Ausrichtung auf das Business

Interview mit Gerhard Neidhöfer, Gründer und geschäftsführender Gesellschafter der ACG Automation Consulting Group GmbH, über die Automatisierung von Geschäftsprozessen und ein funktionierendes Business Continuity Management

IT-DIRECTOR: *Herr Neidhöfer, der Markt für IT-Dienstleistungen ist groß und für Kunden manchmal recht unübersichtlich. Mit welchen Kernkompetenzen sticht ACG hier aus der Menge heraus?*

G. Neidhöfer: Die ACG ist auf die Automatisierung von Geschäftsprozessen mittels IT spezialisiert. Dies setzt klare Strukturen, transparente Abläufe, Verlässlichkeit der IT-Services und zielgerichtete Steuerung in einem flexiblen, lernfähigen und somit wirtschaftlichen Gesamtsystem voraus. Unser Unternehmen verbindet die Kenntnis des Geschäfts mit Informatik und sticht durch seine Kompetenz für die Organisation von Querschnittsprozessen im IT-Lebenszyklus hervor.

Gerhard Neidhöfer, *ACG GmbH*

Mehr als 1.500 Projekte im Bereich Organisation (Prozesse, Strukturen, Verantwortlichkeiten) wurden bei über 150 Kunden in der bislang 25-jährigen Unternehmensgeschichte erfolgreich abgeschlossen. Auftraggeber waren dabei Vorstand und Geschäftsleitung, Stäbe, Fachbereiche, IT-Anwendungsentwicklung sowie die IT-Produktion. Die differenzierten Sichten und Anforderungen dieser Auftraggeber sind in unsere Vorgehensmodelle eingeflossen.

Alle diese Erfahrungen haben wir in ein ganzheitliches Top-Down-Vorgehen eingebunden, welches von den Managementvorgaben über die Geschäftsanforderungen bis zu Richtlinien und Maßnahmen reicht. Durch das praxisorientierte und strategische Vorgehen entsteht ein geschäftszentriertes Gesamtsystem. Es richtet die IT-Services auf die geschäftlichen Anforderungen aus, macht sie steuerbar und integriert das Sicherheits-, Kontinuitäts- und Qualitätsmanagement mit dem Ziel durchgehender Compliance. So können wir IT-Services unternehmensspezifisch optimieren, das Bestehende konsolidieren und standardisieren, aber auch Teilaufgaben lösen – etwa beim Sourcing – oder bei dem Management der Service Level Agreements beraten.

IT-DIRECTOR: *Welche Zielgruppe sprechen Sie mit Ihren Services an?*

G. Neidhöfer: Zu unseren Zielgruppen zählen Finanzinstitute wie Banken, Versicherungen und Krankenkassen sowie die IT-Dienstleister dieser Branchen. Überdies erhalten wir auch Anfragen von Unternehmen anderer Branchen. Dies ist eine besondere Herausforderung, da wir aus unseren Erfahrungen heraus neue Ansätze finden können.

IT-DIRECTOR: *Stichpunkt Business Continuity Management (BCM): Welche Krisenszenarien treffen Sie bei Großunternehmen derzeit an?*

G. Neidhöfer: Die Szenarien reichen von Störungen über Notfälle bis hin zu Krisen, die sich durchaus auch auseinanderentwickeln können. Im Bankenbereich hat die Finanzmarktkrise zur Entwicklung von Strategien zur Früherkennung und Absicherung geführt. Der Ausfall externer Services, nicht nur in der IT, trifft manches Unternehmen unvorbereitet. So führt der Ausfall des Kommunikationsservices oder der Supply Chain schnell zu kritischen Situationen. Wenngleich Sicherheit und Verfügbarkeit bei Finanzinstituten besondere Beachtung genießen, so wird das angestrebte Niveau in seltenen Einzelfällen nicht erreicht. Unternehmen, die hohe und zudem terminkritische Millionenbeträge bewegen, sollten auch dies berücksichtigen. Die Kontinuität in der Stromversorgung ist in Deutschland sehr hoch. Dennoch gibt es Ausfälle, die Unternehmen berücksichtigen müssen. Im Rahmen der Umstellung auf erneuerbare Energien könnte sich dieses Risiko über-

gangsweise erhöhen. Dass nichts unmöglich ist, zeigen z.B. Bombenfunde bei Bauarbeiten neben einem wichtigen Rechenzentrum, die eine Evakuierung auslösten.

IT-DIRECTOR: *Wo bestehen denn Sicherheitslücken?*

G. Neidhöfer: In der IT ragen mehrere Faktoren heraus: organisatorisches, menschliches und technisches Versagen. Gerade die Organisation besitzt dabei einen hohen Stellenwert. Beispielsweise, wenn sich ein redundant geglaubtes Element als „Single Point of Failure" herausstellt, Lizenzen nicht rechtzeitig verlängert werden oder sich vertrauliche Daten aufgrund unzureichender Sicherheit und Data Leakage Prevention abgreifen lassen. Die immer wieder durch die Presse geisternden Datenschutzpannen bestätigen dies.

Der Einsatz von „Schnüffel-Software" ist aktuell. Dahinter steckt ein Internet-Trojaner, der sogar von den Behörden genutzt wurde. Doch nicht nur Behörden nutzen solche Schadsoftware, sondern auch Kriminelle, mit dem Ziel, Informationen auszuspionieren, Passwörter für E-Mail-Konten abzufangen oder Online-Banking zu manipulieren.

Weitere Beispiele waren im Jahr 2011 der Datendiebstahl beim IWF sowie Hackerangriffe auf Citigroup, Sonypictures.com und Google G-Mail. Aber auch menschliches Versagen, etwa beim Einspielen oder Aktivieren von Changes oder der Änderung von Konfigurationsparametern, führt zu IT-Ausfällen. Zeitdruck und massive Überstunden erhöhen die Fehleranfälligkeit und können durch einen Burnout bis zum Ausfall kritischer Leistungsträger führen. Fehlt dann ein gleichwertiger Ersatz, wird die Situation schnell brenzlig.

IT-DIRECTOR: *Was ist aus Ihrer Sicht wichtig für ein funktionierendes Business Continuity Management?*

G. Neidhöfer: Wichtigster Erfolgsfaktor ist die Ausrichtung aller Strategien, Konzepte und Maßnahmen an den Anforderungen des Unternehmens und dessen Geschäftsprozesse. Denn die Geschäftsprozesse generieren Umsatz und Ertrag – jedoch nicht gleichwertig und zu jeder Zeit. Daher ist eine differenzierte Bewertung der Ausfallerträglichkeit und Schutzbedarfe für alle Prozesse und Ressourcen die effektivste Form für die folgende Konzeption und Umsetzung eines angemessenen und durchgängigen Business Continuity Management. Eine entscheidende Rolle spielt dabei die Mitberücksichtigung der Themen Sicherheit und Risiko. Denn auch im Notfall soll ein angemessenes Sicherheits- und Risikoniveau erhalten bleiben.

Für den systematischen und strategischen Aufbau des Kontinuitätsmanagements wenden wir das dreidimensionale Pyramidenmodell nach Dr.-Ing. Müller an. So werden im Konzept alle Unternehmensfunktionen top-down berücksichtigt und anforderungsgerechte Maßnahmen umgesetzt. Dabei spielen die Ablauforganisation und die Abhängigkeiten zwischen Prozessen und Ressourcen eine entscheidende Rolle.

> „Ein zentrales Business-Continuity-Management-Tool stellt Daten, Abhängigkeiten und Dokumentationen bereit und ermöglicht in Krisensituationen die sofortige Ermittlung der Auswirkungen."

Weitere wichtige Erfolgsfaktoren sind eine zentrale, für das Business Continuity Management verantwortliche Organisationseinheit mit zusätzlichen dezentralen Verantwortlichen, eine einheitliche BCM-Dokumentation und in Notfallszenarien geübte Prozesse.

IT-DIRECTOR: *Welche Technologien sollten für das Kontinuitäts- und Krisenmanagement auf jeden Fall berücksichtigt werden?*

G. Neidhöfer: Ein zentrales BCM-Tool ist ab mittlerer Unternehmensgröße erforderlich. Es stellt Daten, Abhängigkeiten und Dokumentationen bereit und ermöglicht in Krisensituationen die sofortige Ermittlung der Auswirkungen. Gleichzeitig dient es dem Nachweis beispielsweise von Notfallübungen. Entscheidend ist dabei, dass das Tool von den Geschäftsprozessen ausgeht sowie auch für Nicht-ITler selbsterklärend und durch das Unternehmen flexibel anpassbar ist. Nicht zuletzt muss das Tool auch in Notfällen arbeitsplatzunabhängig einsetzbar sein. <

ESTHER FUCHS, IS