Protokoll

Sonderfachgremium IT zum Thema „Cloud/IT-Betrieb“
13.12.2022, 10:00 – 12:00 Uhr,
31.05.2023, 10:00 – 12:00 Uhr

per Videokonferenz

Präambel

Im vorliegenden Protokoll werden die maßgeblichen Diskussionsaspekte sowie –ergebnisse aus zwei Terminen des Sonderfachgremiums IT zum Thema „Cloud/IT-Betrieb“ zusammengefasst. Im Nachfolgenden werden die Prozesse und Verfahren betrachtet, welche üblicherweise den IT-Betriebseinheiten zugeordnet sind und in Kapitel 8 der BAIT / VAIT behandelt werden.

Unter den Teilnehmenden des Sonderfachgremiums herrscht Konsens darüber, dass zukünftige Erfahrungen aus der Praxis oder sich ändernde regulatorische Rahmenbedingungen (bspw. DORA) möglicherweise eine Anpassung der Diskussionsergebnisse erfordern. Schon insbesondere deshalb handelt es sich bei den Diskussionsergebnissen nicht um einen abgeschlossenen Implementierungsleitfaden für beaufsichtigte Unternehmen. Vielmehr soll ein Orientierungsrahmen geschaffen werden, dessen Elemente von den beaufsichtigten Unternehmen mit den Cloud-Anbietern ausgestaltet und konkretisiert, vereinbart, implementiert sowie regelmäßig evaluiert werden müssen.

Aufsichtsrechtliche Anforderungen an den IT-Betrieb

Die aufsichtsrechtlichen Anforderungen an den IT Betrieb leiten sich bei Banken vor allem aus den EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken, (insb. Abschnitt 3.3) sowie den Leitlinien zu Auslagerungen, den MaRisk (insb. AT 7.2 Tz. 1 - 5) und den BAIT (insb. Kapitel 8 i. V. m. Kapitel 2) ab. Für die Versicherungswirtschaft leiten sich die Anforderungen aus den EIOPA Leitlinien zum Outsourcing an Cloud-Anbieter sowie den Leitlinien zu Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie, den Mindestanforderungen an die Geschäftsorganisation von Versicherungsunternehmen (MaGo, MaGo für EbAV, MaGo für kleine VU) sowie den VAIT ab.

Es wird nachfolgend – entlang insbesondere der BAIT/VAIT – auf folgende Prozesse fokussiert:

- Prozess zum Management von Veränderungen (8.4 und 8.5 BAIT / VAIT),
- Störungs- und Problembehandlung (8.6 BAIT / VAIT),
- Datensicherungskonzepte (8.7 BAIT / VAIT),

- Lebenszyklus-Management der IT Komponenten (8.3 BAIT / VAIT) sowie
- Kapazitätsmanagement (8.8 BAIT / VAIT).

Problemstellung der beaufsichtigten Unternehmen

Auch im Bereich des IT-Betriebs besteht eine wichtige Herausforderung darin, dass die Erbringung der Cloud-Services durch den Cloud-Anbieter durch eine Abstraktionsgrenze[1] gekennzeichnet ist. Die Abstraktionsgrenze verläuft differenziert nach dem konkret eingesetzten Cloud-Service in Abhängigkeit des beauftragten Service Modells (bspw. SaaS, PaaS, IaaS) und der Art der Nutzung durch das beaufsichtigte Unternehmen. Die Abstraktionsgrenze stellt somit die Grenze der Zuständigkeit zwischen beaufsichtigten Unternehmen und dem Cloud-Anbieter dar. Bezogen auf den IT-Betrieb sind – entsprechend dieser Zuständigkeitsverteilung – unterhalb der Abstraktionsgrenze grundsätzlich die Prozesse und Verfahren des Cloud-Anbieters relevant, oberhalb der Abstraktionsgrenze die Prozesse und Verfahren des jeweiligen beaufsichtigten Unternehmens.

Um einen sicheren und stabilen IT-Betrieb sowie eine angemessene Erkennung und Steuerung von IT-Risiken zu gewährleisten, muss die Schnittstelle zwischen Cloud-Anbieter und beaufsichtigtem Unternehmen über die Abstraktionsgrenze hinweg angemessen ausgestaltet sein. Folgende Cloud-spezifische Herausforderungen stellen sich hierbei insbesondere:

- Eingeschränkte Detailinformationen zur konkreten Ausgestaltung der Cloud-Services, z. B. bezogen auf Architektur oder konkret genutzte IT-Komponenten.
- Üblicherweise keine Bereitstellung von kundenspezifischen Berichtsdokumenten durch den Dienstleister, stattdessen selbstständige Informationsbeschaffung durch das beaufsichtigte Unternehmen im Hol-Prinzip über zu konfigurierende Dashboards / Informations-Plattformen, teilweise mit beschränkter Datengrundlage, bspw. bei der Anzeige von plattformweiten Ausfällen oder Service-Einschränkungen über Availability-Dashboards.
- Üblicherweise kein Einfluss auf die interne Prozessgestaltung des Cloud-Anbieters im IT-Betrieb.
- Das Serviceportfolio eines Cloud-Anbieters ist meist global ausgerichtet – dies kann bedingen, dass nicht alle Services in allen Regionen verfügbar sind.

Die Verantwortung für die Cloud Auslagerung verbleibt aber, ungeachtet der Zuständigkeitsverteilung, beim beaufsichtigten Unternehmen. Es stellen sich somit insbesondere die Fragen (i) ob die IT-Betriebsprozesse beim Cloud-Anbieter den aufsichtlichen und eigenen Anforderungen genügen und (ii) wie die angemessene Verknüpfung zwischen den beiden Zuständigkeitssphären durch das beaufsichtigte Unternehmen sichergestellt werden kann.

Diskussionsergebnisse

[1] Siehe Protokoll des Sonderfachgremium Cloud zum Thema „CMDB“: https://www.bafin.de/SharedDocs/Downloads/DE/Protokoll/dl_01032022_Protokoll_Sonderfachgremium_IT.pdf

Die Angemessenheit der IT-Betriebsprozesse der Cloud-Anbieter ist im Zusammenhang mit dem Service- und Providermanagement durch das beaufsichtigte Unternehmen zu beurteilen. Üblicherweise bieten Cloud-Anbieter als Qualitätszusage für die bereitgestellten Services ein Service Level Agreement (SLA) an, in dem die Dienstleistungsgüte beschrieben und vertraglich zugesichert wird. In diesem Zusammenhang wurden in den vergangenen Sonderfachgremien, insbesondere im Sonderfachgremium Cloud zum Thema „Zertifikate" am 07.10.2021[2], Lösungsansätze erarbeitet, die auch im Kontext des IT-Betriebs anwendbar sind.

Bei der Nutzung der Cloud werden Informationen für den Kunden zumeist nicht vom Dienstleister individuell aufbereitet und übersendet. In der Regel kommt es zu einer Informationsbereitstellung vom Cloud-Anbieter, die das beaufsichtigte Unternehmen gezielt abrufen muss („Hol-Prinzip"). Anstatt einer direkten Kommunikation des Cloud-Anbieters über relevante Änderungen in den Services, bspw. über Vorfälle oder Veränderungen an den Leistungsbeschreibungen, erfolgt eine mandantenneutrale Kommunikation auf der Plattform des Cloud-Anbieters. Dadurch bedarf es zusätzlicher oder angepasster IT-Betriebsprozesse auf Seiten des beaufsichtigten Unternehmens. Daher ist bezogen auf die Verknüpfung zwischen den Zuständigkeitssphären eine angemessene Einbettung in die IT-Betriebsprozesse des beaufsichtigten Unternehmens durch einen ausreichenden Informationstransfer und die geeignete Konfiguration der Cloud-Services erforderlich. Insbesondere geht es um:

- ein ausreichendes Verständnis der eingesetzten Cloud-Services, inklusive der relevanten unterliegenden Verfahrensweisen, IT-Systeme, IT-Komponenten und Schnittstellen des Cloud-Anbieters,
- selbstständige Beschaffung von Informationen / Daten des Cloud-Anbieters, um dem beaufsichtigten Unternehmen die Durchführung der IT-Betriebsprozesse im eigenen Zuständigkeitsbereich („oberhalb der Abstraktionsgrenze") zu ermöglichen, und
- Umsetzung einer geeigneten Konfiguration der Cloud-Services bezogen auf die konkrete Cloud-Nutzung durch das beaufsichtigte Unternehmen.

Grundsätzlich muss das beaufsichtigte Unternehmen ermitteln, welche Information für den Betrieb der Services relevant sind, welche dieser Informationen durch den Cloud-Anbieter bereitgestellt werden, welche Restrisiken durch fehlende Transparenz entstehen und welche Möglichkeiten der Mitigation bzw. Risikobehandlungsstrategien zu implementieren sind. Die nachfolgenden Punkte sind als mögliche Lösungsskizzen zu verstehen und bilden keinen allgemeingültigen Implementierungsleitfaden.

Beschreibung und Überwachung der Dienstleistungsgüte

1. Vertragliche Regelungen bilden die Basis zur Steuerung durch die beaufsichtigten Unternehmen. Für die genutzten Services ist eine Beschreibung der Dienstleistungsgüte seitens des Cloud-Anbieters erforderlich.[3]

[2] Siehe Protokoll des Sonderfachgremium Cloud zum Thema „Zertifikate": https://www.bafin.de/SharedDocs/Downloads/DE/Protokoll/dl_07102021_Protokoll_Sonderfachgremium.pdf?__blob=publicationFile&v=1

[3] Gemäß MaRisk müssen Banken in dem in Textform vereinbarten Auslagerungsvertrag u.a. die vom Cloud-Anbieter zu erbringende Leistung spezifiziert und ggf. abgegrenzt werden, und es muss die Dienstleistungsgüte

2. Zur angemessenen Steuerung der Services hat das beaufsichtigte Unternehmen einen Abgleich seiner eigenen Vorgaben mit der vertraglich zugesicherten Dienstleistungsgüte durchzuführen. Für die Abweichungen von den Vorgaben muss das beaufsichtigte Unternehmen eine Risikoanalyse durchführen und prüfen, ob die Services vor diesem Hintergrund mit den vom Cloud-Anbieter angebotenen Beschreibungen der Dienstleistungsgüte (z.B. SLAs) für die spezifischen Anwendungen verwendet werden können. Dabei kann das beaufsichtigte Unternehmen zur Verbesserung der Bewertung der Services zusätzliche Information, z.B. im Dialog mit dem Cloud-Anbieter, zur Hilfe nehmen.

Risikomanagement

3. In Abhängigkeit des Risikogehalts des IT-Systems muss im Vorfeld der Nutzung des Cloud-Services eine Analyse der inhärenten Risiken der vom Cloud-Anbieter bereitgestellten Services erfolgen, wobei ein Einsatz nur dann statthaft ist, wenn die resultierenden Risiken tragbar sind. Die Risikoanalyse ist regelmäßig zu validieren.
4. Entsprechend des Risikogehaltes des ausgelagerten Sachverhalts sowie der genutzten Services ist der Aufbau eines Service- und Providermanagements zur Steuerung des Cloud-Anbieters auszugestalten, mindestens durch die Durchführung von Regelterminen zwischen beaufsichtigtem Unternehmen und Cloud-Anbieter über verschiedene organisatorische Ebenen zur Informationsbeschaffung der genutzten Services.

Informationsbeschaffung und -verarbeitung

5. Informationen zum Lebenszyklus (Veränderungen oder Abschaltung) zu genutzten Services werden mit der eigenen Planung abgeglichen, um rechtzeitig auf Veränderungen reagieren zu können.
6. Um die vom Cloud-Anbieter bereitgestellten Informationen verarbeiten zu können, muss sich das beaufsichtigte Unternehmen einen Überblick vom Informationsangebot und der genutzten Kommunikationskanäle verschaffen. Dazu gehört eine Erfassung der für die Steuerung der Services relevanten Informationen und der dazugehörigen Kommunikationskanäle, über die der Cloud-Anbieter, z.B. bei Änderungen an seinen Services, informiert. Abhängig von der Relevanz und Änderungshäufigkeit können verschiedene Ansätze zur Umsetzung des Hol-Prinzips verwendet werden:
    a. Bei kurzfristig relevanten Informationen, bspw. Incident-Dashboard des Hyperscalers, wird durch Prozesse und Anwendungen des IT-Betriebs sichergestellt, dass Informationen zeitnah bewertet und verarbeitet werden (bspw. E-Mail-Notification und Bewertung im Falle einer im Availability-Dashboard angezeigten Service-Einschränkung). Eine Integration eines entsprechenden Überwachungsprozesses in die Prozesse des beaufsichtigten Unternehmens ist mit den von Cloud-Anbietern bereitgestellten Dashboards, z.B. Definition und Aufsetzen von Triggern, Alarmen etc. erforderlich.

---

mit eindeutig festgelegten Leistungszielen vereinbart werden (AT 9 Tz. 7 MaRisk). Ab dem 17. Januar 2025 gilt die DORA Verordnung (Artikel 64 DORA). Gemäß Artikel 30 (2) lit e, (3) lit a DORA umfassen die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen u.a. die Beschreibungen der Dienstleistungsgüte.

b. Bei mittel- bis langfristig relevanten Informationen, bspw. Änderungen in den Service Terms oder APIs, müssen durch regelmäßige Überprüfung und Bewertung angekündigter Änderungen eventuelle Auswirkungen auf die verwendeten Services und entsprechende Maßnahmen abgeleitet werden.[4]

Anpassung der Konfiguration von Cloud-Services

7. Empfehlungen des Cloud-Anbieters (z.B. Sizing) sollten regelmäßig geprüft und die allokierten Services entsprechend eigener Vorgaben, unter Berücksichtigung der Empfehlungen der Cloud-Anbieter, angepasst werden.
8. Anforderungen an den Ort der Datensicherungen orientieren sich an den von Cloud-Anbietern vorgesehenen Konzepten zu Regionen und Zonen. Grundsätzlich obliegt es dabei dem beaufsichtigten Unternehmen, sofern es Datensicherungsservices des Cloud-Anbieters nutzt, die erfolgreiche Umsetzung von Datensicherungsaufträgen z.B. durch Log-Analysen oder Dashboards kontinuierlich zu überwachen und regelmäßig zu testen.
9. Das beaufsichtigte Unternehmen kann Aspekte der Kapazitätsplanung in der entsprechenden Servicebeauftragung beim Cloud-Anbieter konfigurieren, sofern dies die Service-Konfiguration ermöglicht.

[4] Ab dem 17. Januar 2025 gilt die DORA Verordnung (Artikel 64 DORA). Gemäß Artikel 30 (2) lit e, (3) lit a DORA umfassen die vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen u.a. die Beschreibungen der Dienstleistungsgüte.

Teilnehmerinnen und Teilnehmer am 31.05.2023

Bacher, David	BayernLB
Baumann, Ina	ARAG Versicherungen
Behrends, Tino	Genossenschaftsverband – Verband der Regionen
Böse, Stefan	DZ BANK
Gärtner, Heino	NordLB
Heuser, Simone	IKB – Deutsche Industriebank
Jäger, Bernd	LBBW
Kastl, Andreas	Verband der Auslandsbanken in Deutschland
Michelsen, Heiko	ING-DiBa
Müller, Dr. Thilo	dwpbank
Muster, Holger	Finanz Informatik
Paßmann, Joerg	Decadia
Pfisterer, Melina	Helaba
Runkel, Dirk	BKM – Bausparkasse Mainz
Saam, Mirko	R+V Allgemeine Versicherung
Schimm, Berit	Bundesverband VR Banken
Schneider, Ralf	Allianz Deutschland
Sieck, Gabriele	GDV
Somma, Michael	Bankenfachverband
Steuber, Martin	UniCredit Bank
Tieves, Arne	HCOB
Trojahn, Frank	DSGV

Paust, Dr. Michael	Deutsche Bundesbank
Schnack, Bjarne	Deutsche Bundesbank
Vogel, Andreas	Deutsche Bundesbank
Wittmann, Daniel	Deutsche Bundesbank
Heuer, Heiko	Bundesanstalt für Finanzdienstleistungsaufsicht
Kleinknecht-Dennart, Dr. Sven	Bundesanstalt für Finanzdienstleistungsaufsicht
Kosche-Steinbrecher, Ira	Bundesanstalt für Finanzdienstleistungsaufsicht
Rebmann, Mark	Bundesanstalt für Finanzdienstleistungsaufsicht