Protokoll

Sonderfachgremium IT zum Thema „Cloud/Ausstieg“
27.11.2023

per Videokonferenz

Präambel

Im vorliegenden Protokoll werden die maßgeblichen Diskussionsaspekte sowie -ergebnisse aus dem Termin des Sonderfachgremiums IT zum Thema „Cloud/Ausstieg“ zusammengefasst. Im Nachfolgenden werden die Prozesse und Verfahren betrachtet, welche den Ausstieg aus wesentlichen Auslagerungen von IT-Aktivitäten an Cloud-Anbieter sicherstellen sollen.

Unter den Teilnehmenden des Sonderfachgremiums herrscht Konsens darüber, dass zukünftige Erfahrungen aus der Praxis oder sich ändernde regulatorische Rahmenbedingungen (bspw. DORA und der damit verbundenen Delegierten Verordnungen) möglicherweise Auswirkungen auf die Diskussionsergebnisse haben. Bei diesem Protokoll handelt es sich nicht um einen Implementierungsleitfaden. Vielmehr soll damit, als Ergebnis der Diskussionen im Sonderfachgremium IT zu diesem Thema, ein Orientierungsrahmen geschaffen werden, dessen Elemente von den beaufsichtigten Unternehmen mit den Cloud-Anbietern ausgestaltet und vereinbart werden müssen.

Aufsichtsrechtliche Anforderungen

Die aufsichtsrechtlichen Anforderungen an den Ausstieg bei wesentlichen IT-Auslagerungen leiten sich bei Banken vor allem aus den EBA-Leitlinien zu Auslagerungen (insb. Kapitel 15) und den MaRisk (insb. AT 9 Tz. 6) ab. Für die Versicherungswirtschaft leiten sich die Anforderungen aus den EIOPA Leitlinien zum Outsourcing an Cloud-Anbieter (insb. Leitlinie 15) und der MaGo (insb. Tz. 288) ab.

Ab dem 17. Januar 2025 gilt die DORA Verordnung (Artikel 64 DORA). Gemäß Artikel 28 (8) und 30 i. V. m. den einschlägigen Delegierten Verordnungen sind für IKT-Dienstleistungen, die kritische oder wichtige Funktionen unterstützen, Ausstiegs-Strategien und -Pläne einzurichten.

Die folgenden Ausführungen beziehen sich auf die **unbeabsichtigte oder unerwartete Beendigung von Auslagerungen**, die mit einer erheblichen Beeinträchtigung der Geschäftstätigkeit verbunden sein können, nicht aber mit einer geplanten oder beabsichtigten Beendigung einer Auslagerungsvereinbarung.

Problemstellung der beaufsichtigten Unternehmen

Bei der Erstellung von Ausstiegs-Strategien und -Plänen sowie deren Tests, schildern beaufsichtigte Unternehmen vielfach große Herausforderungen.

Ein Ausstieg ist typischerweise durch folgende **allgemeine Charakteristika** geprägt:

- Die Durchführung eines umfassenden Ausstiegs erfordert eine große Anzahl von parallelen, sich teilweise bedingenden Aktivitäten, die in der Regel unter großem Zeitdruck durchgeführt werden müssen.
- Die Migration von Anwendungen kann umfangreiche Anpassungen an Anwendungen, der Infrastruktur und ggf. der Prozesslandschaft zur Folge haben, die häufig sehr zeitaufwändig sind.
- Ein Austausch einzelner Komponenten kann komplexe, zuweilen schwer zu durchschauende Auswirkungen auf andere Anwendungen und (geschäftskritische) Prozesse haben.
- Häufig erfordert ein Ausstieg innerhalb kurzer Zeit zusätzliche Ressourcen, die im Tagesgeschäft nicht in ausreichendem Maße im beaufsichtigten Unternehmen vorgehalten werden.

Bei Auslagerung an Cloud-Anbieter beschreiben die Unternehmen weitere **spezifische Charakteristika,** die hinzukommen. Diese leiten sich aus den Kerneigenschaften und Besonderheiten der Cloud-Anbieter ab, die insbesondere bei Hyperscalern beobachtet werden können:

- Das Geschäftsmodell großer Cloud-Anbieter ist von einer **hohen Standardisierung** der Leistungsangebote und der Leistungserbringung geprägt. Eine Einflussnahme durch einzelne beaufsichtigte Unternehmen, z. B. durch individuelle Vereinbarungen zu spezifischen Cloud-Dienstleistungen, sind zumeist nicht oder nur sehr eingeschränkt möglich. Davon sind auch Vereinbarungen betroffen, die die Durchführung eines Ausstiegs mit Unterstützungsleistungen („Post-Termination Assistance“) des Cloud-Anbieters erleichtern können.
- Das Serviceangebot wird seitens der Cloud-Anbieter mit einer **hohen Änderungsfrequenz** flexibel und kurzfristig angepasst. Gründe sind die hohe Innovationsgeschwindigkeit, die stetige Weiterentwicklung von Cloud-Dienstleistungen, die betriebliche Notwendigkeit global standardisierte Dienstleistungen anzubieten und die Ausrichtung an der Nachfrage der Kunden. Dies erfolgt oft mit eher kurzen Vorlauffristen, insbesondere im Vergleich zu traditionellen IT-Dienstleistern. Hinzu kommt, dass Cloud-Dienstleistungen häufig für Anwendungsfälle mit einer typischerweise hohen Veränderungsgeschwindigkeit im beaufsichtigten Unternehmen eingesetzt werden. In einem solchen Umfeld wird die einmalige Erstellung eines Ausstiegs-Konzeptes (z. B. zu Beginn eines Vertragsverhältnisses) nicht ausreichen, da sie nach kurzer Zeit nicht mehr die tatsächliche Nutzung der Cloud abbildet.

- Cloud-Dienstleistungen sind häufig proprietäre Eigenentwicklungen des Cloud-Anbieters mit einer Vielzahl von Funktionalitäten, die teilweise Alleinstellungsmerkmale beinhalten. Durch die hohe Geschwindigkeit der Weiterentwicklung erfolgt eine Bereitstellung für die Kunden oft noch bevor sich Standards für diese Cloud-Dienstleistungen herausbilden. Die daraus resultierende **mangelnde Interoperabilität** erschwert den Ausstieg. So bieten Cloud-Anbieter für viele Cloud-Dienstleistungen lediglich Mechanismen zum Export von Daten an, nicht aber den Transfer von Konfigurationen und Metadaten in andere Zielsysteme oder zu Cloud-Diensten Dritter. Ein Ausstieg bedeutet in solchen Fällen zumeist die Migration der Anwendung.
- Cloud-Dienstleistungen können nur genutzt werden, wenn der Cloud-Anbieter die Dienstleistung aktiv zur Verfügung stellt – es gibt **keine Weiternutzung ohne Unterstützung des Anbieters**. Bei traditionellen Auslagerungen kann eine Anwendung, deren Nutzung beendet werden soll, auch ohne Unterstützung des Anbieters noch für eine gewisse Zeit weiterbetrieben werden, bis z. B. die notwendige Migration abgeschlossen ist.
- Hinzu kommen deutliche **Konzentrationsrisiken**. Aufgrund der geringen Anzahl von Cloud-Anbietern mit einem innovativen und umfassenden Dienstleistungsangebot besitzen diese eine außerordentliche Marktmacht. Daher sind auch mögliche Migrationsziele eingeschränkt. Zudem wird der Public Cloud Markt auf absehbare Zeit von US-amerikanischen Cloud-Anbietern dominiert, wodurch eine geographische Ballung entsteht.
- Erschwerend kommt hinzu, dass bei jedem Ausstieg beaufsichtigte Unternehmen auf Unterstützung des abgebenden bzw. aufnehmenden Cloud-Anbieters angewiesen sind. Sollte eine Vielzahl von Unternehmen gleichzeitig einen Ausstieg vollziehen, würde eine hohe Nachfrage auf ein **begrenztes Angebot an Ressourcen** auf Seiten der Cloud-Anbieter treffen. Ähnliches gilt für die Verfügbarkeit von anderen unterstützenden Dienstleistern.

Diskussionsergebnisse

Für den Fall einer unbeabsichtigten oder unerwarteten Beendigung einer wesentlichen Auslagerung ist zu analysieren, ob diese mit einer erheblichen Beeinträchtigung der Geschäftstätigkeit verbunden ist. Im Rahmen der Prüfung und Festlegung etwaiger Handlungsoptionen sind entsprechende Ausstiegsprozesse festzulegen, die durch entsprechende Ausstiegs-Strategien und –Pläne operationalisiert werden.

Bei der Ausgestaltung von Ausstiegs-Strategien und -Plänen sind die unternehmensspezifische Nutzung der Cloud, Umfang und Komplexität der betroffenen Aktivitäten und Prozesse, sowie die Ergebnisse der individuellen Risikoanalyse(n) zu berücksichtigen.

Die Planung eines Ausstiegs beruht auf Szenarien, welche die Umstände einer unbeabsichtigten oder unerwarteten Beendigung von Auslagerungen beschreiben. Auf dieser Basis entwi-

ckelt das beaufsichtigte Unternehmen eine oder mehrere Ausstiegs-Strategie(n), die geeignete Handlungsalternativen und Vorgehensweisen für den Ausstieg aus dem Dienstleistungsbezug unter Einhaltung der regulatorischen Anforderungen beschreiben. Auf Grundlage der Ausstiegs-Strategie(n) werden detaillierte Ausstiegs-Pläne entwickelt, die den konkreten Ausstiegsprozess spezifizieren. Die Ausstiegs-Pläne sollen zudem festlegen, unter welchen Bedingungen diese ausgelöst werden. Dazu gehört die Etablierung von Indikatoren zur Überwachung der Cloud-Dienstleistung, des Cloud-Anbieters und der Dienstleistungsgüte.
Wie im letzten Absatz beschrieben, werden Ausstiegs-Strategien und Ausstiegs-Pläne regelmäßig und anlassbezogen überprüft; Ausstiegs-Pläne werden regelmäßig und anlassbezogen getestet.

Beaufsichtigte Unternehmen sollen zur Planung eines Ausstiegs plausible Szenarien heranziehen, die auf angemessenen Annahmen beruhen und diese dokumentieren. Neben den **Risiken**, die sich aus dem **Ausstieg** ergeben können, bestimmt der **Zeithorizont des Ausstiegs** in besonderem Maße die zu ergreifenden Maßnahmen. Ermittelt werden die Zeiträume für die Umsetzung eines Ausstiegs (i) auf Basis der absehbar mindestens benötigten Zeiträume für den Ausstieg und (ii) durch die vertraglich vereinbarten Fristen für eine Kündigung durch den Cloud-Anbieter.

Eine Determinante der Ausstiegs-Strategie(n) und -Pläne ist der Umfang der Cloud-Nutzung für wesentliche Aktivitäten und Prozesse. Je geringer der Umfang, desto leichter, je größer der Umfang desto anspruchsvoller und aufwendiger ist ein Ausstieg typischerweise. Vor diesem Hintergrund dürfte es häufig das Ziel beaufsichtigter Unternehmen sein, Vertragsgestaltung, Architektur und Betrieb so zu beeinflussen, dass bei einem möglichst umfassenden Einsatz der Cloud ein Ausstieg weiterhin möglich bleibt. Durch die Nutzung migrationsfreundlicher Technologien und Cloud-Dienstleistungen, Vorhalten von Ressourcen und Fähigkeiten sowie durch vorbereitende Maßnahmen kann das beaufsichtigte Unternehmen einen **Ausstieg durch interne Maßnahmen vereinfachen** und die Umsetzung von Ausstiegs-Plänen beschleunigen. Ein beaufsichtigtes Unternehmen kann aber auch durch die **Beschränkung der eigenen Cloud-Nutzung**, z. B. durch Ausschluss bestimmter Anwendungen, Geschäftsprozesse oder Daten, die Abhängigkeit des Instituts vom Dienstleister verringern und somit die Komplexität eines Ausstiegs begrenzen.

Mögliche Maßnahmen in der Ausstiegs-Planung sollten den gesamten Auslagerungs-Lebenszyklus der Cloud-Nutzung berücksichtigen, also Aktivitäten vor Vertragsabschluss (z. B. Festlegung möglicher Beschränkungen der Auslagerbarkeit in die Cloud), bei der Vertragsgestaltung (z. B. Kündigungsfristen, Garantien zur Migrationsunterstützung auch über das Vertragsende hinaus, Abschluss von Verträgen mit alternativen Anbietern), bei der technischen Umsetzung (z. B. Auswahl migrationsfreundlicher Technologien, Architekturentscheidungen, Identifikation von Alternativlösungen, Ort der Datenspeicherung) und beim Betrieb (z. B. Tooling zur Unterstützung von hybriden Cloud/non-Cloud Umgebungen oder Multi-Cloud-Ansätzen, Vorhalten von on-premises Kapazitäten).

Die zu treffenden Maßnahmen müssen, unter Berücksichtigung der Verhältnismäßigkeit, geeignet sein, die Ziele der Ausstiegs-Strategie zu erfüllen, dazu gehören mindestens die Vermeidung von Unterbrechungen der Geschäftstätigkeit, von Einschränkungen bei der Einhaltung

regulatorischer Anforderungen sowie die Beeinträchtigung der Kontinuität und Qualität der für Kunden erbrachten Dienstleistungen.

Die regelmäßig und anlassbezogen durchzuführenden Überprüfungen der Ausstiegs-Strategien und -Pläne sollen insbesondere die getroffenen Annahmen hinterfragen und Anpassungen auf der Basis neuer Erkenntnisse umsetzen. Veränderungen des Risikos, die sich durch den Ausstieg ergeben können sind im Rahmen des Risikomanagements zu analysieren und zu dokumentieren. Maßnahmen zur Risikoreduktion, etwa durch die Beschränkung der Nutzung oder durch Aktivitäten zur Vereinfachung des Ausstiegs, können ggfs. das gestiegene Risiko ausgleichen.

Beim regelmäßigen Test der Ausstiegs-Pläne soll überprüft werden, dass die Ziele der Ausstiegs-Strategie bei der Umsetzung des Ausstiegs-Plans erfüllt werden und die beteiligten Personen und Funktionen in der Lage sind den Plan umzusetzen. Zudem sollen mögliche Änderungsbedarfe identifiziert werden. Test von Ausstiegs-Plänen können mit einer Reihe von Testmethoden durchgeführt werden, die geeignet sein sollen, die Angemessenheit und Wirksamkeit des Ausstiegs-Plans nachzuweisen. Insbesondere soll der Test nachweisen, dass der Ausstiegs-Plan angemessen dokumentiert ist, realistisch ist und im Einklang mit den geschäftlichen und regulatorischen Anforderungen umgesetzt werden kann. Dazu gehört auch die Überprüfung der Verfügbarkeit der im Plan genannten Ressourcen. Der Umfang der Testaktivitäten soll risikoorientiert festgelegt werden.

Teilnehmerinnen und Teilnehmer am 27.11.2023

Bacher, David	Bayerischen Landesbank
Baumann, Dr. Ina	ARAG Versicherungen
Behrends, Dr. Tino	Genossenschaftsverband – Verband der Regionen e.V.
Bigeschi, Marco	Raiffeisenbank Aidlingen eG
Böse, Stefan	DZ BANK AG Deutsche Zentral-Genossenschaftsbank
Buddensiek, Dirk	Bürgschaftsbank Baden-Württemberg GmbH
Burckhardt, Michael	Commerzbank AG
Dickhoff, Andreas	Atruvia
Dierks, Christian	Deutsche Bank AG
Feller, Julia	Verband Deutscher Bürgschaftsbanken e.V.
Fichelscher, Andreas	Kreditanstalt für Wiederaufbau Anstalt des öff. Rechts
Gärtner, Heino	Norddeutsche Landesbank - Girozentrale -
Heinrich, Johannes	UniCredit Bank AG
Heuser, Simone	IKB Deutsche Industriebank AG
Hönes, Frank	Landesbank Baden-Württemberg
Huber, Ingo	Wüstenrot & Württembergische AG
Kastl, Andreas	Verband der Auslandsbanken in Deutschland e.V.
Koen, Oliver	Atruvia AG
Lehnen, Holger	Deutsche WertpapierService Bank AG (dwpbank)
Michelsen, Heiko	ING-DiBa AG
Müller, Dr. Thilo	Deutsche WertpapierService Bank AG (dwpbank)
Muster, Holger	Finanz Informatik GmbH & Co. KG
Penther, Brigitte	Hamburg Commercial Bank AG
Rabe, Michael	Bundesverbandes Öffentlicher Banken Deutschlands
Saam, Mirko	R+V Allgemeine Versicherung AG
Schaffer, Stefan	Deutsche Bank AG
Scheinhardt, Danny	Commerzbank AG
Schimm, Berit	Bundesverband VR Banken
Schneider, Dr. Ralf	Allianz Deutschland AG
Schwaab, Philipp	Helaba
Sieck, Gabriele	Gesamtverband der Deutschen Versicherungswirtschaft
Skopinski, Gero	Finanz Informatik IT Service
Staffler, Emanuel	Bayerischen Landesbank
Steuber, Martin	UniCredit Bank AG
Trojahn, Frank	DSGV
Weltermann, Christian	Commerzbank AG
Wehnes, Kathrin	Landesbank Hessen-Thüringen Girozentrale
Zimmermann, Karin	BKM - Bausparkasse Mainz AG

Paust, Dr. Michael	Deutsche Bundesbank
Rest, Matthias	Deutsche Bundesbank
Schäfer, Dominik	Deutsche Bundesbank
Wittmann, Daniel	Deutsche Bundesbank
Kleinknecht-Dennart, Dr. Sven	Bundesanstalt für Finanzdienstleistungsaufsicht
Kosche-Steinbrecher, Ira	Bundesanstalt für Finanzdienstleistungsaufsicht
Kiefer, Jan	Bundesanstalt für Finanzdienstleistungsaufsicht
Pohl, Markus	Bundesanstalt für Finanzdienstleistungsaufsicht