*Für Cloud-Kund*innen ergeben sich durch die Nutzung von Cloud-Computing-Diensten verschiedene Vorteile. So entfallen beispielsweise die Kosten für den Betrieb einer eigenen IT-Infrastruktur, und der Umfang der genutzten Ressourcen kann je nach Bedarf flexibel angepasst werden. Die Nutzung von Cloud-Computing-Diensten bringt allerdings auch Risiken mit sich.*

Risiko in der Wolke?

Die Sicherheitsanalyse von Cloud-Anwendungen

Von Maritta Heisel, Denis Hatebur, Ludger Goeke und Isabelle Côté

Der Begriff „Cloud Computing" bezeichnet ein relativ neues Geschäftsmodell und die in diesem Kontext verwendeten Technologien. Im Rahmen des Cloud Computings werden verschiedene Computerressourcen in Form von sogenannten Cloud-Computing-Diensten angeboten. Hierbei bezeichnet „Dienst" unterschiedliche Angebote, wie zum Beispiel Rechenleistung, Server, Speicherplatz und Applikationen. Letztere reichen von einfachen Applikationen, wie beispielsweise Textverarbeitung, bis hin zu komplexen Anwendungen, wie beispielsweise kompletten Lagerverwaltungssystemen. Die Grundidee ist, dass aus einem Ressourcen-Pool (z.B. ein Rechenzentrum, welches virtuelle Maschinen (VMs) nutzt) diese Dienste durch Cloud-Dienstanbieter angeboten werden können.

Hierbei werden die Cloud-Computing-Dienste über ein performantes Netzwerk (Internet) bereitgestellt. Der Zugriff auf die entsprechenden Ressourcen erfolgt mit Hilfe von Standardprotokollen wie beispielsweise TCP/IP. Der Umfang der Nutzung von Ressourcen ist skalierbar und kann sehr schnell an die benötigten Ressourcen eines*einer Kund*in individuell angepasst werden.

Die oben genannten Ressourcen lassen sich drei Ebenen, auch Service-Modelle genannt, zuordnen, die im Folgenden kurz erläutert werden.

Cloud-Ebenen

Cloud-Computing-Dienste werden in Form der Service-Modelle *Software as a Service* (SaaS), Platform as a Service (PaaS) und *Infrastructure as a Service* (IaaS) angeboten. So verwendet ein SaaS-Dienst Funktionalitäten, die durch einen PaaS-Dienst bereitgestellt werden. Ein PaaS-Dienst baut wiederum auf einem IaaS-Dienst auf. Die Service-Modelle auf den verschiedenen Ebenen sind:

- SaaS: Bereitstellung von Applikationen, die innerhalb der Cloud-Infrastruktur ausgeführt werden und durch die Endkund*innen über das Internet genutzt werden. Die Endkund*innen bestellen hier Software, die sie nutzen möchten (z.B. E-Mail, Textverarbeitung, Lagerverwaltung, etc.).
- PaaS: Bereitstellung einer Plattform inklusive einer Programmierschnittstelle und Werkzeugen zur Entwicklung und Ausführung von Cloud-Applikationen durch die Cloud-Kund*innen. Die Kund*innen dieses Dienstes sind häufig Entwickler*innen, welche die Plattform und ihre Schnittstellen als

Maritta Heisel. Foto: Vladimir Unkovic

Grundlage nutzen, um weitere Applikationen zu entwickeln, die dann wiederum als SaaS angeboten werden können.
• IaaS: Bereitstellung von Computerressourcen (Rechenleistung, Speicher, usw.) als Cloud-Infrastruktur. Hierbei ist die unterliegende Cloud-Infrastruktur für Cloud-Kund*innen nicht sichtbar und dementsprechend nicht konfigurierbar. Vielmehr werden den Cloud-Kund*innen beispielsweise Betriebssysteme oder virtuelle Maschinen zur Verfügung gestellt, die diese dann konfigurieren können. Hier können die Kund*innen also Hardware in Anspruch nehmen, ohne dass diese tatsächlich gekauft und in den eigenen Räumen untergebracht werden muss.

Man kann verschiedene Modelle in Bezug auf die Bereitstellung von Cloud-Computing-Diensten unterscheiden[1]:
• Private Cloud (nicht-öffentliche Cloud): Die Cloud-Infrastruktur wird ausschließlich für eine einzige Organisation betrieben. Hierbei kann der Betrieb durch die Organisation selbst oder einen externen Dienstleister erfolgen.
• Community-Cloud: Die Cloud-Infrastruktur ist eine nicht-öffentliche Cloud, die von einer Gemeinschaft von Organisationen mit ähnlichen Anforderungen (z.B. Sicherheitsanforderungen, Verwendungszweck oder Geschäftsfelder) genutzt wird. Hierbei kann eine Community-Cloud durch die Organisationen selbst oder einen externen Dienstleister betrieben werden.
• Public Cloud (öffentliche Cloud): Die Cloud-Infrastruktur kann generell durch die Allgemeinheit oder eine entsprechend große Interessengruppe genutzt werden. Der Betrieb der Cloud-Infrastruktur erfolgt durch eine Organisation, deren Geschäftsszenario in der Bereitstellung von Cloud-Computing-Diensten besteht. Eine solche Organisation wird auch als Cloud-Dienstanbieter bezeichnet. Für die Nutzung der entsprechenden Cloud-Computing-Dienste kann der Cloud-Dienstanbieter je nach Geschäftsmodell ein Entgelt berechnen.
• Hybrid Cloud (hybride Cloud): Die Cloud-Infrastruktur wird durch eine Komposition von zwei oder mehreren Clouds gebildet. Bei den beteiligten Clouds kann es sich um Public Clouds, Private Clouds und/oder Community Clouds handeln. Im Rahmen einer Hybrid Cloud bleiben die einzelnen Clouds eigenständig. Sie werden mit Hilfe entsprechender Technologien verbunden, um den Austausch von Daten zwischen den einzelnen Clouds und die Portabilität von Cloud-Anwendungen zu ermöglichen.

Möglichkeiten des Cloud Computing

Für Cloud-Kund*innen ergeben sich durch die Nutzung von Cloud-Computing-Diensten verschiedene Vorteile. So entfallen beispielsweise die Kosten für den Betrieb einer eigenen IT-Infrastruktur, und der Umfang der genutzten Ressourcen kann je nach Bedarf flexibel angepasst werden. Die Nutzung von Cloud-Computing-Diensten bringt allerdings auch Risiken mit sich. So könnten beispielsweise die Vertraulichkeit und Integrität von Daten der Cloud-Kund*innen durch böswilliges Personal des Cloud-Dienstanbieters oder eine versehentliche Fehlkonfiguration der Cloud-Infrastruktur verletzt werden. Auch die Verfügbarkeit der Kund*innendaten könnte zum Beispiel durch Störungen in Bezug auf die Internetverbindung oder das Rechenzentrum sowie durch die Insolvenz von Cloud-Dienstanbietern gefährdet sein.

Informationssicherheit von Clouds

Ein generelles Hindernis bei der Verbreitung von Cloud-Computing-Diensten besteht darin, dass die Anbieter von Cloud-Computing-Diensten ihre potentiellen Kund*innen nur schwer von der Sicherheit ihrer Dienste überzeugen können. In der Studie „Cloud-Monitor 2016“, die von der Bitkom Research GmbH und KPMG AG erstellt wurde, wird erstmals eine Nutzung von Cloud Computing durch die Mehrheit der befragten Unternehmen beobachtet. Weiterhin sei ein starker Anstieg der Cloud-Nutzung bei Unternehmen von kleiner und mittlerer Größe zu verzeichnen. Es wird allerdings auch angemerkt, dass Sicherheitsbedenken eine noch stärkere Verbreitung von Cloud-Computing-Diensten verhindern würden. In Bezug auf die Public Cloud bezögen sich die größten Befürchtungen der befragten Unternehmen auf unberechtigte Zugriffe auf sensible Unternehmensdaten und den möglichen Verlust von Daten.

Eine stärkere Verbreitung von Cloud Computing könnte erreicht werden, wenn die Cloud-Dienstanbieter die Sicherheitsfunktionalitäten ihrer Dienste transparent für potentielle Kund*innen machen würden. Diese Transparenz kann durch eine Zertifizierung von Cloud-Computing-Diensten durch einen unabhängigen Dritten erreicht werden. Dazu müssen die Sicherheitsanforderungen und die Sicherheitsfunktionalitäten der Cloud-Computing-Dienste genau beschrieben werden.

ISO 27001

Eine Möglichkeit besteht in der Zertifizierung eines sogenannten *Information Security Management Systems* (ISMS). Im Rahmen eines ISMS werden die Prozesse bezüglich der Informationssicherheit einem Management-Rahmen unterstellt. Hierdurch soll erreicht werden, dass ein ausreichendes Niveau an Informationssicherheit innerhalb einer Organisation erreicht und beibehalten wird. Hierbei werden auch Änderungen von Prozessen innerhalb einer Organisation sowie Änderungen in Bezug auf die Gefahrenlage berücksichtigt. Das deutsche Bundesamt für Sicherheit in der

Informationstechnik (BSI) unterstrich 2012 in einer Veröffentlichung[2] ausdrücklich die Notwendigkeit des Betriebes eines ISMS auf Seiten der Cloud-Dienstanbieter.

Bei der *ISO 27001:2013* (ISO/IEC 2013) handelt es sich um einen international anerkannten Standard, der Anforderungen an ein ISMS definiert. Diese Anforderungen beziehen sich auf die Planung, den Betrieb und die kontinuierliche Verbesserung eines ISMS. Ein ISMS nach ISO 27001:2013 wird durch eine akkreditierte Zertifizierungsstelle zertifiziert. Der Managementteil der ISO 27001:2013 definiert die Tätigkeiten, die durchzuführen sind. Hierzu gehören die Definition des Geltungsbereiches des ISMS, die Durchführung einer Risikoanalyse oder die Durchführung interner Audits. Im Anhang A der ISO 27001:2013 werden Maßnahmen definiert, die innerhalb des ISMS umgesetzt werden müssen, wenn sie für die betreffende Organisation relevant sind. Bei diesen Maßnahmen handelt es sich unter anderem um Informationssicherheits-Prozesse oder zu erstellende Informationssicherheits-Richtlinien.

ClouDAT

Ein Problem bei der Umsetzung eines ISMS nach ISO 27001:2013 besteht darin, dass in der ISO-Norm dazu keine konkreten Vorgehensweisen beschrieben werden. Im Rahmen des Forschungsprojektes *ClouDAT*[3] wurde eine musterbasierte Methode für die Planungsphase eines ISMS nach ISO 27001:2013 im Kontext des Cloud Computing entwickelt. Hierbei werden insbesondere die Definition des ISMS-Geltungsbereiches und die Durchführung der Risikoanalyse unterstützt. Zusätzlich wird die entwickelte Methode durch ein Software-Werkzeug unterstützt, das ebenfalls den Namen *ClouDAT* (Cloud Data Analysis Tool) trägt. Das ClouDA-Tool ermöglicht die Erfassung der notwendigen Informationen, sowie die Generierung von notwendigen Dokumentationsartefakten. Dieses Vorgehen unterstützt das Tool durch einen musterbasierten Ansatz. So erfolgt die Definition des ISMS-Geltungsbereichs beispielsweise durch die Instanziierung eines grafischen Musters. Dieses Muster spezifiziert bereits die Elemente, die im Kontext der meisten Cloud-Computing-Dienste relevant sind. Weiterhin werden Kataloge mit textbasierten Mustern in Bezug auf grundlegende Bedrohungen für und Sicherheitsanforderungen an Cloud-Computing-Dienste bereitgestellt. Eine ausführliche Beschreibung der *ClouDAT*-Methode und des ClouDA-Tools geben wir in den Abschnitten „Die ClouDAT-Methode“ und „ClouDA-Tool“. Die ClouDAT-Methode und das ClouDA-Tool wurden im Rahmen einer Fallstudie in Zusammenarbeit mit dem Lanfer Systemhaus aus Dortmund evaluiert. Hierbei wurde ein Cloud-Dienst-Modell in Form von IaaS betrachtet. Ein elementarer Bestandteil von ClouDAT ist die im nächsten Abschnitt beschriebene Risikoanalyse.

Risikoanalyse

Eine Risikoanalyse wird für die Assets einer Organisation durchgeführt. Hierbei bezieht sich der Begriff Asset auf alles, was einen Wert für die Organisation darstellt. So kann es sich bei Assets um Geschäftsprozesse, Informationen oder physische Dinge (z.B. Gebäude, Server, Netzwerk) handeln. Das Ziel der Risikoanalyse besteht darin, einen Wert für das Risiko zu ermitteln, dass die Informationssicherheits-Eigenschaften Vertraulichkeit, Integrität und Verfügbarkeit eines Asset kompromittiert würden. Dazu werden jeweils Werte in Bezug auf die Bedeutung von Assets (engl. Asset Value) bestimmt sowie die Bedrohungen (engl. Threats) für Assets und Schwachstellen (engl. Vulnerabilities) von Assets betrachtet.

Bezüglich der Durchführung der Risikoanalyse definiert die ISO 27001:2013 keine konkrete Methode. Es wird lediglich vorgeschrieben, dass die verwendete Risikoanalysemethode valide Werte produziert, die reproduzierbar und vergleichbar sind. Im Rahmen der ISO 2700x-Normenreihe beschreibt der informative Standard ISO 27005:2011 Hilfestellungen zur Durchführung einer Risikoanalyse.

Die ClouDAT-Methode umfasst ein Vorgehen für die Durchführung der Risikoanalyse, die dementsprechend durch das ClouDA-Tool unterstützt wird. Da die verschiedenen Schritte der ClouDAT-Methode innerhalb des ClouDA-Tools durch separate Plugins umgesetzt werden, könnte die vorhandene Risikoanalysemethode ohne großen Aufwand durch eine andere Methode ersetzt werden. Die Durchführung der ClouDAT-Risikoanalyse wird im Rahmen der Beschreibung der ClouDAT-Methode in Schritt 4 „Risiken bewerten“ ausführlicher diskutiert.

Die ClouDAT-Methode

Mit Hilfe der ClouDAT-Methode können Cloud-Computing-Dienste in Form von SaaS, PaaS und IaaS, sowie die korrespondierenden relevanten Geschäftsprozesse für eine Begutachtung durch Dritte dokumentiert werden. So können für im Aufbau befindliche beziehungsweise bestehende Cloud-Computing-Dienste Sicherheitsrisiken aufgedeckt werden. Sicherheitsrisiken wären beispielsweise das Öffentlichwerden von vertraulich zu haltenden Daten, unbefugte Zugriffe von Mitarbeiter*innen des Cloud-Dienstanbieters auf Daten, Veränderung der Funktionalität von Diensten, oder eine Einschränkung der Verfügbarkeit von Diensten. Die ClouDAT-Methode ist für alle Arten von Clouds einsetzbar.

Bei der Dokumentation der ermittelten Sicherheitsanforderungen an Cloud-Computing-Dienste

müssen das deutsche Recht im Bereich IT-Sicherheit und insbesondere die Einhaltung des Bundesdatenschutzgesetzes durch den Cloud-Dienstanbieter beachtet werden. Ein*e potentielle*r Cloud-Computing-Nutzer*in soll anhand der Dokumentation der realisierten Sicherheitsanforderungen durch den Cloud-Dienstanbieter entscheiden können, ob der erbrachte Dienst seinen*ihren Sicherheitsanforderungen genügt. Wir haben einen Sicherheitsanforderungskatalog erstellt, der für IaaS, PaaS und SaaS eine Zertifizierung nach ISO 27001 ermöglicht. Neben Anforderungen aus Gesetzestexten oder Standards haben individuelle Sicherheitsbedürfnisse der Cloud-Anbieter und der Kund*innen Berücksichtigung gefunden. Zur Dokumentation der Sicherheitsanforderungen werden von ClouDAT Muster bereitgestellt. Konkrete Sicherheitsanforderungen können in diese Muster durch Einsetzen konkreter Elemente eingepasst werden. Die einzusetzenden Elemente und deren Beziehungen untereinander können mit ClouDAT spezifiziert werden.

Cloud-Dienstanbieter wollen oft gegenüber ihren Kund*innen und insbesondere gegenüber Mitbewerbern am Markt ihre Sicherheitsmaßnahmen nicht offenlegen. Auch möchte ein Cloud-Dienstanbieter nicht unbedingt allgemein offenlegen, welche (zertifizierten) Sicherheits-Komponenten verwendet werden. Daher kann nur von einem externen, zur Verschwiegenheit verpflichteten Gutachter geprüft werden, inwieweit die umgesetzten Maßnahmen geeignet sind, die Sicherheitsanforderungen ausreichend zu erfüllen. ClouDAT erlaubt dem Cloud-Dienstanbieter eine erste Validierung bezüglich dieser Fragestellungen selbst durchzuführen.

Für den Zertifizierer werden von ClouDAT Dokumente erzeugt, die die Sicherheitsanforderungen und Maßnahmen beschreiben. Auch werden die Beziehungen der Sicherheitsanforderungen untereinander und auch der Maßnahmen untereinander in nachvollziehbarer Weise dargestellt. Der Zertifizierer kann somit die Validierungen der Anbieter mit geringem Aufwand überprüfen. Die Hauptaufgabe des Zertifizierers ist es, im Rahmen eines Zertifizierungsaudits eines Cloud-Computing-Dienstes zu prüfen, ob die dokumentierten Maßnahmen korrekt realisiert wurden.

ClouDAT hat gegenüber einem informellen Vorgehen folgende Vorteile:

- Es stellt Musterkataloge für Bedrohungen, Sicherheitsanforderungen und eine Liste von möglichen Maßnahmen zur Erfüllung der Sicherheitsanforderungen bereit.
- Es stellt Nachverfolgbarkeits-Verknüpfungen zwischen den verschiedenen Musterkatalogen bereit.
- Es schlägt zum Teil automatisch passende Muster auf Basis der zuvor ausgewählten Muster vor.

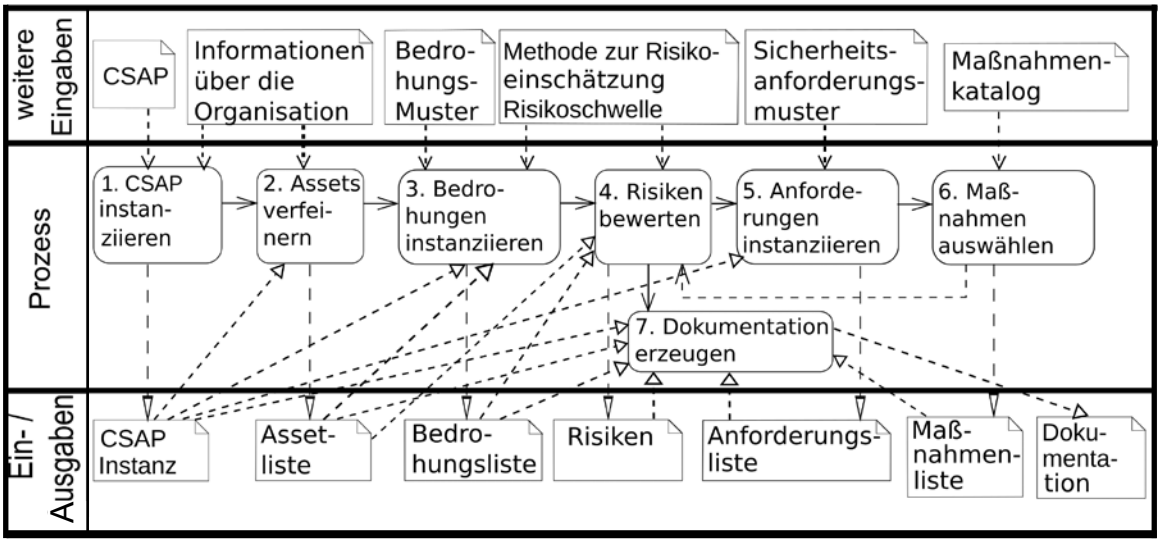
Die von ClouDAT erstellte Dokumentation folgt dem ISO 27001-Standard.

Vorgehensweise zur Erstellung einer geeigneten Dokumentation

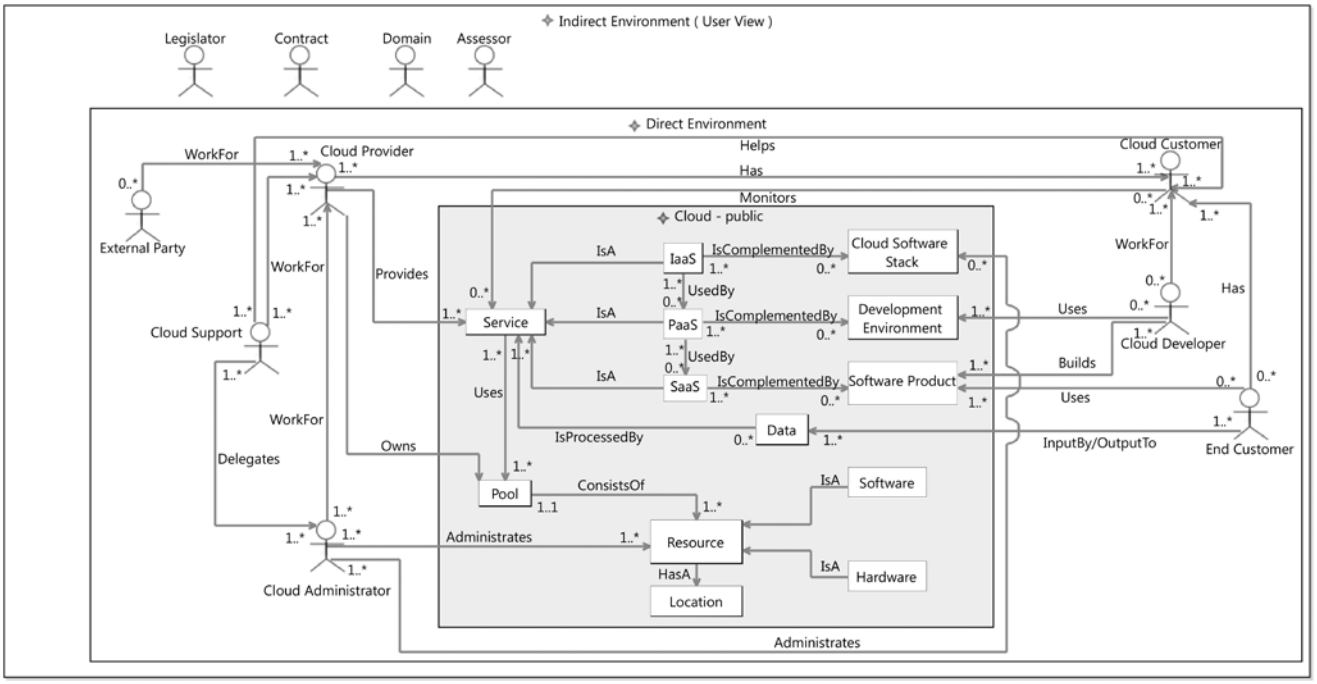
Abbildung (1) gibt einen Überblick über die sieben Schritte der ClouDAT-Methode mit Eingabe- und Ausgabedokumenten, die wir in diesem Abschnitt näher erläutern.

Schritt 1: Instanziierung des CSAP

In diesem Schritt wird der Bereich definiert, für den ein ISMS gelten soll. Dieser Geltungsbereich muss definiert sein, bevor eine Risikoanalyse durchgeführt werden kann. Im Rahmen der ClouDAT-Methode wird dazu das sogenannte Cloud-System-Analysemuster (Cloud System Analysis Pattern, CSAP)[4],



(1) Überblick über die bei ClouDAT angewandte Methode.
Quelle: eigene Darstellung



(2) Das Cloud-System-Analysemuster (CSAP).
Quelle: eigene Darstellung

instanziiert. Im Folgenden diskutieren wir das CSAP, das in Abbildung (2) gezeigt wird.

Das CSAP stellt Elemente zur Verfügung, um einen Cloud-Computing-Dienst zu beschreiben. Hierbei erfolgt eine Beschreibung der direkten Umgebung und indirekten Umgebung des betreffenden Cloud-Computing-Dienstes anhand der Typen von Interessensvertretern (engl. Stakeholders). Zudem wird der Cloud-Computing-Dienst (Cloud) an sich spezifiziert. Hierzu werden verschiedene Typen von Cloud-Elementen verwendet. Wir erklären nun die zuvor genannten CSAP-Elemente und nennen jeweils die Typen der Elemente, die im CSAP definiert sind:

• Indirekte Umgebung (engl. Indirect Environment): Hier erfolgt eine Spezifikation der indirekten Interessensvertreter (engl. Indirect Stakeholder). Diese Interessensvertreter zeichnen sich dadurch aus, dass sie keine direkte Verbindung zum betrachteten Cloud-Computing-Dienst haben. Sie sind allerdings indirekt für den Betrieb des Cloud-Computing-Dienstes relevant. Das CSAP enthält indirekte Interessensvertreter der folgenden Typen

  ◦ Gesetzgeber (engl. Legislator): Gesetzgebungen der Nationen, in der der Cloud-Computing-Dienst betrieben wird.

  ◦ Vertrag (engl. Contract): Vertragliche Vereinbarungen

  ◦ Domäne (engl. Domain): Einschränkungen aus der Anwendungsdomäne, zum Beispiel Basel II/III-Vorschriften für Banken

  ◦ Zertifizierer (engl. Assessor): Unternehmen, das das ISMS des Cloud-Computing-Diensts zertifizieren soll.

• Direkte Umgebung (engl. Direct Environment): Diese Umgebung enthält die Beschreibung der direkten Interessensvertreter, die eine unmittelbare Verbindung zum betreffenden Cloud-Computing-Dienst aufweisen. Die verschiedenen Typen von direkten Interessensvertretern im CSAP spezifizieren Cloud-Dienstanbieter, Cloud-Dienst-Kund*innen (dieser nutzt den Dienst, um Endkunden einen eigenen Dienst anzubieten), Cloud-Dienst-Endkund*innen, Entwickler*innen für Cloud-spezifische Applikationen, Cloud-Administratoren sowie die technische Kund*innenbetreuung (Support) des Cloud-Computing-Dienstes.

• Cloud-Computing-Dienst (Cloud): Hier erfolgt die Definition der verschiedenen Typen von Cloud-Elementen, aus denen sich der betrachtete Cloud-Computing-Dienst zusammensetzt.

Für unseren Beitrag werden wir uns jedoch auf eine Auswahl dieser Typen beschränken: die relevanten Cloud-Dienst-Modelle (IaaS, PaaS, SaaS), den Software-Stack der Cloud-Infrastruktur (Cloud Software-Stack), in der Cloud ausgeführte Softwareprodukte (engl. Software Product), die beteiligten Standorte (Location), die in der Cloud verarbeiteten Daten (Data) sowie die verwendeten Hard- und Software (Hardware, Software) für den Betrieb der Cloud.

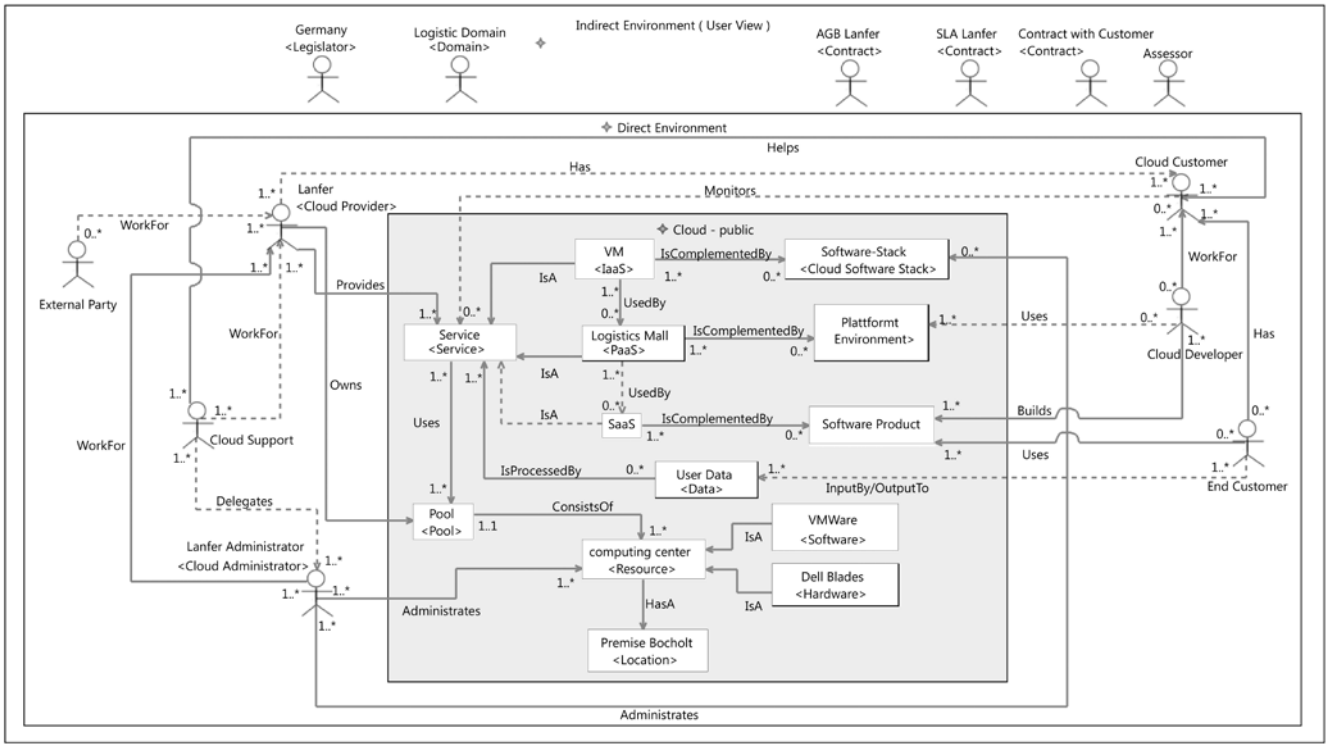
Zusätzlich enthält das CSAP Verbindungen zur Darstellung der logischen Beziehungen zwischen direkten Interessensvertretern und Cloud-Elementen.

Die Namen der verschiedenen CSAP-Elemente (Indirect/Direct

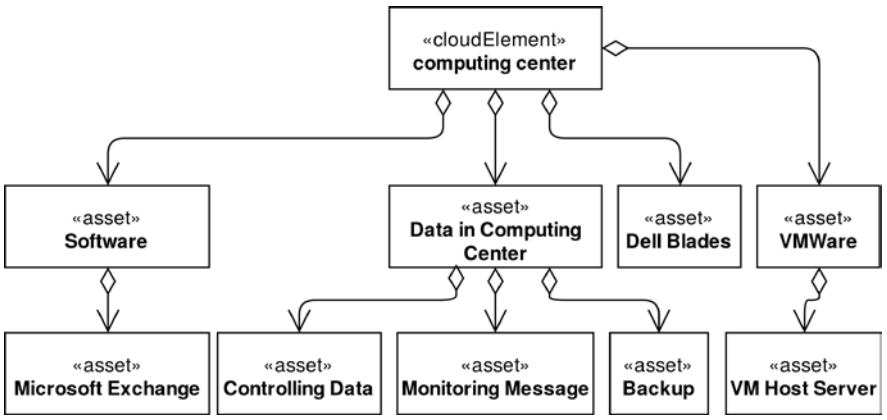
Stakeholder, Cloud-Element) korrespondieren zu ihren sogenannten „Instanztypen“, welche die Art der Elemente beschreiben. In Bezug auf das CSAP enthält dieses beispielsweise einen indirekten Interessensvertreter mit dem Instanztypen „Legislator“ (s. Abb. 2). Bei der Instanziierung des CSAP wird der „Legislator“ durch einen konkreten Namen ersetzt, beispielsweise „Germany“, der den Gesetzgeber der Bundesrepublik Deutschland repräsentiert, siehe Abbildung (3). Die Instanziierung wird für alle relevanten Elemente wiederholt. Sie beginnt zum Beispiel mit der Identifikation der möglichen Kund*innen des Cloud-Computing-Dienstes („Cloud Customer“). Diese nehmen dann die bereitgestellten Cloud-Computing-Dienste in Anspruch, um sie für ihre geschäftlichen Aktivitäten zu nutzen. Der Anbieter der bereitgestellten Cloud-Computing-Dienste muss ebenfalls instanziiert werden. Im Rahmen unserer Fallstudie wird dieser Anbieter durch das Lanfer Systemhaus dargestellt. In dem CSAP werden auch die Gruppen und Regularien betrachtet, die zwar keine direkte Verbindung zu dem Cloud-Computing-Dienst haben, aber trotzdem berücksichtigt werden müssen, wie beispielsweise der Gesetzgeber und andere Regeln (Germany, Dienstleistungsvereinbarungen (engl. Service Level Agreements, SLA), Lanfer, …). Es werden dann auch die Elemente des Cloud-Computing-Dienstes instanziiert (siehe grau hinterlegter Teil in Abb. 3). Diese stellen die vorhandenen Betriebsmittel (z.B. Hardware und Software) und die Dienste, die bereitgestellt werden, dar. Die instanziierten Cloud-Elemente können Assets des Cloud-Dienstanbieters sein. Bezüglich dieser Assets wird die Risikoanalyse ausgeführt, um Sicherheitsrisiken aufzudecken.

Schritt 2: Verfeinerung von Assets

Dieser Schritt bezieht sich auf Assets, die in Form von Cloud-Elementen im CSAP instanziiert wurden. Innerhalb dieses Arbeitsschrittes sind solche Assets relevant, deren Abstraktionsgrad für eine sinnvolle Verwendung innerhalb der Risikoanalyse zu hoch ist. Abbildung (4) zeigt einen Ausschnitt des Verfeinerungsdiagramms aus unserer Fallstudie. Das Rechenzentrum („computing center“) ist ein Asset, dessen Abstraktionsgrad für die Risikoanalyse zu hoch ist. Deshalb ist eine Verfeinerung notwendig: Das Rechenzentrum („computing center“) wird zunächst in die „Software“ und die Daten im Rechenzentrum („Data In Computing Center“) zerlegt. Diese neuen Assets werden weiter zerlegt, da auch hier der Abstraktionsgrad noch zu hoch ist: „Microsoft Exchange“ ist ein Beispiel für „Software“. Daten des Controllings („Controlling Data“), Überwachungsnachrichten („Monitoring Message“) und „Backup“ verfeinern die Daten im Rechenzentrum („Data In Computing Center“). Weitere Verfeinerungen können Abbildung (4) entnommen werden. Wie wir in dieser Abbildung sehen, wurde die „Ist-Bestandteil-von-Beziehung“ benutzt,



(3) Instanz des Cloud-System-Analysemusters für das Lanfer Systemhaus.
Quelle: eigene Darstellung



(4) Beispiel für eine Verfeinerung von Assets.
Quelle: eigene Darstellung

um die Asset-Verfeinerung darzustellen.

Das allgemeine Vorgehen lässt sich wie folgt beschreiben: Betrachte die einzelnen Assets des instanziierten CSAP und nutze gegebenenfalls Prozesse, Richtlinien und Standorte der Organisation, um Assets weiter zu verfeinern.

Für unsere Fallstudie bedeutet das: Um die Assets zu identifizieren, haben wir das instanziierte CSAP als Startpunkt verwendet. Zusätzlich haben wir zur Validierung unseres Ansatzes durch Arbeitsanweisungen, Organigramme, andere Firmendokumente und einen Besuch des Rechenzentrums weitere Assets identifiziert, deren Gesamtanzahl 103 betrug. Unabhängig davon hatten wir dieselben Assets auch durch die Verfeinerungs-Vorgehensweise identifiziert.

Für jedes Asset haben wir (wie auch bei den Cloud-Elementen im CSAP) folgende Informationen dokumentiert:

- Besitzer*in des Assets: Die*Der Besitzer*in ist für das Asset verantwortlich. So muss die*der Besitzer*in beispielsweise die Zugriffsrechte für das Asset kontrollieren.
- Standort des Assets: Hier wird zum Beispiel dokumentiert, dass der „Microsoft Exchange"-Server im „Rechenzentrum 1" steht.
- Art/Typ des Assets: Dokumentation des Typs eines Assets. Dieser Typ entspricht dem Instanztypen von CSAP-Elementen, der bereits in Schritt 1 besprochen wurden. So kann beispielsweise festgehalten werden, ob es sich bei einem Asset um Software oder Daten handelt.
- Relevanz des Assets: Definition, ob ein Asset relevant für die Risikoanalyse ist. Wenn es sich nicht um ein relevantes Asset handelt, wird auch dokumentiert, warum dieses Asset nicht relevant ist. Zum Beispiel wird dokumentiert, dass die Virenschutzsoftware kein Asset an sich ist, sondern zum Schutz der anderen Assets beiträgt.

Die relevanten Assets werden in den folgenden Schritten der Risikoanalyse weiter betrachtet.

Schritt 3: Instanziierung von Bedrohungsmustern mit Schwachstellen

Für alle relevanten Assets aus Schritt 2 wird eine Bedrohungsanalyse durchgeführt. Dabei wird untersucht, ob ein Asset einer Bedrohung ausgesetzt ist, und ob das Asset Schwachstellen besitzt, die durch die bestehenden Bedrohungen ausgenutzt werden könnten. Um diese Analyse zu unterstützen, stellt CloudDAT einen Katalog mit Mustern für Bedrohungen bereit, die auf der Basis des Stands der Technik und der Erfahrung der Autoren erstellt wurden. Der Katalog lässt sich problemlos erweitern. Spezielle Bedrohungen für Cloud-Computing-Dienste sind beispielsweise unsichere Schnittstellen, beziehungsweise Verlust oder ungewolltes Veröffentlichen von Daten.

Die Struktur der Muster für Bedrohungen wird durch ein Modell definiert, bei dem es feste Textpassagen und Platzhalter gibt. Bei den Platzhaltern handelt es sich um die Instanztypen von direkten und indirekten Interessensvertretern und Cloud-Elementen. Die Platzhalter werden durch den Namen des relevanten Elementes aus dem instanziierten CSAP oder der Verfeinerungsdiagramme ersetzt. Der Katalog ist nach den Kategorien Vertraulichkeit, Integrität und Verfügbarkeit sortiert. Für jedes Asset sollten alle Kategorien betrachtet werden. Weitere Kategorien, wie zum Beispiel „Privacy" können ergänzt werden. Ein Beispiel für ein Muster für eine Bedrohung ist:

„Unavailability of [cloud element] for [all end customers and cloud customers]."
(Nicht-Verfügbarkeit eines [Cloud Elementes] für [alle Endbenutzer und Cloudnutzer]).

Um dieses Muster zu instanziieren, muss der Name aus der CSAP-Instanz eingesetzt werden:

„Unavailability of Controlling Data for Lanfer Systemhaus."
(Nicht-Verfügbarkeit der Daten des Controllings für das Lanfer Systemhaus).

Die Verwendung unseres Kataloges reduziert das Risiko, dass wesentliche Bedrohungen in der Analyse nicht betrachtet werden. Ergänzend geben wir Beispiele für Schwachstellen an, die zum Ausnutzen dieser Bedrohung führen können.

Die Identifikation der Bedrohungen und Schwachstellen unterstützt die Einschätzung des Bedrohungspotentials, das wir durch das Interesse des Angreifers und die Größe der Schwachstellen (vulnerability level) beschreiben. Das Inte-

resse des Angreifers klassifizieren wir in LOW, MEDIUM und HIGH als Standardwerte.

Die Schwachstellen beschreiben wir mit L, wenn nahezu alle Schwachstellen mit entsprechenden Maßnahmen adressiert sind, mit M, wenn ein mittlerer Schutz gegeben ist, und mit H, wenn keine geeigneten Maßnahmen existieren, um die Bedrohung abzuwehren.

Aus diesen Informationen werden wir in Schritt 4 das Bedrohungspotential ermitteln. Dieses bestimmt zusammen mit dem Wert des Assets das Risiko, dem das Asset ausgesetzt ist.

Schritt 4a: Risiken bewerten

Wir benutzen eine Risikoschwelle, um zu entscheiden, ob ein Asset im Weiteren behandelt werden muss. Die ISO 27001:2013 verlangt, dass eine angemessene Methode für die Risikoeinschätzung gewählt wird, die vergleichbare und reproduzierbare Ergebnisse liefert, und dass ein Risikowert definiert wird, unterhalb dessen das Risiko akzeptiert wird.

Das Risiko setzt sich aus dem Bedrohungspotential und dem Wert des Asset zusammen. Wir ermitteln es durch Multiplikation zweier numerischer Werte, die diese beiden Faktoren repräsentieren. Dazu definieren wir eine Skala von Werten, anhand derer der Einfluss von Assets auf das Unternehmen untersucht werden kann. Dieser Einfluss bezieht sich darauf, dass die Sicherheitsziele (z.B. Vertraulichkeit, Integrität und Verfügbarkeit) eines Assets im Zuge eines Sicherheitsvorfalls kompromittiert würden. Im Rahmen von CloudAT wird eine Werte-Skala definiert, in der sich der jeweilige Wert für ein Asset aus möglichen Konsequenzen für das Unternehmen ergibt. Der Wert eines Assets ist auf

- 1 zu setzen, wenn keine Konsequenzen aus einem Sicherheitsvorfall erwartet werden müssen,
- 2 zu setzen, wenn mit den Konsequenzen einfach umgegangen werden kann,
- 3 zu setzen, wenn ein moderater Aufwand erforderlich ist, um mit den Konsequenzen umzugehen,
- 4 zu setzen, wenn ein hoher Aufwand erforderlich ist, um mit den Konsequenzen umzugehen und
- 5 zu setzen, wenn das Überleben des Unternehmens durch einen Sicherheitsvorfall gefährdet wäre.

Eine andere Definition der Werte ist einfach möglich.

Das Bedrohungspotential wird folgendermaßen aus den Einschätzungen ermittelt, die wir in Schritt 3 vorgenommen hatten:

- 1 bei L (Interesse des Angreifers), LOW (Schwachstellen),
- 2 bei L, MEDIUM oder M, LOW,
- 3 bei H, LOW oder L, HIGH oder M, MEDIUM,
- 4 bei M, HIGH oder H, MEDIUM
- 5 bei H, HIGH

Nun kann der Risikowert durch eine Multiplikation des Werts des Assets und des Bedrohungspotentials ermittelt werden.

Für unser Asset „Controlling Data“ kamen wir damit zum Beispiel in Bezug auf die Vertraulichkeit auf einen Risikowert von 12 und für unser Asset „VM Host Server“ in Bezug auf die Integrität auf einen Risikowert von 15.

Schritt 4b: Risiko überprüfen

Nachdem das Risiko für alle Assets systematisch abgeschätzt wurde, muss gemäß ISO 27001 geprüft werden, ob der Risikowert ein akzeptables Risiko darstellt. Als Risikoschwelle haben wir den Wert 10 gewählt. Einen Risikowert kleiner oder gleich 10 akzeptieren wir aus den folgenden Gründen:

- Wenn wir keine Konsequenzen erwarten, um mit den Auswirkungen eines erfolgreichen Angriffs umzugehen, oder mit ihnen einfach umgegangen werden kann (Wert des Assets = 1 oder 2), können wir das Risiko akzeptieren, auch wenn Angreifer ein großes Interesse haben und keine Maßnahmen gegen die Schwachstellen vorhanden sind (Bedrohungspotential = 5).
- Wenn wir bei einem erfolgreichen Angriff mittelmäßigen Aufwand erwarten (Wert des Assets = 3), können wir das Risiko akzeptieren, wenn das Bedrohungspotential den Wert 3 hat.
- Wenn durch die Auswirkungen eines erfolgreichen Angriffs das Überleben des Unternehmens gefährdet oder ein hoher Aufwand erforderlich wäre, um damit umzugehen (Wert des Assets = 4 oder 5), können wir das Risiko akzeptieren, wenn nahezu alle Schwachstellen mit entsprechenden Maßnahmen adressiert sind oder bei einem mittleren Schutz von einem Angreifer mit nur mittlerem Interesse ausgegangen werden kann (Bedrohungspotential = 1 oder 2).

Die Vertraulichkeit unseres Assets „Controlling Data“ ist mit dem Risikowert von 12 bewertet und die Integrität unseres Assets „VM Host Server“ ist mit dem Risikowert von 15 bewertet. Für die weiteren hier erwähnten Assets kann bei den gegebenen Maßnahmen das Risiko akzeptiert werden.

Um mit einem Risiko umzugehen, das nicht akzeptabel ist, definiert die ISO 27001:2013 folgende Alternativen:

1. geeignete Maßnahmen anwenden, um das Risiko auf ein akzeptables Maß zu reduzieren,
2. das Risiko explizit akzeptieren,
3. das Risiko vermeiden, oder
4. das Risiko an andere abgeben.

Wir legen unseren Schwerpunkt auf Alternative 1 (Maßnahmen anwenden). Immer, wenn diese Alternative gewählt wird, fahren wir mit Schritt 5 fort. Wenn keine weitere Bewertung einen Risikowert über dem Schwellwert hat beziehungsweise wir eine andere Alternative gewählt haben, können wir zu Schritt 7 gehen.

Schritt 5: Sicherheitsanforderungen instanziieren

In diesem Schritt werden alle Assets betrachtet, bei denen wir ein nicht-akzeptables Risiko identifiziert haben

und für die wir geeignete Maßnahmen durchführen wollen, um das Risiko zu reduzieren. Um geeignete Maßnahmen zu finden, müssen wir Sicherheitsanforderungen definieren. Dazu nutzen wir sogenannte Sicherheitsanforderungsmuster. Diese Muster sind nach dem gleichen Prinzip aufgebaut, wie die Muster für Bedrohungen. Sie enthalten neben fixem Text auch Platzhalter, die den Instanztypen der relevanten CSAP-Elementen entsprechen. Zudem haben wir eine Zuordnung von den Mustern für Bedrohungen zu den Mustern für Sicherheitsanforderungen erstellt. So schlägt unser Werkzeug für jede Instanz eines Bedrohungsmusters die zugeordneten Sicherheitsanforderungsmuster vor, die ebenfalls instanziiert werden. Für die Bedrohung

„Disclosure of stored controlling data of Lanfer Systemhaus by an attacker“,
(Offenlegung von gespeicherten Daten für das Controlling des Lanfer Systemhauses durch einen Angreifer)

ist das entsprechende Muster für eine Sicherheitsanforderung:

„Preserve confidentiality of stored [data] of [cloud customer, end customer] by preventing disclosure by [cloud provider, phone support, cloud administrator, cloud developer, third-party provider, other cloud customer, other end customer, external attacker]“
(Stelle die Vertraulichkeit der gespeicherten [Daten] des [Cloud-Kunden, Endkunden] sicher, indem die Offenlegung durch [Cloud-Anbieter, Hotline, Cloud-Administratoren, Cloud-Entwickler, ausgelagerte Anbieter, andere Cloud-Kunden, andere End-Kunden, externe Angreifer] verhindert wird.)

Dieses Muster kann ausgewählt und wie folgt instanziiert werden (bei der Instanziierung kann die Instanziierung des Bedrohungs-Musters zur Hilfe genommen werden):

SR1 “Preserve confidentiality of stored controlling data of Lanfer Systemhaus by preventing disclosure by an external attacker.“
(Stelle die Vertraulichkeit der gespeicherten Daten für das Controlling des Lanfer Systemhauses sicher, indem die Offenlegung durch externe Angreifer verhindert wird.)

Mit Hilfe der Zuordnung der Muster für Bedrohungen zu den Mustern für Sicherheitsanforderungen haben wir für die Fallstudie Sicherheitsanforderungen für Assets ausgewählt, deren Risiken nicht akzeptiert werden können. Zusätzlich zu SR1 ergaben sich die folgenden Sicherheitsanforderungen:
• Forderung von Integrität in Bezug auf die Kommunikation zwischen den Virtuellen Maschinen und den Mitarbeitern (SR 2),
• Verhinderung von Manipulationen des „VM Host Server“, die zur Nicht-Verfügbarkeit führen würden (SR 3),
• Ausreichender physischer Schutz (keine Fenster im Erdgeschoss, Zutrittskontrolle und beschränkter Zugang durch Besucher*innen, …) (SR 4) und
• Keine Beeinflussung der Verfügbarkeit der bereitgestellten Plattform durch technische Fehler des „VM Host Server“ (SR 5).

Der Vorteil von explizit formulierten Sicherheitsanforderungen besteht darin, dass geprüft werden kann, ob diese erfüllt sind. Wenn alle relevanten Sicherheitsanforderungen für einen Cloud-Computing-Dienst erfüllt sind, ist das erreichte Sicherheitsniveau ausreichend.

Schritt 6: Maßnahmen auswählen

In diesem Schritt werden Maßnahmen ausgewählt, die für die in Schritt 5 identifizierten Sicherheitsanforderungen angemessen sind. Mögliche Maßnahmen haben wir in einem Katalog zusammengefasst und mit den entsprechenden Sicherheitsanforderungen verknüpft, so dass eine Vorauswahl der möglichen Maßnahmen werkzeuggestützt erfolgen kann. Maßnahmen können voneinander abhängig sein. Wenn zum Beispiel die Vertraulichkeit von Daten per Verschlüsselung sichergestellt werden soll, müssen die verwendeten Schlüssel ebenfalls vertraulich sein. Unter Nutzung der Zuordnungen von Sicherheitsanforderungen zu Maßnahmen und der Abhängigkeiten zwischen Maßnahmen haben wir für die genannten Sicherheitsanforderungsmuster die folgenden Maßnahmen aus der ISO 27001:2013 ausgewählt und instanziiert:
• SR 1: zum Beispiel Sicherheit der Geräte, Zugriffskontrolle, und (entsprechend unserer Abhängigkeiten) Sicherheit bezüglich des Personals
• SR 2: zum Beispiel Kryptografische Signaturen und die notwendigen Maßnahmen
• SR 3: Für SR 3 werden die gleichen Maßnahmen, wie für SR 1 gewählt. Zusätzlich werden sichere Bereiche realisiert.
• SR 4: Die Maßnahmen, die SR 4 adressieren, sind bereits zur Behandlung der anderen Sicherheitsanforderungen ausgewählt.
• SR 5: zum Beispiel Maßnahmen für redundante Systeme

Der Katalog wurde auf Basis der ISO 27001, der Cloud Security Alliance Cloud Controls Matrix (Version 3.0.1 von 2014) und eigenen Erfahrungen erstellt. Es ist möglich, ihn zu ergänzen.

Nachdem die Maßnahmen gewählt worden sind, muss geprüft werden, ob mit den Maßnahmen das Risiko für alle Assets auf ein akzeptables Maß reduziert wurde. Dies geschieht durch eine Wiederholung von Schritt 4.

Schritt 7: Dokumentation erzeugen

Zuletzt wird von unserem Werkzeug eine Dokumentation erzeugt. Folgende im Laufe der Anwendung unserer Methode erzeugten Artefakte gehen in die Erzeugung der Dokumentation ein:
Schritt 1: Instanz des CSAP
Schritt 2: Liste der identifizierten Assets
Schritt 3: Liste der Bedrohungen
Schritt 4: Liste der identifizierten Risiken

Schritt 5: Liste der Sicherheitsanforderungen
Schritt 6: Liste der zu realisierenden Maßnahmen

Alle oben genannten Ergebnisse werden in einem Dokument zusammengefasst. Dieses Dokument kann als Grundlage für eine Zertifizierung des ISMS gemäß ISO 27001 dienen.

ClouDA-Tool

ClouDAT ist ein speziell angepasstes Werkzeug für die Analyse und Dokumentation von Sicherheitsanforderungen und Maßnahmen in Bezug auf Cloud-Computing-Dienste. Im Gegensatz zu den sonst oft üblichen Dokumentationen mit Textverarbeitungssystemen und Zeichenprogrammen, können mit Hilfe des ClouDA-Tools logische Zusammenhänge zwischen den erfassten Informationen dargestellt werden. Damit werden interne Konsistenzprüfungen möglich, die zur Verbesserung der Qualität der Analyse beitragen. Durch die standardisierte Darstellung wird eine Prüfung deutlich vereinfacht. Fehler in der internen Konsistenz der Dokumentation sind der größte Kostenfaktor bei einer Zertifizierung. Daher prüft das Werkzeug die interne Konsistenz der Dokumentation, statt auf eine fehleranfällige Prüfung beim Cloud-Dienstanbieter zu setzen. Weiterhin wird durch die Anwendung der ClouDAT-Methode der Arbeitsfluss während der Risikoanalyse verbessert. So werden bei der Instanziierung der Bedrohungs- und Sicherheitsanforderungsmuster für die Ersetzung der Platzhalter potentiell relevante Informationen auf Grundlage der identifizierten Assets automatisch durch das ClouDA-Tool angeboten. Die werkzeuginterne Abbildung der Beziehungen zwischen Assets, Bedrohungsmustern, Sicherheitsanforderungsmustern und Maßnahmen bewirkt, neben der Beschleunigung des Arbeitsflusses, dass diese nicht übersehen werden können. Wir haben verschiedene Designer-Editoren implementiert. Mit diesen können
- das Cloud-System-Analysemuster
- die Kataloge für Bedrohungsmuster, Sicherheitsanforderungsmuster und Maßnahmen sowie
- die Parameter für die Risikoanalyse

modifiziert und/oder erweitert werden. So wird eine hohe Anpassbarkeit und Wiederverwendbarkeit erreicht.

Unser Werkzeug wurde unter der GNU Public License (GPL) veröffentlicht.

Zusammenfassung

Wir haben eine strukturierte Methode zur Risikoanalyse von Cloud-Anwendungen entsprechend dem ISO 27001-Standard vorgestellt. Unsere Methode basiert auf Mustern, um den Kontext und die Struktur eines Cloud-Computing-Dienstes zu beschreiben (CSAP), Bedrohungen zu identifizieren, Sicherheitsanforderungen auszuwählen, sowie entsprechende Maßnahmen zu ermitteln. Unser Werkzeug unterstützt die Anwendung dieser Methode. Sie hat folgende Vorteile:
- Systematische Identifizierung von Bedrohungen durch entsprechende Bedrohungsmuster (engl. Threat Patterns) und deren Beziehung zu Elementen des CSAP, um die Sicherheit von Cloud-Computing-Diensten zu analysieren. Dies erleichtert und beschleunigt die Bedrohungsanalyse.
- Systematische Identifizierung von Sicherheitsanforderungen durch entsprechende Sicherheitsanforderungsmuster und deren Beziehung zu Bedrohungsmustern.
- Systematische Identifizierung von Maßnahmen durch deren Beziehung zu Sicherheitsanforderungsmustern.
- Zusätzliche Effizienz durch das Anwenden der Methode und die Reduzierung des Aufwandes durch die hierarchische Verfeinerung von Assets.

Wir werden in Zukunft unser Werkzeug um weitere Muster erweitern, um damit eine Risikoanalyse für andere Systeme als Clouds durchführen zu können. Zusätzlich planen wir, das Werkzeug so zu erweitern, dass auch die vollständige und kohärente Instanziierung der Muster überprüft werden kann.

Summary

We present a structured method for performing risk analysis for cloud applications according to the ISO 27001 standard. Our method relies on patterns to describe the context and structure of a cloud computing system (using CSAP), to identify threats, to elicit the security requirements, and to select controls. Our ClouDA tool supports the application of this method. Our approach delivers the following main benefits:
- Systematic pattern-based identification of threats using threat patterns and their relationship to CSAP elements, which facilitates and accelerates the threat analysis
- Systematic pattern-based identification of security requirements to be fulfilled by appropriate controls using security requirement patterns and their relationship to threat patterns
- Systematic pattern-based identification of controls using their relationship to security requirement patterns
- Tool support for our approach
- Increased effectiveness of risk analysis by applying the method and reduced documentation effort by hierarchical refinement of assets.

In the future, we want to extend the tool for supporting other types of patterns for performing risk analysis. In addition, we intend to enrich the tool so as to check the complete and coherent instantiation of the patterns.

Danksagung

Wir danken Kristian Beckers für seine Ideen und die Diskussionen mit ihm. Weiterhin danken wir Thomas Santen für seine Kommentare zu diesem Papier.

Anmerkungen

1) entsprechend der vom US National Institute of Standards and Technology (NIST) gegebenen Definition von Cloud Computing 2009, S. 2
2) Eckpunktepapier - Sicherheitsempfehlungen für Cloud Computing Anbieter 2012, S. 25
3)http://www.cloudat.de
4) Beckers et al., 2011

Literatur

– Alebrahim, A., Faßbender, S., Hatebur, D., Goeke, L. & Côté, I. (2015). A Pattern-Based and Tool-Supported Risk Analysis Method Compliant to ISO 27001 for Cloud Systems. In International Journal of Secure Software Engineering (IJSSE)
– K. Beckers, H. Schmidt, J. C. Kuster and S. Faßbender (2011). Pattern-Based Support for Context Establishment and Asset Identification of the ISO 27000 in the Field of Cloud Computing. In Sixth International Conference on Availability, Reliability and Security, pp. 327-333.
– Beckers, K., Côté, I., Goeke, L. & Güler, S., Heisel, M. (2014). A Structured Method for Security Requirements Elicitation concerning the Cloud Computing Domain. In International Journal of Secure Software Engineering (IJSSE)
– ISO/IEC. (2013). International Standard ISO/ICE 27001 Information technology Security techniques Information security management systems Requirements. Second edition.

*Die Autor*innen*

Maritta Heisel ist Professorin für Software Engineering an der Universität Duisburg-Essen und Vorstandsmitglied von paluno – The Ruhr Institute for Software Technology. Sie studierte Informatik an der Universität Karlsruhe, wo sie auch promovierte. Anschließend habilitierte sie sich an der TU Berlin. Es folgten eine Position als Hochschuldozentin an der Universität Madgeburg sowie eine Professur für Praktische Informatik an der Universität Münster. Seit 2004 ist sie Professorin an der Universität Duisburg-Essen. Ihre Forschungsinteressen liegen auf den Gebieten Informations- und Datensicherheit, Anforderungsanalyse, Spezifikation und Entwicklung sicherheitskritischer Software sowie methodischen Aspekten der Softwareentwicklung. Weiterhin ist sie Mitglied in dem seit 2015 von der DFG geförderten Graduiertenkolleg „User-Centred Social Media“.

Isabelle Côté schloss ihr Studium der Informatik 2004 mit Diplom ab und promovierte 2012 an der Universität Duisburg-Essen. Seit 2012 ist sie bei ITESYS Institut für technische Systeme GmbH mit Sitz in Dortmund angestellt. Sie ist für Industrieprojekte im Bereich Automotiv-Safety verantwortlich. Darüber hinaus arbeitet sie auch an Projekten mit dem Schwerpunkt Informationssicherheit mit. Im Rahmen des Forschungsprojektes „ClouDAT“ beschäftigte sie sich mit Informationssicherheit in Cloud-Computing-Systemen. Ihre Forschungsinteressen liegen in der Safety und Security. In diesen Bereichen hat sie verschiedene Konferenz-, Fachzeitschriften- und Workshopbeiträge verfasst und begutachtet.

Denis Hatebur arbeitet an der Universität Duisburg-Essen als wissenschaftlicher Mitarbeiter. Gleichzeitig ist er seit 2003 Geschäftsführer der ITESYS Institut für technische Systeme GmbH in Dortmund. Er arbeitete in verschiedenen Industrieprojekten als Berater. In diesen Safety- und Securityprojekten war er für den Spezifikationen und Testen verantwortlich. Seine Forschungsinteressen liegen in der Entwicklung sicherer und verlässlicher Systeme unter Berücksichtigung des Anforderungs-Engineerings, der Architekturentwicklung und des Testens. In seinem Bereich hat er verschiedene Konferenz-, Fachzeitschriften- und Workshoppapiere verfasst und begutachtet. Er hat ein Diplom der technischen Informatik der Fachhochschule Dortmund, einen Master of Science im Bereich Computer Engineering der Universität Duisburg-Essen und seit 2012 einen Dr.-Ing. der Universität Duisburg-Essen.

Ludger Goeke studierte Allgemeine Informatik an der Fachhochschule Dortmund und schloss 2007 mit Diplom ab. Er ist seit 2007 Angestellter bei der ITESYS Institut für technische Systeme GmbH mit Sitz in Dortmund. In diesem Zusammenhang war er in verschiedenen Industrieprojekten als Berater tätig. Zu Beginn seiner beruflichen Laufbahn bezogen sich die entsprechenden Projekttätigkeiten auf die Themengebiete Änderungs-, Dokumenten- und Prozessmanagement. Seit geraumer Zeit ist er vorrangig an Projekten mit der Thematik Informationssicherheit beteiligt. Hierbei war er für das Testen und die Quellcodeanalyse in Bezug auf Smartcard-Applikationen verantwortlich. Weiterhin befasste er sich im Rahmen des Forschungsprojektes „ClouDAT“ mit der Sicherstellung der Informationssicherheit von Cloud-Computing-Diensten. Seine Forschungsinteressen liegen im Risikomanagement sowie der Systemanalyse zur Sicherstellung von Informationssicherheit. Im Bereich der Informationssicherheit war er an der Erstellung verschiedener Fachzeitschriften- und Workshoppapiere beteiligt.