Business Continuity Management schützt die IT

Von Dieter Ketterle

IT-Ausfälle von Banken schwächen nicht nur das Kundenvertrauen, sie gefährden – je nach Ausmaß – auch das Finanzsystem. Regulatorische Vorgaben schreiben deshalb ein Business Continuity Management vor, damit der Betrieb auch bei Störfällen weitergeführt werden kann. Wichtig dabei, so der Autor, sind neben einem soliden Grundsystem und einem konsistenten Koordinationsfall auch regelmäßige Tests und Störfallsimulationen, um die Notfallpläne einer Bewährungsprobe zu unterziehen. Dann lässt sich die Ausfallsicherheit auch bei Störfällen deutlich verbessern Red.

Die IT von Banken und Finanzdienstleistern ist vielen potenziellen Bedrohungen ausgesetzt. Von Naturkatastrophen über kriminelle Handlungen wie Cyberangriffe, von Stromausfällen bis zu Streiks oder Unterbrechungen der Lieferketten – es kann viele verschiedene Ursachen für Störungen der IT oder gar für IT-Ausfälle bei Banken geben. Solche Ereignisse können die Geschäftstätigkeit von Instituten im schlimmsten Fall zum Erliegen bringen, wenn sie nicht rechtzeitig erkannt werden und gegengesteuert wird.

301 IT-Störungen im Jahr 2018

Die Sicherheit der Systeme und Prozesse muss oberste Priorität haben, um die Auswirkungen solcher Ereignisse und damit den wirtschaftlichen Schaden für die Finanzdienstleister so gering wie möglich zu halten. Der Schlüssel zur Problemlösung und einer deutlichen Verringerung des Ausfallrisikos ist ein professionelles Business Continuity Management, kurz BCM.

Die Anzahl der alljährlich bekannt werdenden Störfälle ist besorgniserregend. Im Jahr 2018 meldeten deutsche Banken insgesamt 301 IT-Störungen bei der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin). Besonders unangenehm können Auswirkungen im Kundengeschäft sein. Vertrauen in den Finanzdienstleister schwindet schnell, wenn beispielsweise der Zugriff auf Online-Konten nicht mehr möglich ist.

Die hohe Zahl der Fälle verdeutlicht, dass die Banken aktiv werden müssen. Die beste Gegenmaßnahme ist ein professionelles Business Continuity Management, mit dem zwar nicht immer alle Störungen verhindert, die negativen Auswirkungen aber sehr deutlich reduziert werden können. Denn klar ist: Die Abhängigkeit der Finanzdienstleister von der IT ist unumstritten, ohne die Technik sind Bankgeschäfte heute nicht mehr möglich. Folglich muss die IT sicher sein.

Die Regulatorik

Neben der daraus resultierenden Notwendigkeit, ein professionelles BCM zu installieren, gibt es auch konkrete und komplexe regulatorische Vorgaben, die dies vorschreiben. Finanzdienstleister müssen der Europäischen Zentralbank (EZB) gegenüber den Nachweis erbringen, dass ein Rechenzentrum im Bedarfsfall in kurzer Zeit einen Notbetrieb gewährleisten kann und dass sie über ein geeignetes Business Continuity Management verfügen.

Banken sind außerdem verpflichtet, die Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und die der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) einzuhalten. Das Ziel der Behörden liegt darin, Institute zum Aufbau eines systematischen Notfallmanagements anzuhalten, um so die Kontinuität des Geschäftsbetriebes sicherzustellen und Schäden möglichst einzudämmen beziehungsweise gar

Dieter Ketterle, Business Continuity Manager, Finanz Informatik Technologie Service GmbH & Co. KG, Haar

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Fritz Knapp Verlag GmbH

nicht erst entstehen zu lassen. Die regulatorischen Vorgaben verpflichten Banken dazu, ihr Notfallmanagement und dessen Wirksamkeit ständig durch Tests zu überprüfen. Falls während der Probeläufe Schwachstellen entdeckt werden, sind Anpassungen dringend notwendig. Besonders wichtig ist, dass die Sicherheit unternehmenskritischer Daten jederzeit gewährleistet sein muss. Das gilt selbstverständlich auch für die Sicherheit systemrelevanter Daten, über die Landesbanken verfügen.

Weitreichende Folgen hätte der mögliche Ausfall des Kernbanken-Systems, denn dann wäre die komplette Steuerung lahmgelegt. In einem solchen Fall gäbe es keinen Zugriff auf relevante Kennziffern mehr, Buchungen und Reaktionen auf Marktentwicklungen wären nicht mehr möglich. Diesen Gefahren gilt es mit einem leistungsfähigen BCM entgegen zu treten.

Viele Banken haben ihre IT an einen Dienstleister ausgelagert, nicht zuletzt, weil die Komplexität und die regulatorischen Vorgaben immer mehr zunehmen. Für diese gelten dieselben regulatorischen Vorgaben, wie für die Banken. Die BaFin legt in ihren Mindestanforderungen an das Risikomanagement (MaRisk) zusätzlich fest, was ein IT-Dienstleister können muss und wie die Zusammenarbeit mit der Bank auszusehen hat. Enge Kooperation und Abstimmungen zwischen den Finanzinstituten und ihrem IT-Dienstleister sind nötig, um beispielsweise den Aufbau notfallrelevanter Systeme abzuklären, oder zu definieren, wie lange der maximale Ausfall der Systeme im Notfall dauern darf.

Die wichtigste Säule ist das Grundsystem

Die wichtigste Säule eines professionellen Business Continuity Management, so wie die Regulatorik es vorschreibt und wie es von den Banken bezüglich seiner Leistungsfähigkeit erwartet wird, ist ein solides Grundsystem mit einem sauber aufgebauten technologischem Rückgrat. Darin müssen alle wichtigen Schritte und Prozesse enthalten sein. Dazu gehört auch die Integration konkreter Vereinbarungen zwischen Outsourcing-Provider und Finanzdienstleister.

Aus dem darauf aufbauenden BCM-Prozess muss hervorgehen, welche Maßnahmen und Notfallübungen durchzuführen sind. Finanz Informatik Technologie Service (FI-TS) empfiehlt seinen Kunden, in ein professionelles Notfallmanagement auch die Handlungsfelder IT-Service Continuity Management (ITSCM) und Krisenmanagement zu integrieren. Darin enthalten sind beispielsweise auch die Aufstellungen von Notfallplänen und Notfallteams – das sind Mitarbeiter, die rund um die Uhr bereit stehen, um die Erfüllung aller Vorgaben sicherzustellen. Durch die Verbindung dieser Bereiche kann die Wirksamkeit des BCM sichergestellt werden.

Die wichtigste Regel: immer wieder testen

Ein weiterer wichtiger Faktor ist die Verwendung von Standards. So profitieren Kunden nicht nur von regulationserprobten Prozessen, sondern auch von Skaleneffekten. Dank der hohen Skalierbarkeit kann ein solches BCM sehr gut an die teilweise sehr individuellen Anforderungen der Kunden angepasst werden. Da FI-TS den Aufbau des Grundsystems bereits 2009 in Angriff nahm und seitdem ständig weiterentwickelte, wurden die Prozesse mit den wachsenden Kundenzahlen und deren Anforderungen kontinuierlich angepasst und aktualisiert.

Die wichtigste Regel beim Business Continuity Management lautet: die erarbeiteten Prozesse, Methoden und Abläufe immer wieder zu testen und zu überprüfen, um sicherzustellen, dass sie in der Praxis bestehen und den aktuellen Herausforderungen stets genügen. Testläufe sind extrem wichtig, um auf Ernstfälle vorbereitet zu sein. Das gilt aber nicht nur für die Theorie, sondern auch für die Praxis. Die Erprobung von Notfallplänen hilft, die Ruhe zu bewahren, wenn eine Störung auftritt.

Konsistenten Koordinationsplan erstellen

Die Erstellung eines konsistenten Koordinationsplans ist dabei von zentraler Bedeutung. Hierbei gilt es, zahlreiche unterschiedliche Faktoren zu berücksichtigen und aufeinander abzustimmen. Unter anderem müssen die beteiligten Mitarbeiter ausgewählt, ihre Einsatzgebiete definiert und die teilnehmenden Kunden eingebunden werden.

Die Vorbereitung für den Test wurde in mehrere Phasen unterteilt, um sicherzustellen, dass alle relevanten Faktoren berücksichtigt wurden. Die FI-TS prüfte in verschiedenen Vortests einzelne notfallrelevante IT-Services (Stufe-1-Test), dann ob alle notfallrelevanten IT-Dienste migriert werden konnten (Stufe-2-Test). Zuletzt erfolgte der eigentliche Schwenk der notfallrelevanten IT-Services aller teilnehmenden Kunden, den die BCM-Experten nach einem sorgfältig ausgearbeiteten Ablaufplan vollzogen. Dabei traten im Rahmen des gesamten Tests keine Probleme auf. Dank der erfolgreich bestandenen Bewährungsprobe wissen jetzt alle Beteiligten, dass die erarbeiteten Pläne nun in einem Störfall bedenkenlos eingesetzt werden können. Für jedes definierte Worst-Case-Szenario existiert dabei ein detaillierter Geschäftsfortführungsplan. Ein Schnittstellendokument hält die Eckpunkte der dafür notwendigen Zusammenarbeit zwischen den einzelnen Arbeitsebenen fest.

Ausfallsicherheit steigt auch bei Störfällen an

Regelmäßige Kontrolle der Strategie und praxisbezogene Tests – das sind die wichtigsten Säulen bei der Durchführung eines professionellen, regulationskonformen Business Continuity Management. Nur wenn Prozesse, Vorkehrungen und Maßnahmen regelmäßig auf die Probe gestellt werden, ist im Ernstfall Verlass auf sie. BCM-Experten führen daher Business Impact Analysen durch, sodass sie wissen welche Prozesse und Ressourcen besonders geschützt werden müssen.

Empfehlenswert ist es, den BCM-Zyklus möglichst schnell zu dokumentieren. Die daraus gewonnen Erkenntnisse sollten unternehmensweit stets präsent und abrufbar sein, etwa in Leitfäden. Die entsprechende Durchsetzung liegt in letzter Verantwortung auf der Führungsebene der Unternehmen. Dort ist eine hohe Aufmerksamkeit der leitenden Angestellten nötig, denn ohne deren Unterstützung ist die Umsetzbarkeit eines wirkungsvollen und professionellen BCM nur schwer möglich – es erfordert viel Zeitaufwand und entsprechende finanzielle Investitionen. Doch wenn ein solides BCM etabliert wurde, steigt damit die Ausfallsicherheit der IT auch bei Störfällen deutlich an. ■

Dieser Artikel ist urheberrechtlich geschützt. Die rechtliche Freigabe ist für den Abonnenten oder Erwerber ausschließlich zur eigenen Verwendung.
Fritz Knapp Verlag GmbH