© GaudiLab/Getty Images/iStock.

Was Bank-Technologen den Rücken freihält

Finanzinstitute und ihre IT sehen sich mit zahlreichen Risiken konfrontiert. Deshalb arbeiten Experten nicht nur an der Effizienz, sondern auch an der Sicherheit von Systemen und Prozessen. Mit Business Continuity Management können diese Bemühungen gebündelt und die Ausfallsicherheit erhöht werden.

Dieter Ketterle

Die Abhängigkeit der Banken und Sparkassen von der IT unterstreicht, warum gerade im Finanzsektor die Bedeutung eines reibungslosen Betriebs mit hoher Verfügbarkeit kaum groß genug eingeschätzt werden kann. Allein 2018 meldeten deutsche Geldhäuser bei der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) insgesamt 301 IT-Störungen. Dem müssen Banken aktiv mit Business Continuity Management, kurz BCM, gegensteuern. Denn durch geeignete Maßnahmen lassen sich zwar nicht alle Störungen verhindern, aber ihre Auswirkungen deutlich begrenzen.

Mögliche Auslöser für eine Störung der IT gibt es viele, angefangen bei gravierenden Ereignissen wie Naturkatastrophen über kriminelle Handlungen wie Cyberangriffe bis zu eher alltäglichen Ereignissen wie Streiks oder Störungen der Lieferkette. Ohne ein geeignetes BCM können sie Unternehmen komplett lahmlegen. Um das zu verhindern, verlangt die Europäische Zentralbank (EZB) von Finanzdienstleistern deshalb ein professionelles BCM und den Nachweis, dass ein Rechenzentrum im Bedarfsfall in kurzer Zeit einen Notbetrieb sicherstellen kann.

Nicht nur auf europäischer Ebene, sondern auch auf Bundesebene gewinnt das Thema BCM an Bedeutung. Daraus entstehen immer konkretere und komplexere regulatorische Vorgaben für Finanzinstitute. Banken müssen sich also nicht nur an die Vorgaben der EZB halten, sondern beispielsweise auch die Standards des Bundesamts für Sicherheit in der Informationstechnik (BSI) berücksichtigen. Das übergeordnete Ziel der Vorschriften besteht darin, dass Unternehmen oder Behörden ein systematisches Notfallmanagement aufbauen, das die Kontinuität des Geschäftsbetriebs sichert und mögliche Schäden gering hält. Die Regulierung verpflichtet Banken auch dazu, regelmäßig die Wirksamkeit und Angemessenheit ihres Notfallmanagements durch Tests zu überprüfen und nötigenfalls Anpassungen vorzunehmen.

Kompakt

- Aufgrund der komplexen regulatorischen Anforderungen sollte Business Continuity Management (BCM) in Banken hohe Priorität genießen.
- Das technologische Rückgrat des BCM muss sauber aufgebaut sein, auf die individuellen Ansprüche des Instituts zugeschnitten werden sowie die Handlungsfelder IT-Service Continuity Management und Krisenmanagement enthalten.
- Erarbeitete Abläufe und Prozesse müssen immer wieder überprüft werden, da sich Vorgaben und Rahmenbedingungen ständig verändern.

Beim BCM in der Finanzwirtschaft steht die sensible Infrastruktur besonders im Fokus. Die Sicherheit von unternehmenskritischen Daten muss zu jedem Zeitpunkt garantiert sein. Fällt ein Kernbanksystem aus, ist die komplette Steuerung des Instituts betroffen. Es kann dann etwa nicht mehr auf relevante Kennziffern zugreifen und auf Entwicklungen am Markt reagieren. Auch Buchungen sind ohne das Kernbanksystem nicht möglich.

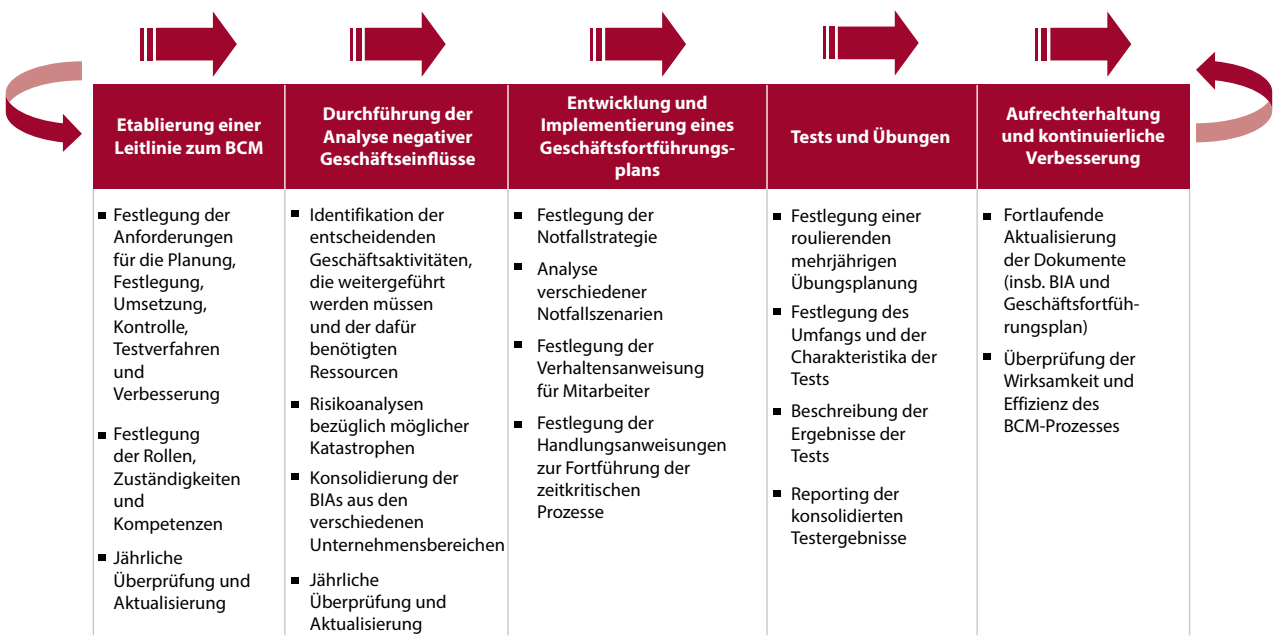
Aufgrund der wachsenden Komplexität und der immer strengeren regulatorischen Vorgaben haben viele Banken ihre IT an Dienstleister ausgelagert. Für diese gelten in Bezug auf das BCM die gleichen Vorschriften wie für Kreditinstitute selbst. Zusätzlich legt die BaFin in ihren Mindestanforderungen an das Risikomanagement (MaRisk) fest, was Dienstleister können müssen und wie die Zusammenarbeit mit der jeweiligen Bank für das BCM zu gestalten ist. Die enge Abstimmung ist hier wichtig. Zu klären ist etwa, wie notfallrelevante Systeme aufgebaut sein sollen oder wie viele Stunden die Systeme maximal ausfallen dürfen.

Dienstleister müssen ebenso hohe Ansprüche erfüllen wie Banken

Die Anforderungen an Dienstleister in Sachen BCM sind ebenfalls hoch. Sie sind dazu verpflichtet, alle Themen, die für das BCM von Bedeutung sind, nicht nur zu analysieren und zu bewerten, sie müssen auch Vorsorgemaßnahmen ergreifen und deren Wirksamkeit durch Tests belegen (siehe Kasten Seite 42). Business-Impact-Analysen zeigen, welche Prozesse und Ressourcen besonders geschützt werden müssen. Tritt trotz Vorsorgemaßnahmen ein Notfall ein, müssen Dienstleister über Pläne und Abläufe verfügen, um die Folgen für Geschäftsprozesse zu minimieren.

Zu den Anforderungen der Regulierer kommen noch die Anforderungen der Banken. Neben Notfallplanung und -vorsorge erwarten die Institute von ihren Dienstleistern, dass deren BCM auch die Notfallorganisation beinhaltet. Die

Modell zur Umsetzung eines Business Continuity Managements



BCM = Business Continuity Management
BIA = Business Impact Analysis, Analyse negativer Geschäftseinflüsse
Quelle: Anna-Luisa Müller: Business Continuity Management bei Finanzdienstleistungsunternehmen, in: Stefan Reinheimer, Susanne Robra-Bissantz (Hrsg.): Business-IT-Alignment, Wiesbaden 2017

Trainierte Abläufe helfen dabei, Ruhe zu bewahren

Prozesse immer wieder auf die Probe zu stellen und die erarbeiteten Notfallpläne ausgiebig zu testen, gehört zu den grundlegenden Maßnahmen bei einem professionellen Business Continuity Management (BCM). Diese Tests erfolgen nicht nur theoretisch, sondern trotz ihres großen Aufwands auch in der Praxis. Die Übungen machen deutlich, wie wichtig es ist, sich gezielt und mit System auf den Ernstfall vorzubereiten. Trainierte Abläufe helfen in einem plötzlich auftretenden Notfall dabei, Ruhe zu bewahren, statt in chaotische Hektik zu verfallen, und die notwendigen Maßnahmen durchzuziehen.

Im September 2018 probte die Finanz Informatik Technologie Service (FI-TS) den Ernstfall. Mit 16 Kunden, darunter große Landesbanken, simulierte sie den einwöchigen Ausfall eines auf Banken und Versicherer spezialisierten Rechenzentrums. Wie in den Notfallplänen vorgesehen, musste der komplette Betrieb schnellstmöglich auf ein anderes Rechenzentrum übertragen werden. Dank eines stabilen Grundsystems, um das herum alle Prozesse aufgebaut sind, verlief der Schwenk problemlos. Auf Kundenseite konnten alle Geschäftstätigkeiten ohne Störungen fortgesetzt werden. Das ist keine Selbstverständlichkeit, denn immerhin war eine dreistellige Zahl von Systemen von dem Test betroffen.

Zentraler Bestandteil der Testvorbereitung ist die Erstellung eines konsistenten Koordinationsplans. Dabei müssen zahlreiche Faktoren berücksichtigt und aufeinander abgestimmt werden, etwa die Auswahl der beteiligten Mitarbeiter und ihre Einsatzgebiete sowie die Einbindung der teilnehmenden Kunden. Für die Übung im Jahr 2018 wurde die Vorbereitung in mehrere Phasen unterteilt, um alle für den Test relevanten Faktoren zu berücksichtigen. Während dieser Phasen prüfte die FI-TS in verschiedenen Vortests einzelne notfallrelevante IT-Services im so genannten Stufe-1-Test und im Stufe-2-Test, ob alle notfallrelevanten IT-Services der Kunden migriert werden können. Den eigentlichen Schwenk der notfallrelevanten IT-Services aller teilnehmenden Kunden vollzogen die BCM-Experten der FI-TS gemäß dem Ablaufplan als letzten Schritt.


© fotovika/Fotolia

Der Test ermöglichte es der FI-TS, ihre Notfallpläne einer Bewährungsprobe zu unterziehen. Die Pläne können somit bedenkenlos bei einem tatsächlichen Störfall eingesetzt werden. Dabei existiert für jedes definierte Worst-Case-Szenario ein detaillierter Geschäftsfortführungsplan. Die Eckpunkte der dafür notwendigen Zusammenarbeit zwischen den einzelnen Arbeitsebenen sind in einem Schnittstellendokument festgehalten.

Trotz aller Vorbereitungen und der bestandenen Übung wissen die BCM-Experten von FI-TS, dass das Testen nie aufhört. Denn zum einen sieht der Regulierer eine regelmäßige Überprüfung vor. Und zum anderen gilt: Nur wer seine Prozesse und Vorkehrungen kontinuierlich auf die Probe stellt, kann sich im Ernstfall auf sein BCM verlassen.

IT-Unternehmen arbeiten daher zum Beispiel mit Notfallrechenzentren, um bei Störungen ein schnelles Umschalten des Betriebes garantieren zu können. Des Weiteren stehen bei den Dienstleistern rund um die Uhr Mitarbeiter in Notfallteams bereit. Empfehlenswert ist außerdem, in das Notfallmanagement auch die Handlungsfelder IT-Service Continuity Management (ITSCM) und Krisenmanagement zu integrieren.

Für ein professionelles BCM, wie es Regulierer und Banken von IT-Dienstleistern in der Finanzwirtschaft erwarten, ist vor allem ein solides Grundsystem von großer Bedeutung. Alle wichtigen Schritte und Prozesse müssen darin enthalten sein, ebenso wie konkrete Vereinbarungen zwischen Outsourcing-Provider und Finanzdienstleister. Auf dieser Grundlage baut der gesamte BCM-Prozess auf. Aus ihm muss hervorgehen, welche Maßnahmen und Notfallübungen durchzuführen sind. Empfehlenswert ist ein auf Standards basierendes BCM mit regulierungserprobten Prozessen, bei dem Banken von Skaleneffekten profitieren und dieses zugleich auf ihre individuellen Anforderungen anpassen lassen können. ■

Autor

Dieter Ketterle
ist Business Continuity Manager bei Finanz Informatik Technologie Service (FI-TS), einer Tochtergesellschaft der Finanz Informatik.