Protokoll

Sonderfachgremium Cloud zum Thema „CMDB“ 01.03.2022

Videokonferenz

Sonderfachgremium Cloud am 26.01.2021, 09:30 – 13:30 Uhr per Videokonferenz

Begrüßung
Die Aufsicht stellt die Gäste der heutigen Veranstaltung aus der Versicherungsbranche (Expertengremium IT) vor und erläutert die Unterschiede und Gemeinsamkeiten von Fach- und Expertengremium. Zudem stellen sich die weiteren Teilnehmenden dem Expertengremium kurz vor.

Diskussion des Fokusthemas CMDB im Kontext 8.2 BAIT
Ein Teilnehmer der Cloud-Praxisarbeitsgruppe IT/Ops des IT-Roundtables erläutert das Fokusthema CMDB (Configuration Management Database) und den damit verbundenen Umgang bezogen auf Cloud Service Provider (CSP) bzgl. des IT-Betriebs gemäß 8.2 BAIT. Unter Proportionalitätsgesichtspunkten kann es unterschiedliche Wege geben, die Anforderungen nach einem Bestandsverzeichnis für Komponenten der IT-Systeme sowie deren Beziehungen zueinander zu erfüllen. Eine CMDB bspw. diene der Sicherstellung eines dokumentierten Überblicks über die für die Aufrechterhaltung bzw. Wiederherstellung des Geschäftsprozesses erforderlichen Bausteine / Serviceelemente und deren Konfiguration/Zusammenspiel (CSP/Kunde).

Bei der Public Cloud-Nutzung großer Hyperscaler handele es sich immer um virtuelle Assets, bei welchen der Standort nicht immer bekannt sei und die, sowie die Konfiguration, eine gewisse Dynamik besitzen. Teilweise geschehen Änderungen in Real-Time, daher sei deren Erfassung in einer CMDB des Kunden nicht vollumfänglich möglich. In der Praxis seien die klassischen Sourcing Mechanismen (Beschaffungsmechanismen) im Cloud-Umfeld schwierig anwendbar, daher bestehe das Ziel darin, Best Practices zu identifizieren und daraus Umsetzungskonzepte abzuleiten, zu entwickeln und zu etablieren.Geklärt werden müsse hierfür die operative Verantwortung im Kontext 8.2 BAIT aufseiten des CSP und auf Seiten des Kunden sowie die Schnittstellen inklusive deren Dokumentation.

Anhand einer schematischen Darstellung der übereinander gelagerten Schichten bei verschiedenen Modellen der Cloud-Auslagerung wurde erörtert, wie die Steuerung innerhalb der CMDB unter Berücksichtigung der Abstraktionsschichten bzw. deren -grenzen stattfinden könne. Diese schematische Betrachtung umfasse bspw. sieben Schichten (Rechenzentrum, Netzwerk & Speicherung, Physische Server, Virtualisierung, Betriebssystem, Datenbank, Anwendung) und vier Servicemodelle (on premise, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)). Die Servicemodelle unterschieden sich dadurch, welche der Schichten vom Kunden und welche vom CSP betrieben würden. Gemeinsam betriebene Schichten würden die sogenannte Abstraktionsgrenze bilden. Die Schichten

oberhalb (unterhalb) der Abstraktionsgrenze würden in der Regel ausschließlich vom Kunden (CSP) betrieben. Abstraktionsschichten besäßen verschiedene Ausprägungen, die sich dynamisch ändern könnten. Entscheidend für das Risikomanagement sei das, was der Kunde vom CSP konsumiere und wie er diesen Konsum erfasse. Es sei darauf hingewiesen, dass dies eine schematische Darstellung ist. In der Praxis maßgeblich sei, welche Cloud Services jeweils vom Institut genutzt werden. D.h. es kann sein, dass von einem Institut sowohl IaaS als auch hochfunktionale PaaS oder SaaS genutzt werden.

Es werden verschiedene ausgewählte Fallbeispiele aus der Praxis zu den genannten Servicemodellen diskutiert

Diskussionsergebnisse

Bzgl. des IT-Betriebs wird in den Anforderungen der BAIT gemäß Tz. 8.2 ausgeführt: „Die Komponenten der IT-Systeme und deren Beziehungen zueinander sind in geeigneter Weise zu verwalten, und die hierzu erfassten Bestandsangaben regelmäßig sowie anlassbezogen zu aktualisieren."

Unter Proportionalitätsgesichtspunkten kann es unterschiedliche Wege geben, die Anforderungen nach einem Bestandsverzeichnis für Komponenten der IT-Systeme sowie deren Beziehungen zueinander zu erfüllen. Eine Configuration Management Database (CMDB) des IT-Betriebs dient der Sicherstellung eines dokumentierten Überblicks über die für die Aufrechterhaltung bzw. Wiederherstellung der Geschäftsprozesse des Instituts erforderlichen Elemente und deren Konfiguration sowie Zusammenspiel.

Ziel ist, ein gemeinsames Verständnis zwischen Instituten und der Aufsicht zu den folgenden Punkten zu entwickeln:
- Erfassung von Elementen und Konfigurationsdaten auf Seiten des CSP und des Kunden
- Verantwortung für die Schnittstellen inklusive deren Dokumentation auf Seiten des CSP und des Kunden.

Es besteht Einvernehmen, dass für die weitere Diskussion eine Abstraktion mittels einer schematischen Betrachtung der Cloud-Dienste (vgl. Merkblatt – Orientierungshilfe zu Auslagerungen an Cloud-Anbieter) bspw. auf Basis von sieben Schichten (von unten nach oben: Rechenzentrum, Netzwerk & Speicherung, Physische Server, Virtualisierung, Betriebssystem, Datenbank, Anwendung) zielführend ist. Zudem erscheint eine grundsätzliche Unterscheidung nach Service- und Bereitstellungsmodellen sinnvoll (bspw. on premise, Infrastructure as a Service, Platform as a Service, Software as a Service).

Die Servicemodelle unterscheiden sich dadurch, welche Schichten für den jeweiligen Service vom Institut und welche vom CSP betrieben werden. Die beim CSP eingekauften Services bilden die Abstraktionsgrenze im jeweiligen Servicemodell und sind in der Regel das einzige Element, das in das Konfigurationsmanagement des Instituts aufgenommen wird. Die Schichten oberhalb (unterhalb) der Abstraktionsgrenze werden in der Regel ausschließlich vom Institut (CSP) betrieben.

Es besteht über folgende Prinzipien Einvernehmen:

1. Oberhalb der Abstraktionsgrenze betreibt das Institut die Schichten. Die Einbindung der Services/Assets/Prozesse erfolgt vollständig in die IT Betriebsfunktionen des Instituts. Oberhalb der Abstraktionsgrenze ist also insbesondere eine vollständige Abbildung und komplette Dokumentation innerhalb der CMDB des Instituts möglich und notwendig.

2. Unterhalb der Abstraktionsgrenze betreibt der CSP die Schichten. Es erfolgt in der Regel keine Aufnahme von Komponenten des CSP in die CMDB des Instituts.

3. An der Abstraktionsgrenze (dies ist der jeweilige vom Institut genutzte Cloud Service) erfolgt eine Aufnahme in die CMDB des Instituts: In die CMDB werden hierbei sowohl die durch das nutzende Institut vorzunehmende Parametrisierungen der Services als auch die Servicebeschreibungen des CSP aufgenommen. Für die Servicebeschreibungen werden entsprechende regelmäßige Aktualisierungen auf Basis von Vereinbarungen zwischen Institut und CSP vorgenommen (entsprechend der Weiterentwicklung der Nutzung von Services nach Art und Umfang).

Das heißt also insbesondere, dass an und unter der Abstraktionsgrenze in Vereinbarungen zwischen dem Institut und dem CSP geregelt werden muss, welche Daten in der CMDB des Instituts erfasst werden. Oberhalb der Abstraktionsgrenze liegt ein normaler Prozess des Unternehmens vor, unterhalb dieser Grenze ist es der Prozess des CSP und an der Grenze gilt es, ggf. neue Prozesse zu vereinbaren und aufzusetzen. Eine Maßnahme hierfür kann sein, dass ein Institut eine Schnittstelle zur CMDB des CSP hat, um hierfür notwendige Informationen (z. B. über den tatsächlichen Standort von Daten oder erfolgte Zugriffe auf ihre Daten durch den CSP) abrufen zu können.

Bzgl. der Abstraktionsgrenze weist die Aufsicht darauf hin, dass Institute ggf. näher untersuchen müssen, ob das Bestimmen der Abstraktionsgrenze je nach Nutzungsmodell ausreichend sei oder individueller erfolgen müsse, und dass das genaue Setzen der Abstraktionsgrenze pauschal nicht darstellbar sei.

Verabschiedung

Es folgt ein Ausblick auf das nächste Sonderfachgremium am 03.05.2022.

Teilnehmer*innen Sonderfachgremium Cloud zum Thema „CMDB“ 01.03.2022

André Nash	Bundesverband Deutscher Banken
Andreas Fichelscher	KfW
Andreas Kastl	VAB
Berit Schimm	BVR
Brigitte Penther	HCOB
Christian Saller	Bayern LB
Christian Weltermann	Commerzbank
Daniel Wagenknecht	KPMG
Frank Hoenes	LBBW
Frank Trojahn	DSGV
Gabriele Sieck	GDV
Heiko Michelsen	ING
Heiko Pälecke	BB-MBG
Heino Gärtner	Nord LB
Holger Muster	Finanz Informatik
Ingo Huber	Wüstenrot & Württembergische AG
Jörg Passmann	RWE
Karin Zimmermann	Bausparkasse Mainz AG
Marcus Scheidl	VÖB
Martin Steuber	UniCredit
Michael Burckhardt	Commerzbank
Michael Somma	BFACH
Oliver Koen	Atruvia
Oliver Semmler	Börse Stuttgart GmbH
Philipp Schwaab	Helaba
Ralf Jurk	HUK-Coburg
Simone Heuser	IKB
Stefan Böse	DZ Bank
Sven Lausus	DEVK
Uwe Gropengiesser	Deutsche Bank

Ira Kosche-Steinbrecher	Bundesanstalt für Finanzdienstleistungsaufsicht
Jan Kiefer	Bundesanstalt für Finanzdienstleistungsaufsicht
Dr. Frank Beekmann	Bundesanstalt für Finanzdienstleistungsaufsicht
Mark Rebmann	Bundesanstalt für Finanzdienstleistungsaufsicht
Sophia Merker	Bundesanstalt für Finanzdienstleistungsaufsicht
Dr. Michael Paust	Deutsche Bundesbank
Andreas Vogel	Deutsche Bundesbank
Anke Habicht	Deutsche Bundesbank
Anna-Maria Philipp	Deutsche Bundesbank
Daniel Wittmann	Deutsche Bundesbank
Jörg Bretz	Deutsche Bundesbank
Rainer Englisch	Deutsche Bundesbank
Dr. Rainer Janlewing	Deutsche Bundesbank