



# Leadership

Das IT-Magazin von Hewlett-Packard Schweiz

1/04

## 4 Risik Management

Tools und Strategien zur Risikokontrolle im Unternehmen

## 10 Verfügbarkeit

Wie Swisscom Mobile dem IT-Service-Gedanken nachlebt

## 12 Adaptive Enterprise

HP Utility Data Centers revolutionieren die IT



## \*Frank Romeike

ist Gründer und Initiator von RiskNET ([www.risknet.de](http://www.risknet.de)), dem führenden deutschsprachigen Internetportal rund um das Thema Risikomanagement, und gleichzeitig Herausgeber von RISKNEWS, dem Fachmagazin für Risikomanagement. Frank Romeike hat ausserdem einen Lehrauftrag an der FHTW Berlin (Schwerpunkt: Innovatives Controlling; Risikomanagement) und trainiert, coacht und berät seit mehr als zehn Jahren Unternehmen aller Branchen und Unternehmensgrößen. Zuvor war er Risk Manager bei einem multinationalen IT-Konzern, wo er den gesamten Risk-Management-Prozess verantwortete.



Proaktives Risk Management sorgt für sichere Landungen: Im freien Markt wirkt eine gelebte Risiko- und Kontrollkultur wie ein Gleitschirm. Risiken erkennen und erfassen verhindert den unkontrollierten Sinkflug.

# Vom Wert des proaktiven Risk Mana

Frank Romeike, Risknet.de\*

**Unternehmerisches Handeln erfolgt stets auf unsicherem Boden. Damit er nicht unter den Füßen wegbricht, ist ein proaktives Risk Management vonnöten. Das steigert nicht nur den Wert eines Unternehmens, sondern erweist sich in Krisenzeiten als Rettungsboot.**

Unternehmer müssen für den Erfolg etwas riskieren, ohne gleich als Hasardeure aufzutreten. Denn nur ein kalkuliertes Risiko führt zu einem nachhaltigen Erfolg. Sie müssen sich deshalb mit kalkuliertem Risiko im Markt bewegen. Was früher häufig aus dem Bauch heraus erfolgte, wird heute in verschiedener Ausprägung von Hard- und Software erledigt – das Abschätzen von Risiken und das Abstützen IT-getriebener Business-Prozesse. Für Unternehmen werden die optimale Informationsverteilung sowie die Integration der Unternehmensprozesse und der IT zunehmend zum strategischen Erfolgsfaktor.

Die technische Abhängigkeit der Kernprozesse von der IT in der Wertschöpfungskette nimmt rapide zu – und damit auch das IT-bezogene Risiko. Die IT-Prozesse in einem Unternehmen unterstützen auf der einen Seite die Kernprozesse eines Unternehmens und reduzieren dadurch auch die Unternehmensrisiken. Gleichzeitig beinhaltet die Informationstechnologie wiederum ein neues Risikopotenzial. Vor diesem Hintergrund steigt die Bedeutung eines proaktiven IT Risk Management als Bestandteil eines integrierten und unternehmensweiten Risk Management deutlich.

**Mit beschlagener Frontscheibe** In den vergangenen Jahren wurde Risikomanagement häufig eher reaktiv bzw. retrospektiv und situativ betrieben. Viele Unter-

nehmen verhalten sich wie ein Autofahrer, dessen Frontscheibe beschlagen ist und der deshalb mit Hilfe des Rückspiegels fährt. Risikomanagement sollte jedoch proaktiv, also vorausschauend, ausgerichtet sein. Mehr als 75 Prozent der Fortune-1000-Unternehmen sind nicht ausreichend auf ernsthafte Störungen ihrer kritischen Geschäftsprozesse vorbereitet. In einer aktuellen Studie hat die International Data Corporation (IDC) herausgefunden, dass 90 Prozent der europäischen Unternehmen mit einem Umsatz von mehr als 100 Millionen Euro keinen Business Continuity Plan ausgearbeitet haben. Die Diskrepanz zwischen den Anforderungen an die Geschäftskontinuität und den praktischen Sicherheitsvorkehrungen kann auf vielfältige Ursachen zurückgeführt werden. Einerseits sind Investitionen im Bereich IT-Security nicht messbar und nachvollziehbar. Ein integriertes (IT) Risk Management ist häufig nicht oder nur stellenweise umgesetzt.

Ein effizient funktionierendes Risikomanagement und eine gelebte Risiko- und Kontrollkultur werden aber immer mehr zu wesentlichen Erfolgsfaktoren für Unternehmen. Nur die Unternehmen, die ihre Risiken effizient steuern und kontrollieren, werden langfristig erfolgreich sein und den Unternehmenswert steigern. Dazu werden sie indirekt gezwungen: Neben dem sich durchsetzenden Management-System der «Corporate Governance» stellen insbesondere die neue Basler Eigenkapitalvereinbarung (besser bekannt unter dem Begriff «Basel II») sowie das Pendant für die Versicherungen (Solvency II) höhere Anforderungen an das Control-

ling und Risikomanagement von Unternehmen. Die Fremdkapitalfinanzierung für Unternehmen mit einem effizienten und integrierten Risikomanagement und einem «guten Rating» wird sich tendenziell verbilligen. Die Höhe des erforderlichen Eigenkapitals wird sich stärker an den individuellen Risiken der Kredite und der Höhe der operationellen Risiken der einzelnen Bank orientieren. Mit den entsprechenden Auswirkungen auf die IT: So haben etwa der Basler Ausschuss für Bankenaufsicht (BCBS = Basle Committee on Banking Supervision) sowie die US-amerikanische Währungsaufsichtsbehörde (OCC = Office of the Comptroller of the Currency) Richtlinien zum IT-Risikomanagement der Banken erlassen.

**Fazit:** Es wird immer schwieriger, ja beinahe unmöglich, mit Hilfe von «unternehmerischer Intuition» und reaktiven Steuerungssystemen die Komplexität der Prozesse und Risiken zu erfassen und zu analysieren.

**Risiken erkennen und erfassen** Das operative Risk Management beinhaltet den Prozess der systematischen und laufenden Risikoanalyse der Geschäftsabläufe. Die Identifikation der Risiken kann je nach Unternehmen aus verschiedenen Perspektiven erfolgen; beispielsweise auf der Ebene der Risikoarten (leistungswirtschaftliche, finanzwirtschaftliche, externe Risiken etc.), der Ebene der Prozesse (Projekte, Kern- und Unterstützungsprozesse etc.), der Geschäftsfelder (Dienstleistungen, IT Services,



Corbis



DHL Luft

HP sichert die Geschäfte von DHL zu Lande, zu Wasser und in der Luft.

## DHL setzt auf Business Continuity Services von HP

[sandro.bernardi@hp.com](mailto:sandro.bernardi@hp.com), Business Continuity Services

**Extreme Fremdeinwirkungen wie Naturkatastrophen können Unternehmen in den Ruin treiben. DHL als führender Anbieter von Transport- und Logistikdienstleistungen hat sich gegen existenzbedrohende Ausfallzeiten abgesichert: Der Business Continuity Service von HP gewährleistet die Weiterführung der Geschäfte, wie die Beispiele Basel und Brüssel zeigen.**

Sollte eine Stadt von einem Erdbeben erschüttert und ein DHL-Gebäude dabei schwer beschädigt werden, so käme das operative Geschäft des stark IT-abhängigen Konzerns praktisch zum Stillstand, die Existenz wäre gefährdet. Dirk Herbots, CIO des Global Coordination Center am DHL-Hauptsitz in Brüssel, schildert die Problematik aus Sicht des Kunden: «Als IT-Verantwortlicher möchte man am liebsten eine Kopie der kompletten Infrastruktur anlegen, um notfalls darauf zurückgreifen zu können – was aus Kostengründen natürlich eine Utopie ist.»

Mit dem Business Continuity Service (BC) bietet HP da genau die gewünschte und erforderliche kostenoptimierte Lösung. Gemeinsam mit dem Kunden werden die Geschäftsprozesse analysiert und kritische Applikationen bestimmt. Bei der anschließenden Konzeption einer Lösung wird definiert, welche maximalen Ausfallzeiten das Unternehmen verkraften könnte und welche damit verbundenen Kosten der vorgeschlagenen Business-Recovery-Lösung vertretbar sind.

**Mobiles Rechenzentrum** ... Um optimal auf die individuellen Bedürfnisse eingehen zu können, bietet HP seinen Kunden im Bereich BC-Service die unterschiedlichsten Möglichkeiten. So wurden für DHL aufgrund der spezifischen Anforderungen des Unternehmens gleich zwei verschiedene Lösungen ausgearbeitet. Im Global Coordination Center in Brüssel, wo Marketing, Sales und Business Intelligence domiziliert sind und man sich für die gründliche Recovery schon mal ein paar Tage Zeit nehmen kann, hat sich der Kunde für ein mobiles Rechenzentrum entschieden: HP fährt im Notfall mit einem komplett ausgestatteten Service

Center vor, das über einen eigenen Generator verfügt und deshalb auch eingesetzt werden kann, wenn der Strom für längere Zeit ausfällt oder das Gebäude nicht mehr genutzt werden kann. Das mobile Service Center steht innert 48 Stunden vor Ort. Im gleichen Zeitraum werden die Backup-Daten geliefert und direkt eingespielt.

... oder «Ship to Site»-Lösung Bei den operativen Centern von DHL sind Ausfälle natürlich viel kostspieliger. Für diese Standorte hat DHL deshalb die «Ship to Site»-Lösung gewählt. Dabei wird die im Continuity Plan definierte heterogene Server-Landschaft innerhalb von 24 Stunden geliefert; innert 48 Stunden muss die gesamte Infrastruktur wieder in Betrieb sein. Christian Würger, IT-Leiter von DHL Basel, fasst die Erfahrungen mit HP zusammen: «Die Projektbegleitung war sehr gut, und dass HP bis ins Detail auf unsere spezifischen Bedürfnisse einging, war besonders hilfreich.» Mitentscheidend bei der Evaluation war für Würger auch, dass HP als Generalunternehmer auftreten konnte, dass DHL folglich einen einzigen Ansprechpartner hat. Hätte er dieses Projekt noch einmal zu begleiten, so würde sich Würger wieder für HP entscheiden. Und Dirk Herbots vom Global Coordination Center in Brüssel schliesst sich dem Urteil an: «HP hat sich für uns als perfekte Wahl erwiesen.»

### Die Geschäftsidee der glorreichen drei

DHL ist ein Paket- und Brief-Expressdienst, dessen Bezeichnung sich zusammensetzt aus den ersten Buchstaben der Nachnamen der Gründer Adrian Dalsey, Larry Hillblom und Robert Lynn. Die drei nahmen ihre Geschäftstätigkeit im Jahr 1969 auf, indem sie in San Francisco Schiffsbriefe entgegennahmen und diese per Flugzeug persönlich in Honolulu abliefern.

Seit 2002 gehört DHL zum Konzern Deutsche Post World Net und ist derzeit der weltweit grösste Expressversender. Unter dem Namen DHL arbeiten mittlerweile auch der Schweizer Logistikkonzern Danzas (gehört zur Deutschen Post) und der Paketversand der Deutschen Post.

# gement

Produktion etc.), der Applikationen sowie der IT-Infrastruktur (Betriebssysteme, Standardsoftware, Netzwerk etc.). In der Praxis wird man erkennen, dass Risikokategorien nicht losgelöst voneinander erfasst werden können, sondern vielmehr durch positive und negative Rückkoppelungen miteinander verbunden sind. Bei der Identifikation von operationellen Risiken sollte man sich primär an den Geschäftsprozessen orientieren und die möglichen Risiken durch und auf die IT analysieren.

**Risiken kartografieren** Sind die Risiken erkannt, so erfolgt in der nächsten Phase der Risikobewertung eine Quantifizierung der Risiken hinsichtlich des Erwartungswerts. Der Erwartungswert bestimmt sich aus der Multiplikation der Eintrittswahrscheinlichkeit mit dem Schadensausmass (Risikopotenzial, Tragweite). Die Risikobewertung zielt darauf ab, die Risiken hinsichtlich ihres Gefährdungspotenzials in eine Rangordnung zu bringen sowie ein unternehmensindividuelles Risikopotenzial (auch Risikolandschaft, Risikomatrix oder Risk Map genannt) abzubilden. So erhält der Unternehmer im Zusammenspiel mit verschiedenen Simulationsmethoden ein aktuelles Bild seines Gesamt-Risikopotenzials. Darin nimmt die IT als unterstützende Kraft vieler Business-Prozesse eine wichtige Funktion ein. Es leuchtet ein, dass sich hier viele Risiken reduzieren lassen – ebenfalls mit technischen Mitteln. Zur Hängeregistratur anstelle einer Datenbank zurückzukehren kann sich nämlich kein Unternehmer mehr leisten.

# «Risikokontrolle ist sehr wichtig»

Ob Flutwellen oder Virenschäden: Risiko-Experte Bruno Porro sieht in der IT ein Mittel zur Kontrolle von Risiken. IT Governance ist für ihn zentral.

**Die Sensibilität für Risiken ist heute allgemein sehr hoch, die Qualität des Risikomanagements indessen variiert. «Leadership» hat sich mit Bruno Porro über das Thema unterhalten. Porro ist beim Rückversicherungskonzern Swiss Re Chief Risk Officer, Leiter der Division Risk & Knowledge und Mitglied des Geschäftsleitungsausschusses.**

**«Leadership»:** Bruno Porro, in welche Richtung haben sich die Risiken in den vergangenen Jahren verlagert?

**Bruno Porro:** Vor 25 Jahren hatten wir es hauptsächlich mit Haftpflichtfällen in den USA – zum Beispiel Asbest – und mit Sachschäden zu tun. Letztere, verursacht durch Naturgewalten, wird es immer geben. Heute sind wir aber auch ganz anderen Bedrohungen ausgesetzt: Pharmazeutische Schäden ziehen Massenklagen nach sich, Fettleibige machen die Lebensmittelindustrie für ihr Problem verantwortlich oder es tauchen unbekannte Viren auf, um nur einige der neuen Gefahren zu nennen.

**Wo sehen Sie die grössten Risiken?** Einerseits gibt es ganz bestimmte Szenarien: Beispielsweise könnte eine Insel im Atlantik versinken und eine Flutwelle auslösen, die die ganze Ostküste der USA verwüsten würde. Auch wenn die Wahrscheinlichkeit von solchen Katastrophen sehr klein ist, müssen wir immer mit ihnen rechnen. Das wissen wir nicht erst seit dem Einsturz des World Trade Centers. Andererseits stellen Naturkatastrophen grosse Risiken dar, weil die Bevölkerungs- und Versicherungsdichte sowie die Schadenempfindlichkeit in gefährdeten Gebieten kontinuierlich zunehmen. Erdbeben oder Orkane können enorme Schäden anrichten.

**Können Sie einen solchen Schaden, beispielsweise ein Erdbeben in Kalifornien, beziffern?** Die Schätzungen ge-

hen in Richtung 100 Milliarden Dollar versicherte Schäden. Das wäre rund zweieinhalb Mal so viel wie im Fall des World Trade Center.

**Wie steht es um das Risikomanagement innerhalb von Firmen und Konzernen?** Die Unternehmen sind sich bewusst: Wer aufgrund falscher Risikoeinschätzungen den Betrieb über längere Zeit stilllegen muss, verliert seinen Marktanteil und ist als Folge davon weg vom Fenster. Die Sensibilität für alle möglichen Arten von Risiken ist deshalb heute sehr hoch.

**Wie zuverlässig sind die Risikoanalysen von Unternehmen?** Wird ein Risk Report von Experten erstellt, die wir kennen und denen wir vertrauen, gibt es keine Probleme. Sind wir uns dessen nicht sicher, machen wir selbst eine Analyse.

**Wann ist das der Fall?** In der Pharmaindustrie etwa schauen wir uns die ganze Produktpalette an; mit Blick auf allenfalls drohende Sammelklagen in den USA ist das unabdingbar. Wir wollen die in einem Medikament enthaltenen Wirkstoffe kennen. Erhalten wir die Informationen nicht oder nur teilweise, so ist der Ausschluss gewisser Produkte möglich. Denn für jede Art von Risikomanagement gilt: Je besser ich das Risiko kenne, desto eher weiss ich, mit welchen Konsequenzen und welchen finanziellen Auswirkungen im Schadenfall zu rechnen ist.

**Wie wichtig ist Risikomanagement im IT-Bereich?** Die IT ist heute das Rückgrat eines Unternehmens, entsprechend wichtig ist die Einschränkung der Risiken. Bedauerlich ist, dass die IT-Sicherheit den Attacken von Hackern oder dem Viren-Schauer aus dem Internet nie zuvorkommen kann, sondern mit den Abwehrmassnahmen dauernd hinterherrennt. Zentrale Bedeutung kommt der IT Governance zu, wobei die Risikokontrolle ein wichtiges Element darstellt. Einerseits muss die IT selbst geschützt werden, andererseits mit ihrer Hilfe der gesamte Businessprozess. Auf der Basis einer konsequenten Umsetzung der IT-Governance hilft IT als Ganzes Unternehmen ihre Geschäftsrisiken besser abzuschätzen.

**Wo steht das Risikomanagement in der Schweiz heute generell?** Der Standard ist gut, die Sicherheitsphilosophie ebenfalls. Der Haken ist, dass effizientes Risikomanagement Geld kostet. Und falls der Rotstift eingesetzt werden muss, wird auf diesem Gebiet zuerst gespart.

**In welchen Ländern bestehen die höchsten Risiken?** Viele Industrien haben ihre Produktionsstandorte in Ländern wie Tschechien, Taiwan oder China verlagert. Dort ist das Risikomanagement in den neuen Fabriken geradezu vorbildlich, genauso wie die dort hergestellten Produkte. Aber Vergleiche sind schwierig. Massgeblich sind nicht Länder oder Kontinente, sondern die einzelnen Branchen. Die grössten Risiken bestehen dort, wo Strukturänderungen zu einem starken Preiskampf führen und die Margen auf ein Minimum schrumpfen.



Im Windkanal des Marktes werden Firmen geformt.

**Adapter**

## Voll im Wind

**Der Mensch ist kein Meisterwerk der Aerodynamik. Zu viel Fläche, zu wenig Tiefe beim aufrechten Gang. Der Gegenwind wird zum Hindernis. Unwillkürlich adaptieren wir uns an die Windlage, senken den Kopf, neigen den Körper in Richtung des Gebläses. Im Windkanal des Lebens finden wir unbewusst stets die beste Form.**

Das Formel-1-Team von BMW-Williams hat es da etwas schwerer. Es muss die feste Form seiner Boliden so gestalten, dass die Luftwirbel im Rennen nicht wie eine Bremse wirken. Den Aerodynamik-Fachleuten des Rennstalls stehen zwei HP Alpha Server Supercomputer sowie ein Linux-Cluster für die Analyse und Berechnung der Modelle zur Verfügung. «Unsere Entwicklungszeit hat sich halbiert», sagt Aerodynamik-Spezialist Naethan Eagles. «Anpassungen haben wir heute in wenigen Stunden erledigt.» Die Wirkung: Der BMW-Williams FW26 weist eine völlig neu geformte «Schnauze» auf.

Möglichst wenig Luftwiderstand bei gleichzeitig möglichst grossem Abtrieb für maximale Bodenhaftung: etwas, das jede Firma, ob klein oder gross, anstrebt. Denn im Markt herrscht Gegenwind aus allen Richtungen. Schnell vorankommen, die Nummer 1 im Markt sein und sich nachhaltig entwickeln – das sind die Ziele jedes Unternehmens.

HP hat es sich zur Aufgabe gemacht, Unternehmen mit Technologien und Services und Lösungen beim Streben nach der optimalen geschäftlichen Aerodynamik zu unterstützen. Denn ähnlich wie sich der menschliche Körper den Kräften der Winde beugt, passen sich Firmen den Kräften des Marktes an. Dass sich diese Fitness in Sachen Flexibilität lohnt, zeigt gerade BMW-Williams. Der Computer macht den Wind sichtbar. Er stellt die Luftströmungen bildlich dar und zeigt, warum der eine Frontflügel besser als der andere funktioniert.

Unternehmen, die Widerstände nicht nur spüren, sondern auch sehen, überwinden sie leichter. HP macht sie sichtbar: Unternehmen werden agil. Wind bewegt. Und schafft Form. Das weiss auch das BMW-Williams Team und hat deshalb einen neuen 30 Millionen Dollar teuren Windkanal gebaut. Denn der Kampf um die schlüpfrigste Form dauert an – Runde um Runde.

**Otto Prozessor**