Bundesamt
für Sicherheit in der
Informationstechnik

Sichere Nutzung von Cloud-Diensten

Schritt für Schritt von der Strategie bis zum Vertragsende

Inhaltsverzeichnis

Einleitung 5

1 Bedrohungen bei der Nutzung von Cloud-Diensten 8

1.1 Bedrohungen für die Cloud-Infrastruktur und den Cloud-Dienst 8

1.2 Bedrohungen bei der Nutzung von Cloud-Diensten 8

1.3 Bedrohungen bei Einführung und Nutzung der Cloud 9

2 Der sichere Weg in die Cloud 11

2.1 Am Anfang steht die Cloud-Strategie 11

2.2 Sicherheitsanforderungen (Sicherheitsrichtlinie) 12

2.3 Definition von Service/Schnittstellen/ Verantwortungsbereichen 15

2.3.1 Service-Definition 15

2.3.2 Schnittstellen-Definition 15

2.3.3 Verantwortungsbereiche 15

2.4 Vorausschauende Planung der Nutzung 16

2.4.1 Migrationsplan 16

2.4.2 Planung der Nutzung 16

2.5 Sicherheitskonzept 17

2.6 Auswahl des Cloud-Anbieters 18

2.6.1 Service-Beschreibung 19

2.6.2 Kosten-Nutzen-Analyse 19

2.6.3 Vertrag mit dem Cloud-Anbieter 19

2.7 Migration und Betrieb 21

2.8 Beendigung der Cloud-Nutzung 21

2.9 Datenschutz/Compliance 22

3 Zusammenfassung 24

4 Anhang 26

4.1 Schematischer Überblick über einen sicheren Cloud-Nutzungsprozess 26

4.2 Literatur 27

Einleitung

Einleitung

Cloud Computing ist kein Hype mehr, Cloud Computing ist Realität. Und es verändert grundlegend die Art und Weise, wie IT-Dienste erbracht und genutzt werden. Dieses Dokument setzt voraus, dass sich der potenzielle Cloud-Anwender mit Cloud Computing befasst hat und Möglichkeiten sieht, es in der eigenen Institution zu nutzen.

Die vorliegende Publikation soll Institutionen, wie Unternehmen und Behörden hier zusammenfassend genannt werden, auf dem Weg zum sicheren Nutzen von Cloud-Diensten unterstützen. Sie ist anwendbar

» für **jedes Bereitstellungsmodell** (Private Cloud, Community Cloud, Public Cloud, Hybrid Cloud [3]),

» für **jedes Service-Modell** (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) oder andere (XaaS)) und

» für **normalen und hohen Schutzbedarf** [4].

Sie zeigt einen Weg durch alle Phasen: von der Strategie bis zur Beendigung der Nutzung eines Cloud-Dienstes. Grundlage hierfür ist der IT-Grundschutz Baustein „Cloud-Nutzung“, der auf der IT-Grundschutz-Methodik [11] basiert. Dieses Papier ist jedoch in sich abgeschlossen, sodass eine nähere Kenntnis des IT-Grundschutzes und seiner Methoden nicht notwendig ist, um es zu verstehen und anzuwenden.

Mit dem Anforderungskatalog Cloud Computing C5 (Cloud Computing Compliance Controls Catalogue) hat das BSI das Niveau an Sicherheitsanforderungen definiert, welches von Cloud-Anbietern nie unterschritten werden sollte, ebenso wie die Nachweise die mindestens erforderlich sind. Dies wird in der nun vorliegenden Version dieses Dokuments berücksichtigt.

IT-Grundschutz:
Baustein B 1.17 Cloud-Nutzung [4]

BSI Anforderungskatalog Cloud Computing C5 [2]

Folgende **Zielgruppen** werden hier adressiert:

» Verantwortliche und Mitarbeiter in Projektgruppen zur Cloud-Nutzung

» IT-Sicherheits-Beauftragte

» IT-Verantwortliche

» Entscheidungsträger (Management)

Der hier beschriebene Weg zur sicheren Cloud-Nutzung kann und soll je nach Art und Umfang des Cloud-Services angepasst werden.

Was ist eine sichere Cloud?

Oft wird dem BSI die Frage gestellt, was denn eine sichere Cloud sei. Die Antwort fällt für den Fragesteller oft unbefriedigend aus, da er sich mehr konkrete Aussagen wünscht. Wenden wir die Frage analog auf ein Auto an, wird der Grund hierfür leicht ersichtlich.

Angenommen ein populäres Auto der Mittelklasse wird als ein sicheres Auto angesehen. Warum werden in den Oberklasse-Modellen verschiedenste Assistenzsysteme eingebaut, um die Sicherheit zu erhöhen? Würde ein Rennfahrer mit dem Mittelklasse-Modell auf die Rennstrecke gehen? Sicher nicht, denn einen Unfall bei 180 km/h wird wohl weder er noch das Auto überleben. Für einen hochrangigen Politiker oder Wirtschaftsvertreter ist der Mittelklassewagen auch kein sicheres Auto. Fragen nach schusssicheren Scheiben, Feuerlösch- und Sauerstoffanlage im Innern etc. müssten wohl negativ beantwortet werden. Auch ein Single und ein Familienvater haben unterschiedliche Anforderungen an die Sicherheit des Autos.

Beim Autokauf werden Autokategorien (Kleinwagen, Mittelklasse, Geländewagen) oder Automarken ein gewisses Sicherheitsniveau unterstellt. Zusätzlich gibt es gesetzliche Vorschriften (z. B. für Airbags), die aber nur eine untere Grenze definieren. Crashtest-Ergebnisse und Erfahrungen anderer runden unseren Blick auf die Sicherheit ab. Und letztendlich spielt das Geld eine gewichtige Rolle, denn die Sicherheit will auch finanziert sein und nicht alles, was wünschenswert ist, kann auch umgesetzt werden.

Also: So wie es nicht das eine sichere Auto für alle Situationen gibt, so gibt es auch nicht die eine sichere Cloud für alle Fälle. So wie beim Auto muss auch bei der Cloud gefragt werden, für welche Zwecke sie jeweils genutzt werden soll. Für diese kann dann nach geeigneten Sicherheitsmaßnahmen gesucht werden.

Aber auch die Anforderungen an die Sicherheit nützen nichts, wenn sich der Anbieter im Betrieb nicht an Sicherheitsvorgaben und -vorschriften hält.

Das Ziel lautet daher:

Sicheres Cloud Computing und nicht die sichere Cloud. Letztere gibt es nicht.

1 Bedrohungen bei der Nutzung von Cloud-Diensten

1 Bedrohungen bei der Nutzung von Cloud-Diensten

Beim Thema Informationssicherheit muss geklärt werden, welche Informationen und Prozesse geschützt und welche Bedrohungen abgewehrt werden müssen. Dies gilt ohne Einschränkung auch für Cloud Computing. Vertraulichkeit, Integrität und Verfügbarkeit der Informationen sind zu schützen – das sind die sogenannten Grundwerte der Informationssicherheit.

Nutzer eines Cloud-Dienstes sind (externen) Bedrohungen auf die Cloud-Infrastruktur und bei Einführung und Nutzung der Cloud ausgesetzt.

1.1 Bedrohungen für die Cloud-Infrastruktur und den Cloud-Dienst

Die Infrastruktur und die Cloud-Dienste des Cloud-Anbieters müssen von ihm gegen folgende Bedrohungen geschützt werden:

» Datenverlust bzw. Informationsabfluss

» Beeinflussung der verschiedenen Nutzer in der gemeinsamen (shared) Cloud-Infrastruktur bis hin zu Angriffen aus der Cloud heraus.

» Ausfall der Internet- oder Netzverbindung, der den Zugriff auf Daten bzw. Anwendungen unmöglich macht.

» Denial-of-Service Angriffe auf Cloud-Anbieter, die sicher noch zunehmen werden.

» Fehler in der Cloud-Administration, die aufgrund der sehr hohen Komplexität zu erheblichen Sicherheitsproblemen führen (Dienstausfall, Datenverlust, etc.) können. Kleine Fehler oder Pannen können in einer Cloud-Infrastruktur große Auswirkungen (nicht nur auf die Sicherheit) haben.

1.2 Bedrohungen bei der Nutzung von Cloud-Diensten

Der Cloud-Nutzer ist insbesondere folgenden Bedrohungen ausgesetzt:

» Identitätsdiebstahl bzw. Missbrauch von Accounts

» Verlust der Kontrolle über die Daten und Anwendungen

» Verletzung geltender Vorgaben und Richtlinien (z. B. Datenschutzanforderungen)

» Sicherheit der Endgeräte, mit denen die Cloud-Dienste verwendet werden.

» Daten können über das Netz abgefangen und (bei schlechter oder nicht vorhandener Verschlüsselung) ausgespäht werden.

Die Nonprofit-Organisation Cloud Security Alliance (CSA) gibt eine jährlich aktualisierte Liste der wichtigsten Bedrohungen heraus. [5]

Der Report der ENISA (European Union Agency for Network and Information Security) „Cloud computing – Benefits, risks and information security“ (Rev. B – December 2012) gibt im Kapitel 4 eine gute Übersicht über Risiken beim Cloud Computing, die über Angriffe hinausgehen. [6]

1.3 Bedrohungen bei Einführung und Nutzung der Cloud

Die oben genannten Bedrohungen treten auf, wenn der Cloud-Dienst angeboten und genutzt wird. Doch auch auf dem Weg in die Cloud lauern auf einen Cloud-Anwender weitere Gefahren.

» Es gibt keine Cloud-Strategie und deshalb sind die Ziele, die mittels Cloud Computing erreicht werden sollen, weder klar noch überprüfbar.

» Kritische Elemente im Einführungsprozess wurden aufgrund einer mangelhaften Planung übersehen, und das angedachte Cloud Projekt scheitert.

» Der Cloud Service ist ungenau definiert und es kommt zu Differenzen über die Servicequalität mit dem Cloud-Anbieter. Infolgedessen erhält der Cloud-Anwender entweder eine ungenügende Service-Qualität oder teure Nachbesserungen werden notwendig.

» Großer Wille, Cloud Computing auf jeden Fall einzusetzen, führt zu illusorischen Annahmen und zu „geschönten" Kosten-Nutzen-Analysen. Im Endeffekt kommt es zu finanziellen Einbußen.

» Der Weg in die Cloud kann sehr schwierig sein und dabei wird übersehen, dass auch an einen Weg aus der Cloud heraus gedacht werden muss. Andernfalls entsteht eine starke Abhängigkeit vom Cloud-Anbieter, die finanziell von Nachteil sein kann.

» Flexibilität beziehen Cloud-Anbieter auf die innerhalb eines Service zur Verfügung gestellten Kapazitäten. Andere Wünsche der Cloud-Anwender können oft nicht erfüllt werden, eigene Eingriffsmöglichkeiten sind sehr begrenzt.

» Ein Cloud-Anbieter bezieht selbst häufig Dienste (z. B. Administration oder Backup von Daten) von Unterauftragnehmern. Dadurch können beispielsweise personenbezogene Daten an nicht erlaubte Stellen gelangen (was ggf. bußgeldbewehrt ist) oder es kann dadurch ein Sicherheitszertifikat gefährdet werden, weil ein Auditor diesen Unterauftragnehmer nicht überprüfen kann.

» Notfall? Welcher Notfall? Die Cloud ist doch immer da und deshalb hat der Cloud-Anwender keinen Notfallplan.

2 Der sichere Weg in die Cloud

2 Der sichere Weg in die Cloud

Die Gefahr, dass ein Cloud-Projekt scheitert, ist ohne ein strukturiertes Vorgehen deutlich erhöht. Zwar können in manchen Fällen ad-hoc eingeführte Cloud-Dienste erfolgreich genutzt werden, doch das ist eher die Ausnahme. Planung und Evaluierung dürfen aber nicht so umfangreich werden, dass das Ziel – die Nutzung von Cloud-Diensten und den damit einhergehenden Vorteilen – nicht erreicht werden kann.

Um zu einer tragfähigen und auch wirtschaftlichen Entscheidung zu kommen, müssen die Ziele, die mit dem avisierten Cloud-Service verknüpft sind, klar sein. Vonseiten des Cloud-Anwenders ist aber auch Flexibilität gefordert: in Bereichen der Funktionalität ebenso wie in der Sicherheit. Nicht alle Wünsche und Anforderungen werden sich realisieren lassen, da Cloud-Angebote meist stark standardisiert sind. Im Zuge der Evaluation von Cloud-Diensten muss klar werden, wie weit ein angebotener Service von den eigenen Zielen entfernt ist. Nur so lassen sich ggf. alternative Wege einschlagen.

Die nachfolgenden Empfehlungen können und sollten auf die jeweilige, konkrete Situation angepasst werden. Dies betrifft Umfang und ggf. Dokumentation, aber nicht die wesentlichen Inhalte, die für alle Cloud-Projekte gültig bleiben.

2.1 Am Anfang steht die Cloud-Strategie

Unabhängig von der Größe des Cloud-Projekts ist es notwendig, die grundlegenden Anforderungen und Rahmenbedingungen zu kennen und daraus eine Handlungsanleitung zu schaffen. Andernfalls ist das Projekt von Anfang an in einer Schieflage.

Projektteam einsetzen

Die Leitung vergibt folgenden Auftrag an ein Projektteam, in dem Entscheidungsträger für die IT-Strategie und für die Unternehmensstrategie vertreten sind:

» Formulierung und Dokumentation der Ausgangslage und des gewünschten Nutzens

» Definition des Untersuchungsgegenstands: welcher Service, welches Service-Modell und welches Bereitstellungsmodell. An dieser Stelle können noch Punkte offen sein oder explizit gegeneinander abgewägt werden.

Vorsicht:

» Es ist wenig sinnvoll, bei diesem Projektschritt schon zu konkrete Vorgaben zu machen, wie z. B. einen bestimmten Service eines Anbieters zu untersuchen. Ziel ist, einen Service zu finden, der den eigenen Anforderungen möglichst gut entspricht.

» Das Projektteam, das die Untersuchung durchführt, braucht genügend Ressourcen und Zeit, sonst ist die Qualität des Projekts gefährdet!

Machbarkeitsstudie

Das Projektteam erstellt eine Machbarkeitsstudie, deren Umfang und Ausführung sich am geplanten Cloud-Dienst orientieren sollen. Folgende Punkte sollen adressiert werden:

» Untersuchung der **rechtlichen Rahmenbedingungen** (z. B. Datenschutz, Geheimschutz, Aufsichtsbehörden) und der unternehmens- bzw. behördeneigenen Richtlinien (Compliance). Welche Art von Daten soll in der Cloud verarbeitet werden? Dürfen die Daten in eine Cloud? Gibt es Einschränkungen bzgl. des Speicher- und Verarbeitungsorts (z. B. aufgrund von Zugriff auf die Informationen durch Dritte, Spionage)? Ergeben sich daraus Einschränkungen bezüglich des Bereitstellungsmodells (Public Cloud, Community Cloud, Private Cloud oder Hybrid Cloud)?

» Hat die IT des Unternehmens oder der Behörde die **nötige Reife,** Cloud-Dienste nutzen zu können? Bei der Nutzung von IaaS in größerem Stil ist zu fragen: Lassen sich die betroffenen Dienste virtualisieren? Lassen sie sich standardisieren? Erst wenn das gegeben ist, kann eine Nutzung von IaaS gelingen.

» Die Auslagerung von Diensten führt immer zu **internen Anpassungen.** Sind diese nicht realisierbar, kann der untersuchte Cloud-Dienst nicht genutzt werden. Beispiel: Ein Cloud-Dienst benötigt eine hohe Bandbreite und einen redundanten Internetzugang, was in ländlichen Gegenden mit nur einer verfügbaren 6-MBit-Leitung nicht gegeben ist.

Nun kann konkreter festgelegt werden, welches **Service**- und welches **Bereitstellungsmodell** genutzt werden kann und im nächsten Schritt weiter untersucht werden soll.

Risikoanalyse

Entscheidend für die Definition der Anforderungen an einen Cloud-Dienst ist die Klassifikation (Schutzbedarf) der zu verarbeitenden Informationen. Die Einteilung sollte mindestens drei Kategorien haben, wobei der Schaden, den der Verlust, die Veränderung oder die Nicht-Verfügbarkeit der Informationen mit sich bringen würde, das Maß für die Einstufung ist. Es ist wichtig, zwischen Vertraulichkeit, Integrität und Verfügbarkeit zu unterscheiden.

Informationssicherheit basiert immer auf einem Risiko-Managementprozess, dessen Herzstück, die Risikoanalyse ist. Hierüber muss sich jede Institution Gedanken machen. Die Risiken können zwar allgemein beschrieben werden, die Auswirkungen beim Eintritt des Schadensfalls können jedoch stark variieren.

In dieser groben Risikoanalyse sollen mindestens folgende Gefährdungen betrachtet werden:

» Zugriff auf die Daten durch den Cloud-Anbieter

» Zugriffsmöglichkeiten durch staatliche Behörden aufgrund der (ggf. ausländischen) Jurisdiktion, die für den Cloud-Anbieter zutrifft

» Nicht-Verfügbarkeit der Daten und Dienste

» Kompromittierung der Authentisierung

» Datenverlust

» Datenmanipulation

Diese Analyse liefert bereits Bereiche, in denen besondere Sicherheitsmaßnahmen notwendig werden bzw. bei denen Risiken entstehen, die nicht behandelt werden können. Ein für alle Anwendungsfälle sicheres Cloud Computing durch externe Cloud-Anbieter gibt es nicht.

Kosten-Nutzen-Abschätzung

Sind die oben genannten Punkte geklärt, folgt eine grobe Kosten-Nutzen-Abschätzung, die mindestens folgende Aspekte betrachtet:

» Nutzungskosten des Service

» interner Administrationsaufwand

» Schulung von Mitarbeitern und Administratoren

» bei Bedarf neue IT oder neue Netzanbindung

» Kosten der der Anpassung von Prozessen

» Kosten der Migration

» Interne Einsparungen

Diese Abschätzung liefert, wenn sie gut und realistisch gemacht ist, einen ersten Eindruck, ob sich ein Cloud-Service rechnen könnte. Die Ergebnisse werden zusammengefasst und den Entscheidungsträgern vorgelegt. Sie entscheiden über den Fortgang des Projekts.

IT-Grundschutz: M 2.534 Erstellung einer Cloud-Nutzungs-Strategie [4]

2.2 Sicherheitsanforderungen (Sicherheitsrichtlinie)

Hat die Leitung auf Basis der Machbarkeitsstudie, der Risikoanalyse und der Kosten-Nutzen-Abschätzung entschieden, den Einsatz eines Cloud-Service weiter voranzutreiben, folgen nun konkrete Umsetzungsschritte.

Neben den funktionalen Anforderungen, die hier nicht vorrangiger Gegenstand sind, sind die Anforderungen an die Informationssicherheit und die Verfügbarkeit des Cloud-Dienstes darzulegen. Darunter sind nicht nur diejenigen an den Cloud-Anbieter zu verstehen, sondern auch an die eigene Institution.

Die erste grobe Risikoanalyse dient als Gerüst, das nun weiter verfeinert wird. Zusätzlich sollte die in der Institution (hoffentlich) bereits bestehende Risiko- oder Sicherheitsanalyse herangezogen werden. Zudem müssen Anforderungen aus den rechtlichen Rahmenbedingungen beachtet werden.

Wer bisher noch keine eigenen Sicherheitsanforderungen aufgestellt hat, wird sich schwer tun, dem Cloud-Anbieter konkret zu sagen, was er von ihm erwartet. So kann die geplante Nutzung von Cloud-Diensten ein Treiber sein, sich auch über die Informationssicherheit der bestehenden

IT und die Verfügbarkeit der mit ihnen durchgeführten Geschäftsprozesse Gedanken zu machen. Vom Cloud-Anbieter eine „sichere“ und „immer verfügbare“ Cloud zu fordern, ohne konkrete Anforderungen zu stellen, kann nur schief gehen: Entweder reicht das Sicherheitsniveau nicht aus oder die angebotene Lösung ist zu teuer.

Als Minimum sollten die Sicherheitsanforderungen aus dem BSI Anforderungskatalog Cloud Computing C5 verlangt werden. Eine eigene Risikoanalyse ist auch dann noch erforderlich.

An dieser Stelle sei nochmals auf die **Klassifikation der Informationen** hingewiesen, ohne die angemessene Anforderungen an die Informationssicherheit und Verfügbarkeit nicht aufgestellt werden können.

Das nachfolgend dargestellte Vorgehen kann genutzt werden, um die Sicherheitsanforderungen zu ermitteln.

Vereinfachter Plan

Erstellung eines vereinfachten Plans, in dem alle an der geplanten Cloud-Nutzung beteiligten Personen(-gruppen) bzw. Rollen, Kommunikationsverbindungen, IT-Systeme und Geschäftsprozesse dargestellt sind. Sowohl auf der Seite der nutzenden Institution als auch (symbolisch) aufseiten des Cloud-Anbieters.

» Nutzendes Unternehmen

- Personengruppen
  - Normale Benutzer
  - Privilegierte Benutzer (i. d. R. Administratoren), die die Nutzung des Cloud-Dienstes aufseiten des eigenen Unternehmens steuern
  - weitere Benutzer mit speziellen Rechten, wie z. B. die Buchhaltung für die Rechnungslegung
- Kommunikationsverbindungen
  - Internetverbindung(en) der nutzenden Institution oder auch die Kommunikationsverbindung in ein abgeschlossenes Netz
- IT-Systeme aufseiten der nutzenden Institution
  - Schnittstellensysteme
  - Netzwerkkomponenten (Router, Firewalls, Virtual Private Network-(VPN)-Gateways, …)
  - Endgeräte zur Nutzung des Service
  - Endgeräte für die Service-Administration
- Geschäftsprozesse (in Behörden werden unter Geschäftsprozesse in der Regel die Fachaufgaben der jeweiligen Organisationseinheiten verstanden)

» Cloud-Anbieter

- Personengruppen
  - Administratoren
  - Andere Mitarbeiter des Anbieters
- Kommunikationsverbindungen
  - Internetverbindung(en) des Anbieters oder auch die Kommunikationsverbindung in ein abgeschlossenes Netz
- IT-Systeme
  - Schnittstellensysteme, die eine Web-Oberfläche oder einen Webservice anbieten
  - Netzwerkkomponenten (wie oben und zusätzlich Load Balancer)
  - Administrations-IT
  - Datenbanken

Angriffsvektoren

Erarbeiten, wo und auf welchem Weg unberechtigt auf die Informationen zugegriffen oder die Auslieferung und Nutzung des Dienstes verhindert werden könnte. Wichtigste Angriffsvektoren sind:

» Authentisierung gegenüber dem Cloud Service wird gefälscht

» Authentisierungsverfahren gegenüber dem Cloud-Dienst ist zu unsicher

» Backdoors bei der Authentisierung (z. B. Standard-User und Passwort)

» Fehlerhafte Implementierung der Schnittstelle (z. B. Webanwendung anfällig für Injection-Angriffe)

» End-Point-Security beim Nutzer

» Zugriff auf Informationen durch Personal des Cloud-Anbieters (insbesondere Administratoren) oder externe Mitarbeiter

  • Verschlüsselte Daten werden zur Verarbeitung entschlüsselt

  • Zugriff auf gesicherte oder archivierte Daten (auch Snapshots von virtuellen Maschinen)

» Mithören der Kommunikation (verschlüsselte Kommunikation, Transport Layer Security (TLS) 1.2, VPN)

» Direkter Angriff auf IT-Systeme und Netzkomponenten, die nicht gepatcht bzw. nicht gehärtet sind.

Aus den erarbeiteten Angriffsvektoren werden Anforderungen formuliert, die noch nicht technisch sein müssen, aber sein können (Beispiel: Das Rechenzentrum muss redundant an das Internet angebunden sein).

Erstellen der Sicherheitsrichtlinie

In der Sicherheitsrichtlinie sind die wichtigsten Angriffsvektoren aufgeführt und Sicherheitsanforderungen formuliert. Die Auswahl von Sicherheitsmaßnahmen ist noch offen, außer es liegen in dieser Phase schon Gründe vor, dies zu tun.

Sollten die Sicherheitsanforderungen so hoch sein, dass sie mit einer Cloud-Nutzung nicht zu erfüllen sind, ist der Prozess zur Cloud-Nutzung abzubrechen.

Können die Sicherheits-Anforderungen mit einer Public Cloud-Lösung nicht erreicht werden, ist nach Rücksprache mit den Entscheidungsträgern das Projekt einzustellen oder zu prüfen, ob auch eine Community Cloud oder auf eine Private Cloud umgeschwenkt werden kann.

IT-Grundschutz: M 2.535 Erstellung einer Sicherheitsrichtlinie für die Cloud-Nutzung [4]

Risikoanalyse auf der Basis von IT-Grundschutz (BSI-Standard 100-3) [4]

IT-Grundschutz: Gefährdungskatalog G 0 „Elementare Gefährdungen“ [4]

BSI Anforderungskatalog Cloud Computing C5 [2]

BSI Sicherheitsprofile SaaS Teil 2: Bedrohungs- und Risikoanalyse (durchgeführt für drei verschiedene Cloud-Dienste) [3]

2.3 Definition von Service/Schnittstellen/ Verantwortungsbereichen

Definitionen niederzuschreiben ist eine mühselige Aufgabe, doch ohne diese genau festzulegen, können später im Prozess große Probleme auftreten.

2.3.1 Service-Definition

Der Cloud-Anwender dokumentiert, was der Service können soll und nicht das, was er vermutlich vom Cloud-Anbieter angeboten bekommt. Anpassungen können noch nachträglich gemacht werden, aber für die Auswahl eines geeigneten Service und eines Anbieters ist die Definition der eigenen Anforderungen an den Service zentral.

Durch die vorangegangenen Schritte ergibt sich ein Bild, wie der Service gestaltet sein soll und welche Sicherheitsanforderungen gestellt werden müssen. Die Definition des Services ist vor allem funktional, aber auch funktionale Defizite bergen Sicherheitsrisiken in sich. (Beispiel: Notwendige Funktionen befinden sich beim Anbieter noch in der Beta-Phase, werden später aber eingestellt. So kann das ganze Projekt scheitern.)

Fachabteilung und IT-Abteilung müssen an der Service-Definition mitarbeiten, wobei hier ggf. schon gewichtete Vorgaben verwendet werden können („must have“ – „nice to have“). Service Templates nach Information Technology Infrastructure Library (ITIL) können bei der Strukturierung und Formulierung des Service helfen:

» Servicekürzel und Servicename

» Kurzbeschreibung

» Kategorie

» Sub- bzw. Sekundär-Services

» Varianten

» Technische Parameter

» Service-Parameter/Service Level Agreements (SLA)

» SLA-Messung

» Gültigkeit des Services (Zeitraum)

» Serviceübergabe

» Methoden der Kostenermittlung

» Preis/Verrechnung

» Ansprechpartner für den Service

» Berechtigte und Anfordernde

» Voraussetzungen

2.3.2 Schnittstellen-Definition

Cloud-Dienste werden über Schnittstellen genutzt. Kommt es bei der Definition zu Unklarheiten oder Fehlern, kann das gravierende Auswirkungen auf die Funktionalität und die Sicherheit haben. Folgende Aspekte sind hier zu beachten:

» Generische Beschreibung der Schnittstelle aufseiten des Anwenders mit Infos über Protokolle und/oder eingesetzte Software.

» Beschreibung der Authentisierungsmittel der eigenen Benutzer- und Rechteverwaltung, die für den Cloud-Service genutzt werden sollen. (Empfehlung: 2-Faktor-Authentisierung bei Cloud-Diensten, die über das Internet zu erreichen sind).

2.3.3 Verantwortungsbereiche

Die Abgrenzung der Verantwortungsbereiche zwischen Cloud-Anwender und Cloud-Anbieter ist insbesondere bei den Schnittstellen sehr wichtig. Nur so kann eine strukturierte und lösungsorientierte Vorgehensweise bei Problemen aufgesetzt werden und dies gelingt nur, wenn die Definitionen vollständig und klar sind. In den Verträgen müssen Melde- und Eskalationswege zur Problembehandlung beschrieben sein (siehe Kapitel 2.6.3).

IT-Grundschutz: M 2.536 Service-Definition für Cloud-Dienste durch den Anwender [4]

2.4 Vorausschauende Planung der Nutzung

Bis zu diesem Schritt ist noch kein Cloud-Anbieter ausgewählt, trotzdem sollte sich schon mit der Planung der Migration und des Betriebs auseinandergesetzt werden. Noch bevor konkrete Angebote eingeholt werden, sollte untersucht werden, wie der Cloud-Dienst dauerhaft sicher genutzt werden kann und ob mögliche Hindernisse für die Migration existieren. Diese groben Planungen können bereits erfolgen, selbst wenn der Service noch nicht genau bestimmt ist. Hierbei können noch Kosten und/oder Zeitverzögerungen entstehen, die eine erfolgreiche Nutzung von Cloud-Diensten verhindern können.

2.4.1 Migrationsplan

Für die Planung der Migration ist ein Migrationskonzept wesentlich. Darin wird aufgeführt, was bei der Einführung des Cloud-Dienstes zu beachten ist. Löst der neue Service einen bereits bestehenden ab, sind Daten-Migration, Verfügbarkeit, Berechtigungen und Administrationsmodell anzupassen. Gibt es keinen Vorläufer-Service, so gestaltet sich die Migration einfacher; die Administration und das Berechtigungsmanagement müssen aber erweitert werden.

Cloud Services sind fast immer in andere Prozesse eingebunden und dies ist bei der Migration zu berücksichtigen. Zudem ist vorzubereiten, inwieweit vorhandene Prozessbeschreibungen angepasst werden müssen und wie viel Zeit für Schulungen etc. angesetzt werden muss.

Wie lässt sich überprüfen, ob eine Migration erfolgreich verlaufen ist? Hierfür müssen Test- und Übergabeverfahren festgelegt werden, die nicht nur funktionale, sondern auch sicherheitsrelevante Aspekte abdecken. Bei größeren Cloud-Vorhaben kann ein Dienstleister in Anspruch genommen werden, der die Migration plant und durchführt. In diesem Fall liegt es auf der Hand, dass es festgeschriebene Kriterien geben muss, die der Dienstleister erfüllen muss.

IT-Grundschutz: M 2.537 Planung der sicheren Migration zu einem Cloud Service [4]

2.4.2 Planung der Nutzung

Die Zeit zwischen der Entscheidung für einen Cloud-Dienst und seiner Einführung soll möglichst kurz sein. Deshalb ist vorab zu überlegen, welche Änderungen sich bei Nutzung des Cloud-Dienstes für die bestehende IT ergeben. Wie schon bei der Migration sollen einige grundlegende Aspekte bereits analysiert werden, auch wenn der Cloud-Anbieter noch nicht ausgewählt ist.

Wichtige Aspekte bei der Planung der Nutzung sind:

» Anpassung der Schnittstellensysteme wie Load Balancer, Proxys, Router, Sicherheitsgateways und Federation-Systeme.

» Analyse, ob die vorhandenen Schnittstellensysteme mit dem Cloud Service interoperabel sind oder/und ob neue Schnittstellensysteme benötigt werden, die auch eine längere Lieferzeit haben können.

» Kalkulation der Netzlast und Überprüfung, ob die bestehende (Netz-)Performance ausreicht (Beispiel: Werden Office-Anwendungen als Cloud-Services gestreamt, fallen viel höhere Datenvolumen an als bei einer lokalen Softwareinstallation).

» Das Administrationsmodell sowie das Benutzer- und Berechtigungsmodell müssen an den Cloud-Dienst angepasst werden.

Falls die Daten nicht nur in der Cloud gespeichert werden sollen, sondern auch noch auf eigenen Systemen in der Institution, ist zu klären, ob genug Speicherkapazität zur Verfügung steht und ob diese auch als Backup für den Cloud-Dienst nutzbar ist.

IT-Grundschutz: M 2.538 Planung der sicheren Einbindung von Cloud Services [4]

2.5 Sicherheitskonzept

Im Sicherheitskonzept sind alle sicherheitsrelevanten Punkte der IT niedergeschrieben. Es ist das zentrale Dokument, mit dem eine Institution seine Informationssicherheit festlegt.

Eigentlich sollte in jeder Institution ein solches Konzept für die vorhandene IT existieren, evtl. trägt es einen anderen Namen. Es dient der Dokumentation der notwendigen Sicherheitsmaßnahmen und muss für die Cloud-Nutzung (grundlegend) überarbeitet werden. Als Hilfestellung kann der IT-Grundschutz des BSI herangezogen werden.

Sowohl der Cloud-Anwender als auch der Cloud-Anbieter (und ggf. auch der Netz-Anbieter) benötigen ein Sicherheitskonzept. Der Anbieter sollte dem Cloud-Anwender auf Anfrage Einsicht gewähren.

Im Sicherheitskonzept für die Cloud-Nutzung sollte zusätzlich die besondere Gefährdungslage durch die Erbringung als Cloud Service beschrieben werden. Hierbei sollten insbesondere folgende Punkte betrachtet werden:

» Vorzeitige oder zwangsweise Vertragsbeendigung

» Fehlende Portabilität von Daten (insbesondere bei Software as a Service), Anwendungen (insbesondere bei Platform as a Service) und Systemen (insbesondere bei Infrastructure as a Service) für den Fall, dass der gewählte Cloud-Dienst von etablierten Standards abweicht.

» Abhängigkeit von einem Cloud-Diensteanbieter durch fehlende Möglichkeit, den Anbieter zu wechseln (Vendor Lock-in)

» Nutzung proprietärer Datenformate kann die Integrität der Informationen gefährden und den Wechsel des Anbieters erschweren.

» Gemeinsame Nutzung der Cloud-Infrastruktur durch mehrere Institutionen

» Fehlende Kenntnis über den Speicherort von Informationen

» In der Regel hohe Mobilität der Informationen

» Unbefugter Zugriff auf Informationen, zum Beispiel durch Administratoren des Cloud-Diensteanbieters

Mögliche Sicherheitsmaßnahmen gegen diese Gefährdungen:

» Vorgaben zur sicheren Administration des Cloud-Services (zum Beispiel 4-Augen-Prinzip für bestimmte, besonders kritische administrative Tätigkeiten wie das Kopieren einzelner Datenbestände oder Systeme)

» Vorgaben zu Betriebsprozessen und Prozessen im Sicherheitsmanagement (Schnittstellen zum Beispiel für das Change-, Incident-, Sicherheitsvorfalls-, betriebliches Kontinuitäts- und Risikomanagement)

» Regelungen zur Überwachung der Service-Erbringung und zum Berichtswesen

» Verschlüsselung der Informationen bei Speicherung und Übertragung

» Vergabe und Entzug von Berechtigungen

» Durchführung von Datensicherungen, sowohl durch den Cloud-Anbieter als auch durch den Cloud-Anwender

Das Sicherheitskonzept des Anbieters kann am Besten durch Audits überprüft werden. Diese können vom Cloud-Nutzer oder von unabhängigen Dritten durchgeführt werden. Mit dem Cloud-Anbieter muss dies klar kommuniziert, vertraglich geregelt und auch durchgeführt werden.

IT-Grundschutz: M 2.539 Erstellung eines IT-Sicherheitskonzeptes für die Cloud-Nutzung [4]

IT-Grundschutz-Vorgehensweise (BSI Standard 100-2 Kap. 4) [4]

Webkurs IT-Grundschutz: Sicherheitskonzept [4]

IT-Grundschutz: M 2.195 Erstellung eines Sicherheitskonzepts [4]

2.6 Auswahl des Cloud-Anbieters

Die Cloud-Strategie ist abgenommen, der gewünschte Cloud-Service gut beschrieben und das Sicherheitskonzept erstellt: Nun folgt die Wahl eines geeigneten Anbieters.

Vermutlich bestand schon im Vorfeld des Cloud-Prozesses eine engere Auswahl von Anbietern. Trotzdem ist es wichtig, dass zunächst die eigenen Anforderungen auch an die Sicherheit zusammengestellt werden. Die Service-Beschreibung und die Sicherheitsanforderungen können nun in ein Lastenheft oder eine Leistungsbeschreibung einfließen.

Eine Auswahl:

BSI: Testierung nach BSI Anforderungskatalog Cloud Computing C5 [2]

ISO 27001 auf Basis von IT-Grundschutz [4]

ISO/IEC 27001:2013, Information security management [13]

ECSA – EuroCloud StarAudit, Certification for Cloud Services [14]

Cloud Security Alliance (CSA) Security, Test & Assurance Registry (STAR): STAR Self Assessment, STAR Certification, STAR Attestation, C-STAR Assessment [15]

ISO 22301:2012, Societal security – Business continuity management systems – Requirements (Notfallmanagement) [16]

Datenschutzzertifikate, z. B. EuroPriSe des ULD [17], Trusted Cloud Data Protection Profile [11]

Testierung nach AICPA SOC 1, SOC 2, SOC 3 oder ISAE 3402 (und ggf. vergleichbaren Standards). Nachfolger von SSAE 16 (Statements on Standards for Attestation Engagements) und SAS70 (Statement on Auditing Standards) No. 70, Service Organizations [18]

IDW-Standards (Institut der deutschen Wirtschaftsprüfer) [19]

Existieren Regeln für die Vergabe, so sind diese zu beachten (Beispiel: Für Behörden gilt die Verordnung über die Vergabe öffentlicher Aufträge).

Schon aus dem Sicherheitskonzept (siehe Kapitel 2.5) sollte hervorgehen, welche Sicherheitsanforderungen der Cloud-Anbieter erfüllen muss und ob er das auch durch Zertifikate nachweisen soll.

Bei Zertifikaten und Testaten muss geprüft werden, ob der Zertifizierungsgegenstand den gesamten angebotenen Cloud-Service enthält und was die wesentliche Aussage des Zertifikats ist.

IT-Grundschutz: M 2.540 Sorgfältige Auswahl eines Cloud-Diensteanbieters [4]

Zur Überprüfung der Eignung eines Anbieters sollten folgende Kriterien berücksichtigt werden:

- Reputation (überprüfbare Referenzen)
- Rankings oder Bewertungsmatrizen von (möglichst unabhängigen) Organisationen
- Ist Cloud Computing das Kerngeschäft des Anbieters? Falls nicht, könnte es sein, dass der Cloud-Dienst rasch eingestellt oder von einem anderen Anbieter übernommen wird.
- Welche Zugriffe durch den Diensteanbieter oder Dritte werden erlaubt oder sind möglich?
- An welchen Standorten werden die Informationen verarbeitet und gespeichert?
- Welches geltende Recht liegt einem Vertrag zugrunde, welchen rechtlichen Rahmenbedingungen unterliegt der Anbieter?
- Angabe der Subunternehmen zur Service-Erbringung um Abhängigkeiten des Cloud-Anbieters beurteilen zu können.

Ein Prüfbericht mit Testat auf Basis des BSI Anforderungskatalogs Cloud Computing C5 bietet hier Antworten auf viele der genannten Punkte und sollte deshalb nachgefragt werden. Mit dem Prüfbericht testiert ein Wirtschaftsprüfer die Einhaltung der Anforderungen, sowie die Richtigkeit von Angaben zu Umfeldparametern des Cloud-Dienstes (z. B. tatsächliche Standorte der Datenverarbeitung, Sub-Unternehmer). Gleichzei-

tig werden Angaben zur Qualifikation des Prüfungsteams getroffen (Vorliegen von einschlägigen Personenzertifizierungen). Der Kunde sollte den Prüfungsbericht mit Hilfe der im Anforderungskatalog Cloud Computing C5 genannten Hinweise auswerten.

Spionage:

Seit den Enthüllungen von Edward Snowden, durch die das Ausmaß und die Möglichkeiten staatlicher Überwachung zu Tage kam, ist Spionage als Gefährdung deutlich in den Fokus gerückt. Für das Cloud Computing besonders relevant sind die Möglichkeiten von Strafverfolgungsbehörden Cloud-Anbieter zu zwingen, Daten seiner Kunden herauszugeben, ohne diese zu informieren und überhaupt eine Aussage darüber machen zu dürfen. Dies schürt Misstrauen, weniger gegen den Anbieter selber, sondern gegen den Rechtsraum, in dem die Informationen in der Cloud verarbeitet werden bzw. in dem der Hauptsitz des Cloud-Anbieters liegt.

Das BSI fordert schon seit 2011, dass Cloud-Anbieter offenlegen müssen, welche Eingriffsmöglichkeiten staatliche Stellen oder andere Dritte auf die Kundendaten haben. Dies ist bei globalen Clouds, in denen die Daten über alle Kontinente verteilt sind, ein schwieriges Unterfangen. Ggf. sollte daher eher ein Cloud-Anbieter gewählt werden, bei dem an dieser Stelle Klarheit herrscht.

2.6.1 Service-Beschreibung

Im Angebot des Cloud-Anbieters müssen die angebotenen Services ausreichend klar beschrieben sein, andernfalls sind die Punkte schriftlich zu klären. (Beispiel: Wird neben der Angabe der Verfügbarkeit auch angegeben, welche Definition zu deren Berechnung angewendet wird?)

2.6.2 Kosten-Nutzen-Analyse

Bei Eignung und nach der Bewertung der Angebote ist eine detaillierte Kosten-Nutzen-Analyse durchzuführen. Diese muss auch Kosten für Migration, Anpassungen, Schulungen und Aufrechterhaltung des Betriebs enthalten. Auch sollte diese Analyse Kosten betrachten, die beim Beenden des Vertragsverhältnisses mit dem Cloud-Anbieter entstehen. Dabei sollten die Fälle „Migration zu einem anderen Anbieter“ und „Insourcing“ getrennt betrachtet werden.

Muss nun der Schluss gezogen werden, dass der angebotene Cloud-Dienst nicht den wirtschaftlichen Erwartungen entspricht oder die Kosten den neuen Möglichkeiten nicht entsprechen, wird das Projekt hier abgebrochen.

2.6.3 Vertrag mit dem Cloud-Anbieter

In den Angeboten der Cloud-Anbieter sind immer auch vertragliche Bestandteile (AGB) enthalten. Diese sind zu überprüfen, ob sie für den Cloud-Anwender tragbar sind.

Cloud-Computing-Verträge sind in der Regel nicht so komplex wie Outsourcing-Verträge. Dennoch muss ihnen viel Zeit und Aufmerksamkeit gewidmet werden.

Im Vertrag müssen mindestens die aufgeführten Bestandteile enthalten sein:

» Ort der Leistungserbringung

» Subunternehmer

» Einhaltung von Sicherheitsanforderungen, möglichst mindestens nach dem BSI Anforderungskatalog Cloud Computing C5

» Infrastruktur des Cloud-Diensteanbieters und Personal

» Kommunikationswege und Ansprechpartner

» Regelungen zu Prozessen, Arbeitsabläufen und Zuständigkeiten

» Ggf. besondere Regelung bei Sicherheitsvorfällen oder Betriebsunterbrechungen beim Cloud-Anbieter (z. B. Zugriff auf Log-Dateien)

» Beendigung und Datenlöschung

» Notfallvorsorge

» Regelungen zu rechtlichen Rahmenbedingungen

» Änderungsmanagement

» Kontrollen

» Vertragsstrafen bei Nichterfüllung

» Haftungsfragen

Strafzahlungen (Pönalien) können vereinbart werden, deren Durchsetzung kann sich aber als schwierig erweisen. Meist bietet der Cloud-Anbieter Gutschriften auf zukünftige Leistungen. Die Durchsetzung einer Haftung des Cloud-Anbieters für eingetretene Schäden ist anzustreben, aber äußerst schwierig durchzusetzen

Falls notwendig, muss geregelt sein, wie die Lizenzierung eingesetzter Software gehandhabt wird.

Cloud Computing basiert auf Standardisierung, damit sehr viele Kunden die Angebote nutzen können und so die „Economy of Scale“ zum Tragen kommt. Dementsprechend sind die Service Level Agreements (SLA) und Operational Level Agreements (OLA) meist fest und nicht verhandelbar. Für die angebotenen Funktionen ist das oft in Ordnung, das Sicherheitsbedürfnis und die -anforderungen sind von Kunde zu Kunde verschieden – nicht zuletzt deshalb, weil die vom Cloud-Service verarbeiteten Informationen je nach Kunde anderen Wert besitzen.

Trotzdem sollte möglichst darauf beharrt werden, dass die eigenen Sicherheitsziele eingehalten werden. Im professionellen Umfeld ist die Möglichkeit ein SLA zu verhandeln gegeben, während als Privatkunde hier meist keine Möglichkeit besteht.

Für die Vereinbarung von Sicherheitsanforderungen ist es sinnvoll, mindestens die Einhaltung des BSI Anforderungskatalogs Cloud Computing C5 mit dem Cloud-Anbieter zu vereinbaren. Damit einhergehen sollte die Vereinbarung der regelmäßigen Vorlage von Prüfungsberichten auf dessen Basis. Bei der Vertragsgestaltung sollten dann auch die weiteren Hinweise zum Verhältnis zwischen Cloud-Dienstleister, Cloud-Kunde und Wirtschaftsprüfern berücksichtigt werden (z. B. Berichterstattung über Mängelbeseitigung).

Grundsätzlich können auch Prüfungsrechte für den Cloud-Kunden vereinbart werden, die auch für die Prüfung der Informationssicherheit genutzt werden können. In bestimmten Fällen kann dies sogar regulatorisch oder aus Erwägungen des eigenen Risikomanagements geboten sein. Sind eigene Prüfungsrechte für den Cloud-Kunden erforderlich, so ist darauf zu achten, dass diese vertraglich hinreichend klar und umfassend fixiert werden. Analoges gilt für die Meldung von Sicherheitsvorfällen und die Risikoberichterstattung.

In jedem Falle bleibt der Cloud-Kunde selbst für die Einhaltung seiner eigenen regulatorischen Vorschriften verantwortlich. Daher ist der Vertrag mit dem Cloud-Anbieter vor Abschluss auch unter Compliance-Gesichtspunkten zu prüfen.

Weitere Dokumente zur Vertragsgestaltung:

IT-Grundschutz: M 2.541 Vertragsgestaltung mit dem Cloud-Diensteanbieter [4]

Trusted Cloud: Vertragsgestaltung beim Cloud Computing [7]

BITKOM: Leitfaden Cloud Computing Kap. 4 [1]

Zum Lizenzmanagement:

Kompetenzzentrum Trusted Cloud: Arbeitspapier – Lizenzierungsbedarf beim Cloud Computing [8]

2.7 Migration und Betrieb

Die Migration zu einem Cloud-Service erfolgt in mehreren Stufen mit Test- und Pilotbetrieb. Die einfache Nutzbarkeit von Cloud-Services darf nicht darüber hinwegtäuschen, dass nicht nur die IT, sondern auch die Organisation mit ihren Prozessen angepasst werden und störungsfrei laufen müssen. Dies muss auf jeden Fall getestet werden und bei größeren Anpassungen empfiehlt sich eine Pilotphase, bei der zunächst ein Teil der Anwender den Cloud-Service nutzt.

Zum kontinuierlichen, sicheren Betrieb des Cloud-Dienstes gehört die Kontrolle der Leistungserbringung. Ein enger Kontakt zum Cloud-Anbieter ist unerlässlich. Insbesondere ist zu achten auf:

» regelmäßige Aktualisierung der Dokumentationen und Richtlinien

» regelmäßige Kontrollen von unter anderem:

- Sicherstellung der ordnungsgemäßen Administration
- Regelmäßige Kontrolle der Service-Erbringung (gemäß SLA)
- Regelmäßige Service-Reviews mit Cloud-Anbieter
- Sicherheitsnachweise durch den Cloud-Anbieter
- Ordnungsgemäße Durchführung von Datensicherungen
- Einhaltung vorgesehener und vereinbarter Prozesse
- Audits, Sicherheitsprüfungen, Penetrationstests oder Schwachstellenanalysen

» Regelmäßige Abstimmungsrunden mit dem Cloud-Anbieter

» Planung und Durchführung von Übungen und Tests

IT-Grundschutz: M 2.542 Sichere Migration zu einem Cloud Service [4]

IT-Grundschutz: M 2.543 Aufrechterhaltung der Informationssicherheit im laufenden Cloud-Nutzungs-Betrieb [4]

IT-Grundschutz: M 2.544 Auditierung bei Cloud-Nutzung [4]

2.8 Beendigung der Cloud-Nutzung

Für die Beendigung der Nutzung eines Cloud-Dienstes kann es mehrere Gründe geben: Wechsel zu einem anderen Cloud-Anbieter, keine Verwendung mehr für den Cloud-Service oder Insourcing. Dies kann je nach Cloud-Service sehr aufwendig sein, unabhängig davon sind folgende Punkte zu beachten:

» Alle notwendigen Daten müssen an den Cloud-Anwender übertragen beziehungsweise übergeben werden.

» Alle Daten des Cloud-Anwenders müssen beim Cloud-Anbieter sicher gelöscht werden.

» Es ist empfehlenswert, vertraglich eine Übergangsfrist zu vereinbaren, in der der Cloud-Anbieter noch für Rückfragen und Hilfestellungen zur Verfügung steht bzw. die Daten noch nicht gelöscht sind.

IT-Grundschutz M 2.307 Geordnete Beendigung eines Outsourcing- oder Cloud-Nutzungs-Verhältnisses [4]

2.9 Datenschutz/Compliance

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

Neben datenschutzrechtlichen Anforderungen muss der Cloud-Nutzer die geforderten rechtlichen Bestimmungen einhalten (Compliance). Dies können Anforderungen z. B. aus dem Telekommunikationsgesetz (TKG), der Abgabenordnung (AO) bei der Verarbeitung steuerrechtlicher Daten, dem Handelsgesetzbuch (HGB) bei der Verarbeitung buchführungsrelevanter Daten und dem Strafgesetzbuch (StGB) sein.

In allen Fällen gilt, dass bei einer Verarbeitung solcher Daten in einer Cloud die Verantwortung (in der Regel) beim Cloud-Nutzer bleibt und er sicherstellen muss, dass die Daten beim Cloud-Anbieter gemäß dieser Vorschriften und Gesetze behandelt werden.

EuroCloud Leitfaden Recht, Datenschutz & Compliance [10]

Trusted Cloud: Datenschutzprofil TCDP (Trusted Cloud Data Protection Profile) [11]

Arbeitskreise Technik und Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises: Orientierungshilfe Cloud Computing [9]

ISO/IEC 27018:2014, Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors [12]

3 Zusammenfassung

3 Zusammenfassung

Cloud-Dienste bieten neue Möglichkeiten und versprechen Kostenersparnis, die sie oft auch einhalten. Die Chancen und Risiken der Cloud-Nutzung sowie die effektiven Kosten müssen sachlich und nachvollziehbar erhoben, nüchtern bewertet und klug abgewogen werden. Jede andere Vorgehensweise führt in Zustände, die nicht mehr kontrolliert werden können.

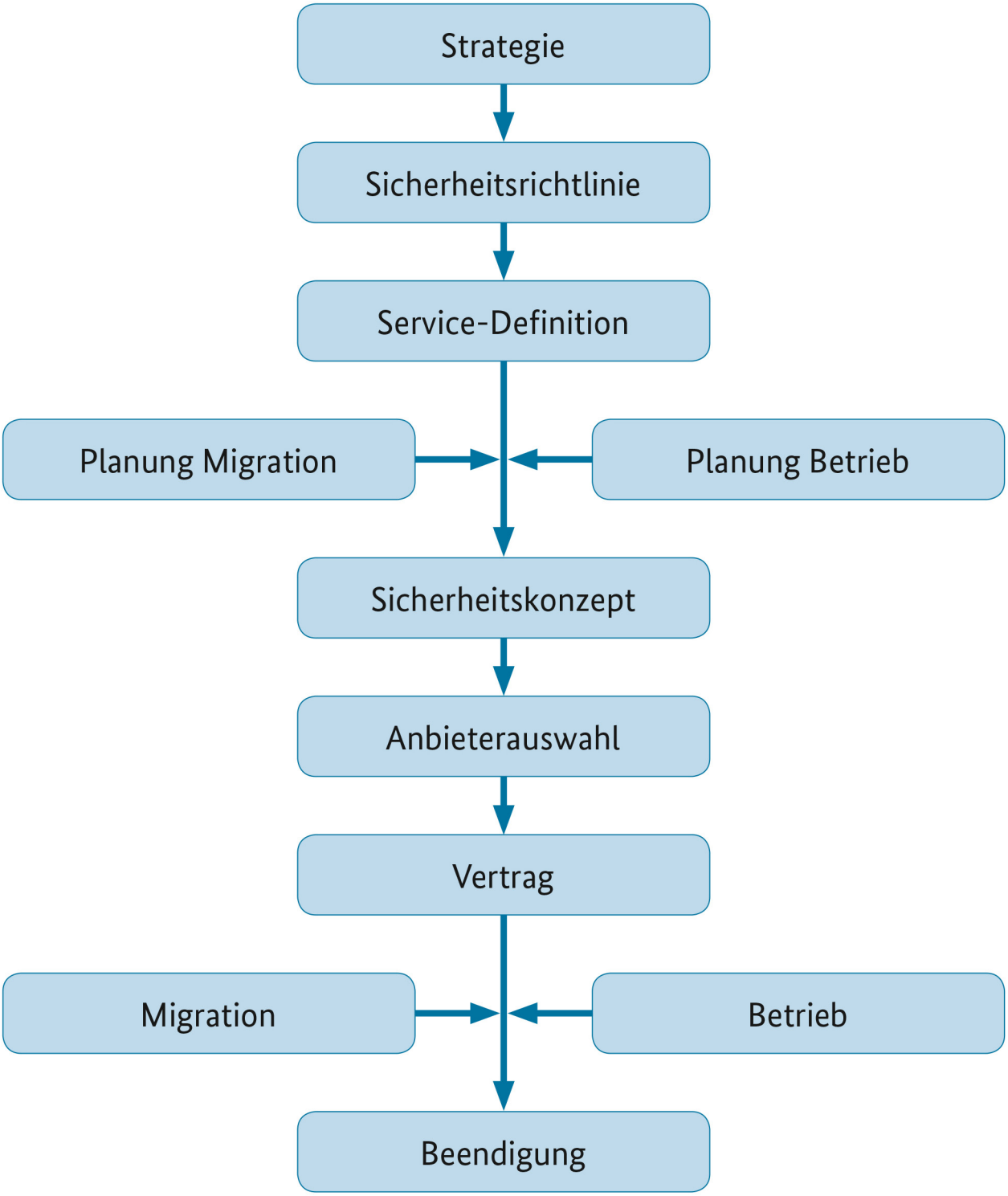
Cloud Computing zu nutzen ist eine strategische Entscheidung und kann nicht auf Arbeitsebene getroffen werde. Zwar besteht dort der Bedarf an Cloud-Diensten, aber die Möglichkeit, Cloud-Dienste effizient und sicher einzuführen, hat nur das Management bzw. die Behördenleitung. Es ist eben kein „One-Click-Job“, wie einem die Werbung gelegentlich suggeriert. Mag es auch technisch nicht so komplex sein, organisatorisch bleibt es immer ein Aufwand. Hierfür ist ein (angepasster) Prozess von der ersten Planung bis zur Einführung notwendig.

Denn das größte Risiko bei Cloud Computing ist: „Denn sie wissen nicht, was sie tun!“

4 Anhang

4 Anhang

4.1 Schematischer Überblick über einen sicheren Cloud-Nutzungsprozess



4.2 Literatur

[1] BITKOM Leitfaden: Cloud Computing – Evolution in der Technik, Revolution im Business, Oktober 2009,
www.bitkom.org/Publikationen/2009/Leitfaden/Leitfaden-Cloud-Computing/090921-BITKOM-Leitfaden-CloudComputing-Web.pdf

[2] „Anforderungskatalog Cloud Computing C5 (Cloud Computing Compliance Controls Catalogue) - Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten“, BSI, Februar 2016,
www.bsi.bund.de/C5

[3] „Sicherheitsprofil SaaS“, BSI, 2014,
www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Sicherheitsprofile/sicherheitsprofil_saas_node.html

[4] Alle Dokumente zum IT-Grundschutz des BSI,
www.bsi.bund.de/grundschutz

[5] Cloud Security Alliance (CSA) jährlich aktualisierte Liste der wichtigsten Bedrohungen,
www.cloudsecurityalliance.org/topthreats

[6] European Union Agency for Network and Information Security (ENISA): Cloud Computing Risk Assessment,
www.enisa.europa.eu/publications/cloud-computing-risk-assessment/at_download/fullReport

[7] Kompetenzzentrum Trusted Cloud: Leitfaden – Vertragsgestaltung beim Cloud Computing,
www.trusted-cloud.de/sites/default/files/media/article/downloads/ap_3_vertragsleitfaden.pdf

[8] Kompetenzzentrum Trusted Cloud: Arbeitspapier – Lizenzierungsbedarf beim Cloud Computing,
www.trusted-cloud.de/sites/default/files/media/article/downloads/arbpap_2_lizensierungsbedarf_0.pdf

[9] Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur – Orientierungshilfe Mandantenfähigkeit – Version 1.0 vom 11.10.2012,
www.bfdi.bund.de/DE/Infothek/Orientierungshilfen/Artikel/OHCloudComputing.pdf

[10] Leitfaden Recht, Datenschutz & Compliance, EuroCloud Deutschland_eco e.V.,
www.eurocloud.de/wp-content/blogs.dir/5/files/eurocloud-leitfaden_rdc.pdf

[11] Zertifizierung nach dem Trusted Cloud Data Protection Pofile,
www.trusted-cloud.de/artikel/trusted-cloud-datenschutzprofil

[12] ISO/IEC 27018:2014, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors,
www.iso.org/iso/catalogue_detail.htm?csnumber=61498

[13] ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements,
www.iso.org/iso/home/standards/management-standards/iso27001.htm

[14] ECSA – EuroCloud StarAudit, Certification for Cloud Services,
staraudit.org/

[15] Cloud Securty Alliance Zertifizerung „Open Certification Framework“,
www.cloudsecurityalliance.org/research/ocf

[16] ISO 22301:2012, Societal security – Business continuity management systems – Requirements (Notfallmanagement),
www.iso.org/iso/catalogue_detail?csnumber=50038

[17] Datenschutzzertifikat EuroPriSe des ULD,
www.european-privacy-seal.eu

[18] Standards der AICPA (American Institute of Certified Public Accountants): SSAE 16 (Statements on Standards for Attestation Engagements), SOC 1 (Service Organization Controls), SOC 2, SOC 3,
www.aicpa.org

[19] IDW-Standards (Institut der deutschen Wirtschaftsprüfer),
www.idw.de

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
Postfach 20 03 63
53175 Bonn
E-Mail: cloudsecurity@bsi.bund.de
Internet: www.bsi.bund.de/cloud

Stand
August 2016

Druck
Druck- und Verlagshaus Zarbock
Frankfurt am Main

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bildnachweis
Titelbild: Fotolia, Grafik: BSI

Artikelnummer
BSI-MIBro16/201

www.bsi.bund.de