

Protokoll

Sonderfachgremium IT zum Thema „Cloud/IT-Notfallmanagement“

27.11.2023

per Videokonferenz

Präambel

Im vorliegenden Protokoll werden die maßgeblichen Diskussionsaspekte sowie -ergebnisse aus dem Termin des Sonderfachgremiums IT zum Thema „Cloud/IT-Notfallmanagement“ zusammengefasst. Im Nachfolgenden werden die Prozesse und Verfahren betrachtet, welche die Fortführung und Wiederherstellung zeitkritischer IT-Aktivitäten und -Prozesse des Finanzunternehmens sicherstellen und in Kapitel 10 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 und der damit verbundenen Delegierten Verordnungen) 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 das IT-Notfallmanagement

Die aufsichtsrechtlichen Anforderungen an das IT-Notfallmanagement leiten sich bei Banken vor allem aus den EBA-Leitlinien für das Management von IKT- und Sicherheitsrisiken (insb. Abschnitt 3.7), den Leitlinien zu Auslagerungen (insb. Tz. 48f), den MaRisk (insb. AT 7.3) und den BAIT (insb. Kapitel 10) 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.¹

Problemstellung der beaufsichtigten Unternehmen

Für das Thema IT-Notfallmanagement im Cloud-Umfeld besteht eine wichtige Herausforderung darin, dass die Erbringung der Cloud-Services durch den Cloud-Anbieter durch eine

¹ Ab dem 17. Januar 2025 gilt die DORA Verordnung (Artikel 64 DORA). Gemäß Artikel 5, 6, 11, 12 und 28 i. V. m. der einschlägigen Delegierten Verordnung sind angemessene IT-Notfallmaßnahmen einzurichten.

Abstraktionsgrenze² gekennzeichnet ist. Die Abstraktionsgrenze verläuft differenziert nach dem konkret eingesetzten Cloud-Service in Abhängigkeit des beauftragten Service Modells und der Art der Nutzung durch das beaufsichtigte Unternehmen.

So hat ein beaufsichtigtes Unternehmen z. B. keine Detailinformationen zu den konkret genutzten IT-Komponenten, die dem beauftragten Cloud-Dienst zu Grunde liegen und üblicherweise keinen oder nur geringen Einfluss auf die interne Prozessgestaltung beim Cloud-Anbieter. Eine individuelle Berücksichtigung von kundenspezifischen Anforderungen aus dem IT-Notfallmanagement wird zumeist vom Cloud-Anbieter abgelehnt, vielmehr stellt dieser häufig standardisierte Dienstleistungen und Informationen für alle Kunden zur Verfügung. Aus diesem standardisierten Leistungsangebot können die beaufsichtigten Unternehmen eine für sie zum eigenen Anforderungsniveau passende Herangehensweise wählen.

In der Regel wird der Ausfall einzelner IT-Komponenten unterhalb der Abstraktionsgrenze dem beaufsichtigten Unternehmen durch den Cloud-Anbieter nicht angezeigt und kann teilweise durch die laufende Überwachung nicht erkannt werden, da die IT-Servicebereitstellung in vielen Fällen über mehrere Rechenzentren, vielfach sogar überregional verteilt, erfolgt. Diese redundante IT-Servicebereitstellung führt dazu, dass das Risiko aus einer etwaigen Beeinträchtigung zeitkritischer Aktivitäten und Prozesse für das auslagernde Unternehmen üblicherweise deutlich reduziert ist.

In der Praxis bedeutet dies meist Folgendes:

- Die Auswahl und die konkret gewählte Konfiguration der Cloud-Dienste sowie der Architektur der Cloud-Anwendung durch das beaufsichtigte Unternehmen bestimmen maßgeblich die „Notfallfestigkeit“ der Cloud-Nutzung.
- Eine kundenspezifische Abstimmung der eigenen Notfallkonzepte sei aufgrund der hochstandardisierten Dienste und Prozesse des Cloud-Anbieters häufig nicht möglich.
- Aufgrund der Art der IT-Servicebereitstellung in der Cloud sind durch den Cloud-Anbieter in vielen Fällen bereits Redundanz- und Hochverfügbarkeitsmechanismen etabliert, die auch einen Teil des Charakters von Cloud-Dienstleistungen ausmachen.
- Durch die Virtualisierung, die Nutzung verteilter Systeme und Rechenzentren, ist die Nachweisbarkeit der Wirksamkeit und Angemessenheit der IT-Notfallpläne für bestimmte Szenarien andersartig als bisher umzusetzen. Dazu zählen insbesondere der Nachweis eines Rechenzentrumswechsels oder eines Systemausfalltests.
- Über die gezielte Abschaltung bestimmter Cloud-Dienste durch das beaufsichtigte Unternehmen lassen sich Ausfälle und Wiederherstellungen virtuell simulieren und dokumentieren. Eine physische Abschaltung von geteilten Komponenten beim Cloud-Anbieter kann durch den Kunden üblicherweise nicht beauftragt werden.
- Individualisierte Nachweise für IT-Notfalltests oder zwischen Dienstleister und Nutzer koordinierte IT-Notfalltests, die bei einem IT-Dienstleister typischerweise beauftragt werden konnten, sind bei Cloud-Anbietern in der Praxis oftmals nicht oder nur schwer erhältlich.

² Siehe Protokoll des Sonderfachgremium Cloud zum Thema „CMDB“: https://www.bafin.de/Shared-Docs/Downloads/DE/Protokoll/dl_01032022_Protokoll_Sonderfachgremium_IT.pdf

Diskussionsergebnisse

Das beaufsichtigte Unternehmen ist für ein angemessenes IT-Notfallmanagement verantwortlich, dies beinhaltet auch die ausgelagerten Cloud-Dienstleistungen. Für die IT-Notfallpläne und die Durchführung von IT-Notfalltests durch das beaufsichtigte Unternehmen gilt der Ansatz der Abstraktionsgrenze analog, d.h. die Verteilung der Zuständigkeiten orientiert sich an ihr. Die Abstraktionsgrenze stellt somit die Grenze der Zuständigkeit zwischen dem beaufsichtigten Unternehmen und dem Cloud-Anbieter dar. Bezogen auf das IT-Notfallmanagement ist – entsprechend dieser Zuständigkeitsverteilung – unterhalb der Abstraktionsgrenze grundsätzlich das IT-Notfallmanagement des Cloud-Anbieters relevant, oberhalb der Abstraktionsgrenze das IT-Notfallmanagement des jeweiligen beaufsichtigten Unternehmens.

Die IT-Systeme und -Komponenten oberhalb der Abstraktionsgrenze lassen sich in der Regel ohne größere Herausforderungen in die bestehenden IT-Notfallmanagementprozesse einbetten. Dazu werden auf Basis der Notfallkonzepte die IT-Systeme und -Komponenten, die zeitkritische Aktivitäten und Prozesse unterstützen, identifiziert. Bei Nutzung der Cloud sind hierfür die genutzten Cloud-Dienste oberhalb bzw. an der Abstraktionsgrenze relevant.

Unterhalb der Abstraktionsgrenze muss das beaufsichtigte Unternehmen sicherstellen, dass beim Cloud-Anbieter ein angemessenes IT-Notfallmanagement eingerichtet ist, sowie die mit den genutzten Cloud-Diensten verbundenen Risiken bewerten und eigene Maßnahmen ergreifen, um nicht akzeptable Schäden auszuschließen. Dazu muss es bei wesentlichen Auslagerungen regelmäßig, zumindest aber jährlich, entsprechende Berichte³ über die ergriffenen IT-Notfallmaßnahmen und durchgeführten IT-Notfalltests vom Cloud-Anbieter einfordern und auswerten. Der Nachweis über vom Cloud-Anbieter bereitgestellte Zertifikate/Prüfberichte ist dafür nicht ausreichend.

Bezogen auf den Notbetrieb, den Wiederanlauf und die Wiederherstellung der IT-Systeme gilt ebenfalls die bereits ausgeführte Teilung der Zuständigkeiten. Im Falle eines IT-Notfalls bei einem Cloud-Anbieter leitet dieser die durchzuführenden Maßnahmen eigenständig ein. Wenn nötig werden vom beaufsichtigten Unternehmen ergänzende Maßnahmen (eigenständig oder auf Empfehlung des Cloud-Anbieters) durchgeführt, üblicherweise erfolgt dies asynchron. Eine zwingende Abhängigkeit zwischen den Maßnahmen von Cloud-Anbieter und Nutzer im IT-Notfall besteht in der Regel nicht, d. h. ein IT-Notfall des Cloud-Anbieters kann zu einem IT-Notbetrieb des beaufsichtigten Unternehmens führen, muss es aber nicht.

Bei Schwächen im IT-Notfallmanagement des Cloud-Anbieters entwickelt dieser eigenverantwortlich Maßnahmen und setzt sie um. Über die Ergebnisse der Bearbeitung der Maßnahmen werden die beaufsichtigten Unternehmen verpflichtend informiert, damit eine geeignete Berücksichtigung im Risikomanagement erfolgen kann, insbesondere auch durch eigene Maßnahmen.

³ Siehe Art. 10 Abs. 2 lit. a des Draft Regulatory Technical Standards to specify the detailed content of the policy in relation to the contractual arrangements on the use of ICT services supporting critical or important functions provided by ICT third-party service providers as mandated by Regulation (EU) 2022/2554

Notfallkonzept

1. Das beaufsichtigte Unternehmen stellt durch seine Cloud-Architektur und -Konfiguration sicher, dass die Schutzziele seiner Geschäftsprozesse und Daten sowie der zugehörigen Geschäfts-/ Softwareanwendungen eingehalten werden.
2. Das Notfallkonzept des beaufsichtigten Unternehmens basiert auf der durch das Institut vorzunehmenden architekturellen, geografischen und serviceseitigen Konfiguration der Cloud-Dienste und Cloud-Anwendungen (z. B. Festlegung von Availability Zones, Regionen, SLAs) zur Erreichung der geforderten Verfügbarkeit und Redundanz.
3. Durch diese architekturellen und konfigurationsseitigen Einstellungen soll erreicht werden, dass auch singuläre, kritische Ereignisse auf Seiten des Cloud-Anbieters nicht zu einer Unterschreitung der zwischen dem beaufsichtigten Unternehmen und dem Cloud-Anbieter vertraglich festgelegten Verfügbarkeiten führen.
4. Bei sehr hohen Anforderungen des beaufsichtigten Unternehmens an die Verfügbarkeit, die nicht allein durch die architekturellen und konfigurationsseitigen Einstellungen eines einzelnen Cloud-Anbieters abgedeckt werden können, sind darüber hinausgehende Maßnahmen durch das beaufsichtigte Unternehmen vorzusehen.

IT-Notfalltest / -überprüfung

5. Die IT-Notfalltests auf Seiten des beaufsichtigten Unternehmens umfassen die geforderten Szenarien, die sich oberhalb bzw. bis an die Abstraktionsgrenze erstrecken und damit Bestandteil der eigenen Notfallkonzepte und IT-Notfallpläne sind. Somit sind die Cloud-spezifischen IT-Systeme / IT-Komponenten bis zur Abstraktionsgrenze in das IT-Notfallmanagement des beaufsichtigten Unternehmens integriert und werden regelmäßig getestet. Dies beinhaltet z. B. auch die Erreichbarkeit bzw. den Ausfall eines Service oder einer Availability Zone – jedoch keine Szenarien, die in den Verantwortungsbe- reich des Cloud-Anbieters hineinreichen, einschließlich übergreifender Szenarien wie bspw. „Ausfall Rechenzentrum am Standort A“, „Stromausfall im Rechenzentrum B“ o- der „Störung der Kommunikation zwischen Rechenzentrum A und B“.
6. Die IT-Notfalltests für die IT-Systeme und IT-Komponenten unterhalb der Abstraktions- grenze werden vom Cloud-Anbieter eigenständig durchgeführt. Hierbei ist keine zeitli- che oder logische Abhängigkeit bzw. Verknüpfung mit den IT-Notfalltests des beauf- sichtigten Unternehmens erforderlich.
7. Bei nicht erfolgreichen Tests der beaufsichtigten Unternehmen wird der Cloud-Anbieter von dem beaufsichtigten Unternehmen über die erkannten Lücken informiert, sofern diese unterhalb der Abstraktionsgrenze liegen. Hier entwickelt der Cloud-Anbieter zur Schließung der Lücken im Rahmen des Notfallmanagements ebenfalls Maßnahmen, setzt diese um und informiert die beaufsichtigten Unternehmen. Handelt es sich um Lü- cken im Zuständigkeitsbereich der beaufsichtigten Unternehmen oberhalb der Abstrak- tionsgrenze, wird dieses eigenverantwortlich Maßnahmen definieren und umsetzen. Die Lücken werden dabei im eigenen Risikomanagement berücksichtigt.

Nachweis der IT-Notfallpläne und IT-Notfalltests beim Cloud-Anbieter

8. Dem beaufsichtigten Unternehmen muss mindestens für IT-Systeme, die zeitkritische Prozesse unterstützen, eine aussagekräftige Berichterstattung des Cloud-Anbieters über die gewählten IT-Notfallmaßnahmen sowie Art der Tests, die Testabdeckung, Informationen zur Durchführung und das Ergebnis der relevanten IT-Notfalltests auf Seiten des Cloud-Anbieters vorliegen. Als relevant gelten diejenigen Maßnahmen und Tests, die sich auf die vom beaufsichtigten Unternehmen genutzten Cloud-Dienste beziehen.
9. Das beaufsichtigte Unternehmen analysiert alle vorliegenden Informationen, führt ggf. Anpassungen an seiner Notfallkonzeption durch, wirkt, falls notwendig, auf entsprechende Anpassungen seitens des Cloud-Anbieters hin und berücksichtigt Einschränkungen der IT-Notfalltests inkl. zu erbringender Nachweise im Rahmen des Risikomanagements. Darüber hinaus legt das beaufsichtigte Unternehmen Nachweise zusammen mit der eigenen Dokumentation sicher ab. Die Nachweise des Cloud-Anbieters müssen nicht kundenspezifisch sein.
10. Darüber hinaus sind in regelmäßigen Abständen eigene Prüfungen des IT-Notfallmanagements (z. B. in Form von Revisionsprüfungen, Pool-Prüfungen, Beauftragung Dritter) risikoorientiert durchzuführen, um eine unabhängige Einschätzung über die Qualität des IT-Notfallmanagements zu erhalten.

IT-Notfall, IT-Notbetrieb, Wiederherstellung und Wiederanlauf

11. Das beaufsichtigte Unternehmen stellt vertraglich sicher, dass die im Falle eines IT-Notfalls relevanten Informationen innerhalb der erforderlichen Fristen dem Unternehmen und dort den konkreten Servicenutzern zur Verfügung stehen.
12. Ergänzend zu den vom Cloud-Anbieter bereitgestellten Informationen über allgemeine Informationskanäle⁴, informiert der Cloud-Anbieter aktiv und zeitnah über vereinbarte Informations- bzw. Kommunikationskanäle (z.B. E-Mail, Telefon, SMS) über schwerwiegende Störungen, welche die zugesicherte Dienstleistungsqualität (z.B. Verfügbarkeit, Performance) seiner Services an der Abstraktionsgrenze maßgeblich beeinträchtigen können.
13. Updates zu diesen schwerwiegenden Störungen durch den Cloud-Anbieter erfolgen ebenfalls über diese Informations- bzw. Kommunikationskanäle. Das beaufsichtigte Unternehmen trägt dafür Sorge, dass der Informationsbezug auf seiner Seite sichergestellt ist.
14. Entscheidungsgrundlage für die im eigenen Verantwortungsbereich des beaufsichtigten Unternehmens ggf. einzuleitenden Maßnahmen bildet die potentielle Auswirkung auf den Betriebszustand der genutzten IT-Systeme und IT-Komponenten oberhalb der Abstraktionsgrenze.
15. Unabhängig davon, ob ein IT-Notbetrieb des beaufsichtigten Unternehmens durch den Cloud-Anbieter oder das beaufsichtigte Unternehmen selbst verursacht ist, sind die auf

⁴ Managementkonsole oder Admin-Dashboards, siehe Protokoll des Sonderfachgremium Cloud zum Thema „IT-Betrieb“: https://www.bafin.de/SharedDocs/Downloads/DE/Protokoll/dl_Protokoll_Sonderfachgremium_IT_am_310523.html

Seiten des beaufsichtigten Unternehmens durchzuführenden Maßnahmen in der Regel unabhängig und entkoppelt von den Service- und Betriebsleistungen bzw. evtl. Notfallmaßnahmen des Cloud-Anbieters.

16. Auch das beaufsichtigte Unternehmen soll dem Cloud-Anbieter schwerwiegende Störungen im Zusammenhang mit den genutzten Cloud-Diensten über die dafür vorgesehenen Meldekanäle für Störungen oder über die vereinbarten zusätzlichen Informations- bzw. Kommunikationskanäle melden, sofern diese auf IT-Systeme und IT-Komponenten an oder unterhalb der Abstraktionsgrenze zurückzuführen sind.
17. Im Nachgang zur Störungsbeseitigung bzw. der Beendigung des IT-Notbetriebs soll das beaufsichtigte Unternehmen einen Abschlussreport mit Root-Cause-Analyse vom Cloud-Anbieter beziehen. In der Nachbetrachtung wird der IT-Notfall analysiert (u.a. Ursache/ Auslöser, Störungsbeseitigung und Kommunikation) sowie daraus abgeleitete Maßnahmen vereinbart (z.B. in gemeinsamen Service-Meetings) und ggf. auch eigene Maßnahmen durch das beaufsichtigte Unternehmen ergriffen. Bestehende Risiken müssen entsprechend den Vorgaben des Risikomanagementprozesses behandelt werden.
18. Das beaufsichtigte Unternehmen überprüft seine IT-Notfallpläne mindestens einmal pro Jahr und passt diese an realisierte Verfügbarkeiten (u. a. Testergebnisse, eingetretene Vorfälle) sowie die allgemeine Bedrohungslage an.

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