IT-Risiken im Fokus

Nicht nur unmittelbar finanzielle Risiken müssen in einem Unternehmen kontrolliert werden, auch die Informations- und Kommunikationstechnologie braucht dringend kontinuierliches Risikomanagement.

von ulrich mattner* | werner.fritsch@informationweek.de

Informationstechnologie macht nur dann vieles einfacher, wenn sie reibungslos läuft. Bricht sie zusammen, steht alles still. Dies erlebten in jüngerer Vergangenheit auch Millionen Telekom-Kunden, als sich ihre Handys plötzlich aus dem Netz verabschiedeten. Notrufe zu Polizei, Rettungssanitätern und Pannendiensten gingen ins Leere. Geschäftsgespräche rissen ab. Dringende Nachrichten blieben auf der Strecke. Schuld war ein Softwarefehler im System zur Überwachung der Mobilfunkstationen.

Ob Industrie oder Finanzdienstleistung, Verkehr oder Gastronomie: In allen Branchen häufen sich Beispiele teilweise dramatischer Softwarepannen. Schon längst hängt fast jeder Geschäftsprozess von zwei Faktoren ab: von einer möglichst störungsfrei arbeitenden IT und einer IT-Abteilung, die auf jeden nur denkbaren Störfall vorbereitet ist. Angesichts dieser hohen Anforderungen ist es kein Wunder, dass die Informationstechnologie als Risikoquelle immer mehr in den Fokus des Risikomanagements gerät. »Bisher standen vor allem kommerzielle Risiken wie Forderungsausfälle und Insolvenzen im Mittelpunkt der Risikokontrolle«, berichtet Dr. Helmut Kriegelstein von der Managementberatung Insentis. »So wurden etwa Zahlungsausfälle nur als Folge von Zahlungsunfähigkeit berücksichtigt. Die kommerziellen Folgen von IT-Pannen stellen oft ein viel höheres Risiko dar als die Zahlungsunfähigkeit einzelner Debitoren.«

Größere Bedeutung der IT

Die parallel zur Bedeutung der IT wachsenden Risiken sind einer der Gründe, warum der Gesetzgeber dem Schutz gegen Systemausfälle eine immer höhere Bedeutung beimisst. Dies zeigen Gesetzesinitiativen wie KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmen), SOX (Sarbanes-Oxley Act) und Euro-SOX (8. EU-Abschlussprüfungsrichtlinie), die – wie auch das jüngst novellierte Datenschutzgesetz – die Sicherheit der IT zur Chefsache machen. Nach dem KonTraG haften Vorstand oder vergleichbare Organe persönlich, wenn sie zum Beispiel den Aufbau eines unternehmensweiten Früherkennungssystems für Risiken versäumt haben. Aus diesem Grund hat das Thema »Zuverlässigkeit der IT« inzwischen einen festen Platz auf der Vorstandsagenda jedes größeren Unternehmens.

Bei der Implementierung eines Früherkennungssystems gegen IT-Pannen profitieren viele Unternehmen vom Know-how externer Spezialisten. Kriegelstein meint dazu: »Das Wichtigste ist, der IT-Mannschaft im Unternehmen die Angst zu nehmen, sie würde zunehmend als Risikofaktor gesehen. Stattdessen kommt es darauf an, der Abteilung zu vermitteln, dass sie weiter an Bedeutung gewinnt. Je mehr die IT für den Geschäftserfolg ausschlaggebende Prozesse steuert, desto mehr gehört sie zur Kernkompetenz eines Unternehmens und desto mehr wirken sich IT-Pannen auf die Performance aus.« Dies nachhaltig zu kommunizieren und die IT-Mitarbeiter von ihrer bedeutenden Rolle im Unternehmen zu begeistern, gelinge externen Beratern zuweilen leichter als der Unternehmungsführung.

Ist die IT-Mannschaft des Unternehmens von der Notwendigkeit der Risikokontrolle überzeugt, erfolgt der nächste Schritt: Die Erfassung und Bewertung von

Risiken in geschäftskritischen IT-Systemen und -Prozessen. Erst dann geht es darum, risikomindernde Maßnahmen zu ergreifen.

Inventar der Risiken erstellen

Im Mittelpunkt des Risikomanagements steht das Risikoinventar. Es beinhaltet auch für die IT weit mehr als eine Aufzählung möglicher Störfälle und Ausfallrisiken. Für jedes IT-Risiko wird ermittelt, wie hoch die Wahrscheinlichkeit des Eintritts ist und welchen Schaden der entsprechende Störfall anrichten kann. Daraus ergibt sich das Risikopotenzial. Risiken lassen sich vergleichen und insbesondere nach der Höhe des potenziellen Schadens gruppieren. In das Ranking können weitere Kriterien – zum Beispiel die Anzahl betroffener Kunden oder Niederlassungen – eingebracht werden. Darüber hinaus listet das Inventar für jedes Risiko die Möglichkeiten zu dessen Minimierung auf. Zudem bewertet es, ob die Kosten, die dafür anfallen würden, unter wirtschaftlichen Gesichtspunkten vertretbar sind. Der Aufwand für das Erstellen eines IT-Risikoinventars ist mitunter beträchtlich.

»Bei einem Unternehmen mit 2500 Mitarbeitern kann dies ohne weiteres sechs bis neun Mannmonate dauern«, weiß Kriegelstein. Hinzu komme ein nicht unerheblicher Aufwand für die Abstimmung der kundenspezifischen Begrifflichkeiten und das Etablieren der Prozesse zur Risikominimierung. Noch vor Erstellung des IT-Risikoinventars gelte es, in Absprache mit dem Vorstand zwischen internen Mängeln und Risiken zu differenzieren. Unter Risiken versteht man in diesem Zusammenhang Ereignisse, die mit einer gewissen Wahrscheinlichkeit unverhofft in einem bestimmten Zeitraum auftreten und substanzielle Schäden für das Unternehmen verursachen.

Als interne Mängel klassifiziert werden hingegen Versäumnisse, die irgendwann zu einem Schaden führen, etwa wenn ein IT-Dienstleister trotz vertraglicher Zusage nicht regelmäßig die Daten seiner Kunden sichert. Unregelmäßige oder fehlende Restore-Tests stellen dagegen ein Risiko dar. Die Abgrenzung mag im Einzelfall schwierig sein, ist aber für die Zuständigkeiten von entscheidender Bedeutung. Die Beseitigung interner Mängel ist nicht Sache des Risikomanagements, sondern der Prozessverantwortlichen. Risiken zu steuern, ist Aufgabe des betrieblichen Risikomanagers.

Risiken erst bewerten, dann reduzieren

Die Liste der Punkte in einem IT-Risikoinventar reicht vom Bewerten der Anfälligkeit der Software- und Systemarchitektur über die Beurteilung der Sicherheit der Stromversorgung bis hin zum Risiko-Check aller betrieblichen Prozesse. Geprüft wird auch, wie schnell IT-Spezialisten eventuelle Schäden beheben und damit die Schadenshöhe begrenzen können. Gleiches gilt für die Frage nach Umgehungslösungen und Notfallplänen. Jedes Risiko muss möglichst genau und sorgfältig spezifiziert werden. Ist es oberflächlich beschrieben, können die Maßnahmen, die die Risiken minimieren sollen, nicht exakt darauf abgestimmt werden. Jedes dokumentierte Risiko löst einen unmittelbaren Handlungszwang aus. Es muss nachvollziehbar bearbeitet, das heißt bewertet und dann reduziert werden. Schuldhaftes Zögern wird als Vorsatz gewertet, für den der Vorstand unter Umständen persönlich haftet. Zur Reduzierung der Risiken gibt es meist mehrere Vorgehensweisen. Dazu gehören präventive Maßnahmen zur Verringerung der Eintrittswahrscheinlichkeit. Dies betrifft etwa die Wahl einer Systemarchitektur, die sich durch hohe Verfügbarkeit und Verlässlichkeit auszeichnet und am Industriestandard orientiert. Korrektive Maßnahmen sollen während einer IT-Panne die Schadenshöhe begrenzen. Hierzu zählen unter anderem die Bereithaltung von Ersatzsystemen und Notfallplänen für die IT-Abteilung. Risiken lassen sich nur dann kontrollieren, wenn auch der Einsatz von Ressourcen wie Personal, Investitionsvolumen und Folgekosten unter Kontrolle ist. Dies gewährleistet der betriebliche Risikomanager.

Auf die Kompetenz des Risikomanagers muss sich der Vorstand verlassen können.

Einmal auf den Weg gebracht, wird das IT-Risikomanagement zum kontinuierlichen Prozess: Neue Risiken kommen hinzu, ältere fallen weg oder ändern sich. Schutzvorkehrungen sind umzusetzen und zu bewerten, da sie Eintrittswahrscheinlichkeiten oder potenzielle Schadenshöhen verändern. Der betriebliche Risikomanager schreibt das Risikoinventar kontinuierlich fort, entscheidet über weitere Schutzvorkehrungen, kontrolliert sein Budget und berichtet an den Vorstand. Auf seine Kompetenz muss sich die Unternehmensführung verlassen können, sonst gerät sie in Gefahr, persönlich für IT-bedingte Schäden haften zu müssen.

Gegen alles und jedes kann auch ein noch so gewissenhafter Risikomanager ein IT-System allerdings nicht schützen. So wurde der Großcomputer der Havard-Universität einmal von einem Risiko lahm gelegt, mit dem keiner gerechnet hatte. Einer Motte war es gelungen, alle Barrieren zu überwinden. Schließlich gelang es einer Wissenschaftlerin, das Insekt aus dem Rechensystem zu entfernen. Seitdem sind sich die IT-Verantwortlichen in Harvard mehr denn je darüber klar, dass selbst kleinste Ursachen eine große Wirkung haben können. ■

* **Ulrich Mattner** ist freier Journalist in Frankfurt am Main.