regelungen zum Gerichtsstandort, dem anwendbaren Recht sowie die Vertragssprache. Die Eigentums- und Urheberrechte an Daten, Systemen, Software und Schnittstellen sind festzulegen.

Es sollten im SLA jedoch auch sicherheitsrelevante Inhalte festgehalten sein. So kann sich der CSP zu bestimmten Sicherheitsmaßnahmen verpflichten (z. B. Nutzung eines Intrusion Prevention Systems). Auch wenn der Nutzer dies nicht sofort überprüfen kann, schafft eine Nennung von Sicherheitsmaßnahmen Vertrauen gegenüber dem CSP. Ebenso sollten Vertraulichkeitsvereinbarungen (Non-Disclosure-Agreements) vertraglich vereinbart werden. Dies kann auch in einem zusätzlichen Security-SLA geschehen.

Setzt ein CSP Subunternehmer zur Erbringung der von ihm angebotenen Services ein (z. B. wenn ein SaaS-Anbieter IaaS von einem Dritten nutzt), so kann vom CSP aus Vertrauen geschaffen werden, indem den Cloud-Nutzern die relevanten Aussagen zur Informationssicherheit und zur Dienstgüte aus den SLAs mit Drittanbietern offen gelegt werden.

Im Falle einer Geschäftsverlagerung oder Insolvenz des CSP muss der Kunde noch auf seine Daten zugreifen können und die Vertraulichkeit der Daten sowie Verfügbarkeit der Anwendungen und Daten müssen weiter gewährleistet sein. Das deutsche Insolvenzrecht kennt hier Regelungen, die einzuhalten sind, um dies zu gewährleisten. Sollte der CSP nicht deutschem Recht unterliegen, sind die entsprechenden Vorschriften dem Kunden zu erläutern.

Cloud Computing Anbieter sollten verpflichtet werden, nach Beendigung eines Auftrags alle gespeicherten Kundendaten inklusive Datensicherungen dem Kunden zu übergeben und alle gespeicherten Kundendaten zu löschen.

Service Level Agreement (SLA)	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Definierte Sicherheitsleistungen durch Security-SLA oder im SLA deutlich hervorgehoben	✓			✓		
Sicherstellung des Betriebs oder der Bereitstellung der Daten im Falle einer Insolvenz des Cloud Service Anbieters unter Beachtung von Vertraulichkeitszusagen und Datenschutzanforderungen		✓	✓		✓	✓

13 Datenschutz und Compliance

13 Datenschutz und Compliance

13.1 Datenschutz[1]

Werden in der Cloud personenbezogene Daten erhoben, verarbeitet oder genutzt, muss der Schutz personenbezogener Daten gemäß den datenschutzrechtlichen Bestimmungen gewährleistet sein.

Charakteristisch für Cloud Computing ist die Weitergabe der Daten vom Cloud-Nutzer an den Cloud-Anbieter. Sofern die Daten (auch) einen Personenbezug aufweisen, handelt es sich bei der Weitergabe im Sinne des Datenschutzrechts um eine Übermittlung personenbezogener Daten oder um eine Auftragsdatenverarbeitung, die nicht als Übermittlung zu qualifizieren ist. Die rechtliche Qualifizierung der Weitergabe ist abhängig von der datenschutzrechtlichen Zulässigkeit der Weitergabe sowie ihrer vertragsrechtlichen Ausgestaltung.

Bei einer Datenübermittlung vom Cloud-Nutzer an den Cloud-Anbieter gibt der Cloud-Nutzer die datenschutzrechtliche Verantwortung ab und überträgt sie voll auf den Cloud-Anbieter. Er verliert damit auch grundsätzlich die Möglichkeit, auf den Umgang mit den von ihm übermittelten Daten Einfluss zu nehmen. Auf zivilrechtlicher Ebene ist aber auch bei entsprechender Vertragsgestaltung eine andere Haftungsverteilung, nämlich ein (Teil-)Haftungsverbleib beim Cloud-Nutzer, möglich. Der Cloud-Nutzer muss vorab prüfen, ob eine solche Lösung seinen Interessen entspricht.

Für die Übermittlung bedarf es einer Rechtsgrundlage im Datenschutzrecht. Soweit es sich beim Cloud-Nutzer um eine nicht-öffentliche Stelle handelt, kommt hierfür entweder die Einwilligung der Betroffenen oder eine Interessenabwägung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG in Betracht, sofern nicht bereichsspezifisches Recht (z. B. § 97 Abs. 1 TKG) gilt. Wenn es dem Cloud-Nutzer um eine pauschale Verlagerung von Teilen oder der kompletten Datenverarbeitung geht, dürfte der Weg über Einwilligungen regelmäßig unpraktikabel sein, da bei nicht erteilten oder später widerrufenen Einwilligungen eine Auslagerung aufgrund fehlender Rechtsgrundlage nicht (mehr) zulässig wäre. Bei der Interessenabwägung

1 Das Kapitel „Datenschutz“ wurde unter Beteiligung des BfDI erstellt

nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG ist eine Verlagerung in die Cloud nur erlaubt, wenn diese zur Wahrung der berechtigten Interessen des Cloud-Nutzers erforderlich ist und kein Grund zu der Annahme besteht, dass die schutzwürdigen Interessen des Betroffenen am Ausschluss der Verlagerung überwiegen. Ob diese Voraussetzzungen gegeben sind, muss im Einzelfall geprüft werden. Es wird in erster Linie darauf ankommen, dass beim Übermittlungsempfänger (Cloud Computing Anbieter) das gleiche Datenschutzniveau wie beim Cloud-Nutzer herrscht, der Betroffene seine Rechte auch beim Anbieter auf einfache Weise geltend machen kann und sichergestellt ist, dass der Anbieter die Daten nur im Rahmen der festgelegten Zweckbestimmung verarbeitet und nutzt.

Bei der Auftragsdatenverarbeitung verbleibt die datenschutzrechtliche Verantwortlichkeit uneingeschränkt beim Cloud-Nutzer als Auftraggeber. Der Cloud-Nutzer behält datenschutzrechtlich die volle Kontrolle über die Daten. Die Auftragsdatenverarbeitung ist grundsätzlich an keine weiteren materiellen Voraussetzungen gebunden; es sind aber eine Reihe formaler Anforderungen umzusetzen. Die Auftragsdatenverarbeitung setzt eine schriftliche Vereinbarung voraus, die die in § 11 Abs. 2 BDSG aufgeführten Punkte mindestens enthalten muss. Der Cloud Computing Anbieter als Auftragnehmer unterliegt den Weisungen des Cloud-Nutzers und darf über die Verarbeitung und Nutzung der Daten nicht eigenverantwortlich entscheiden. Der Auftraggeber hat sich beim Auftragnehmer vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen. Dies muss nicht zwingend durch eine Vor-Ort-Kontrolle geschehen, sondern kann auch durch unabhängige Stellen testiert werden.

Auf die Privilegierung der Auftragsdatenverarbeitung kann nur zurückgegriffen werden, wenn der Cloud Computing Anbieter seinen Sitz innerhalb der EU oder den Staaten des Europäischen Wirtschaftsraums (EWR) hat und die Daten auch dort verarbeitet werden (§ 3 Abs. 8 BDSG). Bei einer Datenverarbeitung in anderen Staaten müssen die Voraussetzungen für eine Datenübermittlung gegeben sein und beim Cloud Computing Anbieter ein angemessenes Datenschutzniveau herrschen. Sofern die EU-Kommission nicht einzelnen Staaten insgesamt ein angemessenes

Datenschutzniveau bescheinigt hat (wie z. B. für die Schweiz, Kanada oder Argentinien), kommen hier verschiedene Maßnahmen in Betracht, die sich im Einzelnen aus § 4c BDSG ergeben.

13.2 Compliance

Neben datenschutzrechtlichen Anforderungen sind vom Cloud Service Anbieter die vom Cloud-Nutzer geforderten sonstigen rechtlichen Bestimmungen einzuhalten (Compliance). Das setzt voraus, dass der Cloud-Nutzer dem Cloud Computing Anbieter seine konkreten rechtlichen Anforderungen, die zu erfüllen sind, benennt, damit der Anbieter ermitteln kann, ob er diese erfüllen kann oder alternativ der Anbieter konkret darlegt, welche rechtlichen Anforderungen er erfüllt und der Nutzer entscheiden kann, ob dies seinen Ansprüchen gerecht wird. Ausschließlich exemplarisch seien erwähnt Anforderungen aus dem Telekommunikationsgesetz (TKG), Abgabenordnung (AO) bei der Verarbeitung steuerrechtlicher Daten, Handelsgesetzbuch (HGB) bei der Verarbeitung buchführungsrelevanter Daten, Strafgesetzbuch (StGB), falls Verschwiegenheitspflichten berührt werden.

Datenschutz und Compliance	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Gewährleistung des Datenschutzes nach deutschem Recht	✓			✓		
Datenschutzrichtlinien und -gesetze, denen der Cloud-Nutzer unterliegt, müssen eingehalten werden	✓			✓		
Bei Datenübermittlung: Rechtsgrundlage für die Übermittlung: » § 28 Abs. 1 Satz 1 Nr. 2 BDSG » Einwilligung	✓			✓		
Bei Auftragsdatenverarbeitung: Schriftliche Vereinbarung zwischen Cloud-Nutzer und Cloud-Anbieter gemäß § 11 Abs. 2 BDSG mit Mindestinhalt nach § 11 Abs. 2 Satz 2 BDSG, u. a.: » Beschreibung von Gegenstand und Dauer des Auftrags » Genaue Bezeichnung der Erhebung, Verarbeitung und Nutzung personenbezogener Daten » Festlegung der technischen und organisatorischen Maßnahmen: Festlegung des genauen Ortes der Verarbeitung personenbezogener Daten beim Cloud-Anbieter einschließlich der technischen und organisatorischen Verarbeitungsumgebung » Umgang mit Ansprüchen Betroffener auf Berichtigung, Sperrung und Löschung personenbezogener Daten » Einhaltung von § 11 Abs. 4 BDSG » Festlegung oder Verbot etwaiger Unterauftragsverhältnisse » Kontrollrechte des Cloud-Nutzers » Weisungsbefugnisse des Cloud-Nutzers » Rückgabe bzw. Löschung von Daten nach Beendigung des Auftrags	✓			✓		

Datenschutz und Compliance	Private ⇨			Public ⇗		
	B	C+	A+	B	C+	A+
Bei Übermittlung und Auftragsdatenverarbeitung: Speicherung und Verarbeitung der personenbezogenen Daten » innerhalb der Mitgliedsstaaten der EU oder eines Vertragsstaats des EWR oder » außerhalb der EU oder eines Vertragsstaats des EWR, wenn ein angemessenes Datenschutzniveau gewährleistet werden kann z. B. durch: – Entscheidung der EU-Kommission – Beitritt zum Safe-Harbor-Agreement (USA) – EU-Standardvertragsklauseln – Genehmigung der Aufsichtsbehörde	✓			✓		
Keine Einbindung von Unterauftragnehmern, die eine Verarbeitung der personenbezogenen Daten unter den oben genannten Voraussetzungen nicht gewährleisten können	✓			✓		
Kontrollrechte des Kunden zur datenschutzkonformen Verarbeitung der personenbezogenen Daten bei der Auftragsdatenverarbeitung durch » Vor-Ort-Kontrolle oder » Testat eines unabhängigen Sachverständigen	✓			✓		
Bei Auftragsdatenverarbeitung: Kontrollrecht der für den Cloud-Nutzer zuständigen Aufsichtsbehörde	✓			✓		
Bei Auftragsdatenverarbeitung: Weisungsrechte des Cloud-Nutzers gegenüber dem Cloud-Anbieter	✓			✓		
Für den Cloud-Nutzer relevante gesetzliche Bestimmungen müssen durch den Anbieter eingehalten werden	✓			✓		

14 Ausblick

14 Ausblick

Cloud Computing verspricht hohe Flexibilität bei der Buchung und Nutzung sowie Stilllegung von Ressourcen, je nach aktuellem Bedarf. Erwartet wird auch ein hohes Einsparpotential im Bereich der ansonsten lokal vorzuhaltenden, zu wartenden und zu erneuernden IT-Systeme. Damit die versprochene Flexibilität auch wirklich gegeben ist, müssen beim Cloud Computing die angebotenen Dienste und die zugehörigen Schnittstellen weitgehend standardisiert werden. Dadurch haben die Kunden auch die Möglichkeit, immer die aktuellsten Techniken zu beziehen. Ein weiterer Vorteil beim Cloud Computing ist die ubiquitäre Verfügbarkeit von Geschäftsanwendungen (je nach Cloud Modell), ein wichtiger Aspekt bei der zunehmenden Mobilität von Mitarbeitern.

Diesen potentiellen Vorteilen steht eine Reihe von Herausforderungen gegenüber, die vor einer Auslagerung von geschäftsrelevanten Daten oder Anwendungen in eine Public Cloud zu lösen sind. Da beim Public Cloud Computing Daten beziehungsweise Anwendungen außer Haus verlagert werden, sind sie somit der unmittelbaren Kontrolle durch die eigene Institution entzogen. Darüber hinaus müssen eine Vielzahl von rechtlichen und vertraglichen Richtlinien und Vorgaben wie zum Beispiel Datenschutzanforderungen beachtet werden, wenn beispielsweise geschäftskritische oder personenbezogene Daten in eine Public Cloud ausgelagert werden. Dazu kommt, dass sich beim Public Cloud Computing unbekannte Nutzer eine gemeinsame Infrastruktur teilen. Damit steigt das Risiko, dass die Grundwerte der Informationssicherheit verletzt werden. Schließlich werden Daten und Anwendungen über das Internet genutzt, so dass ein Ausfall der Internetverbindung den Zugriff unmöglich macht.

Um die potentiellen Vorteile von Cloud Computing nutzen zu können und dennoch die Kontrolle über die IT-Infrastruktur zu behalten, greifen viele Anwender zur Bereitstellung der Dienste auf eigene virtualisierte Rechenzentren (Private Clouds) zurück. Aber auch in einer Private Cloud gibt es eine Reihe von Gefährdungen, vor denen es sich zu schützen gilt. Je nach Implementierung kann auch eine Private Cloud sehr komplex sein. Auch hier können aufgrund der Fülle an Konfigurationseinstellungen und der sich gegenseitig beeinflussenden Parameter, zahlreiche Sicherheitsprobleme entstehen z. B. durch Datenverluste, unerlaubte Zugriffe auf Informationen,

Beeinträchtigung der Verfügbarkeit oder sogar Ausfall von Diensten. Cloud-Anbieter stellen eine Reihe von Schnittstellen zur Verfügung für den Zugriff auf ihre Dienste. Sind diese Schnittstellen unsicher programmiert, dann könnte ein Angreifer Schwachstellen ausnutzen, um unerlaubt auf Daten zuzugreifen. Ferner stellt das Management von Cloud-Plattformen aufgrund der Komplexität und der Dynamik der zugrunde liegenden Prozesse eine große Herausforderung dar und zwar für Public wie auch für Private Clouds.

Diese Herausforderungen können jedoch gemeistert werden können, wenn entsprechende infrastrukturelle, organisatorische, personelle und technische Maßnahmen zum Schutz der bereitgestellten Dienste umgesetzt werden. Neben traditionellen IT-Sicherheitsmaßnahmen müssen in einer Cloud insbesondere Maßnahmen zur sicheren und verlässlichen Trennung von Mandanten umgesetzt werden.

Das vorliegende BSI-Eckpunktepapier zum Thema Cloud Computing, aber auch Arbeiten wie beispielsweise von der Cloud Security Alliance [4], der ENISA [3] oder der NIST [2] stellen hierfür wichtige Grundlagen zur Verfügung.

Aufgrund der erwarteten technischen und wirtschaftlichen Potenziale wird sich Cloud Computing voraussichtlich am Markt durchsetzen können, allerdings nur, wenn die Anbieter es schaffen, die Fragen der Kunden zur Informationssicherheit und zum Datenschutz zu klären. Mit zunehmender Verbreitung in der Fläche werden allerdings Cloud Computing Angebote für Angreifer attraktiver, auch aufgrund der Konzentration vieler geschäftskritischer Ressourcen in zentralen Rechenzentren sowie der erforderlichen Standardisierung der Komponenten und Schnittstellen. Daher wird es auf lange Sicht nötig sein, internationale Standards für Informationssicherheit zu erarbeiten und zu etablieren, auf deren Grundlage Plattformen für das Cloud Computing überprüft und zertifiziert werden können. Eine der zentralen Aufgaben in den nächsten Jahren wird es daher sein, internationale Standards für die Informationssicherheit im Bereich Cloud Computing zu erarbeiten und zu etablieren, auf deren Basis die Sicherheit von Cloud Computing Anbietern zertifiziert werden kann. Nur durch international anerkannte Zertifizierungen von Cloud Computing Anbietern bzw. deren Services wird ein ausreichendes Vertrauen auf Seiten der Kunden geschaffen werden können.

15 Glossar

15 Glossar

Kennzeichnungen in den Tabellen:

Die in den Tabellen aufgeführten Sicherheitsempfehlungen sind drei Kategorien zugeordnet.

B	Basisanforderung, Kategorie dieser Sicherheitsempfehlungen, die sich an jeden Cloud Service Anbieter richtet
A+	Availability high (=Verfügbarkeit hoch), Kategorie dieser Sicherheitsempfehlungen, die zusätzliche Anforderungen für Bereiche mit hohem Verfügbarkeitsbedarf umfasst
C+	Confidentiality high (=Vertraulichkeit hoch), Kategorie dieser Sicherheitsempfehlungen, die zusätzliche Anforderungen für Bereiche mit hohem Schutzbedarf bei Vertraulichkeit umfasst

Außerdem wird das Gefährdungspotential signalisiert, das zu diesen Sicherheitsempfehlungen geführt hat:

⇨	durchschnittliches Gefährdungspotential
⇗	erhöhtes Gefährdungspotential

Abkürzungen / Begriffe	**Definitionen**
Bot	Schadprogramm auf einem Client, das zum Aufbau fernsteuerbarer Rechnernetze (Bot-Netze) dient
BSI	Bundesamt für Sicherheit in der Informationstechnik
COBIT	Control Objectives for Information and Related Technology, Methode zur Kontrolle von Risiken, die sich durch den IT-Einsatz zur Unterstützung geschäftsrelevanter Abläufe ergeben

CSA	Cloud Security Alliance
CSP	Cloud Service Provider
DDoS	Distributed Denial-of-Service, ein koordinierter Angriff auf die Verfügbarkeit von IT z. B. mittels einer größeren Anzahl von angreifenden Systemen
IaaS	Infrastructure as as Service, Bereitstellung von IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netzen als Dienst
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO 27001	Internationale Norm ISO/IEC 27001 „Information technology – Security techniques – Information security management systems – Requirements“ zu Anforderungen an Managementsysteme für Informationssicherheit (ISMS)
ITIL	IT Infrastructure Library, Sammlung von Werken zum Thema IT-Service-Management aus Sicht eines IT-Dienstleisters
NAS	Network Attached Storage, Speichersystem-Variante
OVF	Open Virtualization Format, plattformunabhängiger Standard zur Verpackung und Verteilung von virtuellen Appliances
SAN	Storage Area Network, Speichersystem-Variante
PCI DSS	Payment Card Industry Data Security Standard, Prüfvorgaben zur sicheren Abwicklung von Kreditkartentransaktionen
PaaS	Platform as a Service, Bereitstellung einer kompletten Laufzeit-bzw. Entwicklungsumgebung als Dienstleistung

SaaS	Software as a Service, Bereitstellung von IT-Anwendungen als Dienstleistung
SAML	Security Assertion Markup Language, XML-Framework zum Austausch von Authentisierungsinformationen
SOA	Service-orientierte Architektur, Ansatz zur Realisierung verteilter Systeme, um Institutionen mittels IT bei der Durchführung ihrer Geschäftsprozesse effizient zu unterstützen
VM	Virtuelle Maschine
VPN	Virtuelles Privates Netz

16 Referenzen

16 Referenzen

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI), IT-Grundschutz-Vorgehensweise, BSI-Standard 100-2, Version 2.0, Mai 2008
http://www.bsi.bund.de/grundschutz

[2] Wayne Jansen, Timothy Grance, Guidelines on Security and Privacy in Public Cloud Computing, NIST, Draft Special Publication 800-144, January 2011
http://csrc.nist.gov/publications/drafts/800-144/Draft SP-800-144_cloud-computing.pdf

[3] ENISA, Cloud Computing: Benefits, Risks and Recommendations for Information Security, November 2009
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud computing-risk-assessment/at_download/fullReport

[4] Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, Dezember 2009
http://www.cloudsecurityalliance.org/csaguide.pdf

[5] Dr. Fang Liu, Jin Tong, Dr. JianMa, NIST Cloud Computing Reference Architecture, Version1.0, March 2011
http://collaborate.nist.gov/twiki-cloud-computing/pub/Cloud-Computing/ReferenceArchitectureTaxonomy/NIST_CC_Reference_Architecture_v1_March_30_2011.pdf

[6] Mahesh Dodani: “Architected” Cloud Solutions Revealed, in Journal of Object Technology, vol. 9, no. 2, pages 27 – 36, March - April 2010
http://www.jot.fm/issues/issue_2010_03/column3/

[7] Whitepaper Cloud Computing Use Cases Version 3.0, produced by the Cloud Computing Use Case Discussion Group, February 2010
http://opencloudmanifesto.org/cloud_computing_use_cases_whitepaper-3_0.pdf

[8] Webhost hack wipes out data for 100,000 sites, The Register, June 2009
http://www.theregister.co.uk/2009/06/08/webhost_attack/

[9] Worldwide Infrastructure Security Report, Arbor networks, 2010
http://www.arbornetworks.com/dmdocuments/ISR2010_EN.pdf

[10] OWASP Top 10 - 2010, The Ten Most Critical Web Application Security Risks
http://www.owasp.org/images/0/0f/OWASP_T10_-_2010_rc1.pdf

OWASP Application Security Principles
http://www.owasp.org/index.php/Category:Principle

[11] Bundesamt für Sicherheit in der Informationstechnik (BSI), Notfallmanagement, BSI-Standard 100-4 zur Business Continuity Management, Version 1.0, November 2008
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004.pdf?__blob=publicationFile

[12] Open Virtualization Format Specification, February 2009
http://www.dmtf.org/standards/published_documents/DSP0243_1.0.0.pdf

[13] Open Cloud Computing Interface - Core & Models, January 2010
http://www.ggf.org/Public_Comment_Docs/Documents/2010-01/occi-core.pdf

[14] vCloud API Programming Guide, vCloud API 1.0, 2010
http://communities.vmware.com/servlet/JiveServlet/downloadBody/12463-102-2-14932/vCloud_API_Guide.pdf

17 Dankesworte

17 Dankesworte

Um das Thema Informationssicherheit beim Cloud Computing zu adressieren und Anwender und Anbieter zu unterstützen, hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) das Eckpunktepapier „Mindestsicherheitsanforderungen an Cloud Computing Anbieter“ am 28.09.2010 als Diskussionsentwurf veröffentlicht und um Kommentierung gebeten. Das Eckpunktepapier wurde positiv aufgenommen und konstruktiv kommentiert. Allen sei gedankt, die sich durch Anregungen, konstruktive Kritik und Verbesserungsvorschläge an der Verbesserung des Eckpunktepapiers beteiligt haben.

Wir danken außerdem folgenden Experten und Institutionen, die mit ihren Beiträgen, ihrer Unterstützung bei der Qualitätssicherung und hilfreichen Diskussionen wesentlich zur Entstehung und Weiterentwicklung dieses Werks beigetragen haben:

» Bayerische Landesbank, Sven-Torsten Gigler

» Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), Sven Hermerschmidt

» BITKOM e.V., in Vertretung für die Mitglieder des BITKOM-Kompetenzbereichs Sicherheit, Lutz Neugebauer

» Cyber-Ark Software Ltd., Jochen Koehler

» EMC, Klaus Böttcher, Wolfgang Reh †

» Eurocloud Deutschland_eco e.V., Andreas Weiss

» Google, Robin Williamson, John Collins, Thorsten Koch

» ITDZ Berlin, Kai Osterhage

» Microsoft, Gerold Hübner

» ORACLE Deutschland B.V. & Co. KG, Lutz Kahlenberg

» Pironet NDH, Dr. Clemens Plieth

» RSA, Alexander Hoffmann, Thomas Köhler

» SAP AG

» Siemens, Dr. Bernd Grobauer, Steffen Fries

» Symantec, Ilias Chantzos, Zoltán Précsényi

» ToolBox Solution GmbH, Tillmann Basien

» TÜV Informationstechnik GmbH (TÜViT), Adrian Altrhein

» VMware, Stephan Bohnengel

» VZM GmbH, Werner Metterhausen

Außerdem sei den Mitarbeitern des BSI gedankt, die dieses Dokument erstellt haben:

Alex Didier Essoh, Dr. Clemens Doubrava, Isabel Münch.

Wichtige Impulse und Diskussionsbeiträge haben darüber hinaus die folgenden Mitarbeiter des BSI geliefert:

Horst Flätgen, Dr. Hartmut Isselhorst, Andreas Könen, Dirk Reinermann, Dr. Stefanie Fischer-Dieskau, Thomas Caspers, Oliver Zendel, Holger Schildt, Dr. Dörte Rappe, Thomas Borsch.

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
53133 Bonn

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53133 Bonn
E-Mail: cloudsecurity@bsi.bund.de
bsi@bsi.bund.de
Internet: www.bsi.bund.de/cloud
Telefon: +49 (0) 22899 9582 - 0
Telefax: +49 (0) 22899 9582 - 5400

Stand
Februar 2012

Druck
Druckpartner Moser Druck + Verlag GmbH
53359 Rheinbach

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Artikelnummer
BSI-Bro12/314

www.bsi.bund.de