

# Strategisches Risikomanagement auf der „Insel der Seligen“?

Von Ines M. Kaldas

*Leadership*, Wirtschaftsforum der Führungskräfte, April 2008 (in print)

**Papst Paul VI. wird in Bezug auf Österreich der Ausdruck „Insel der Seligen“ in den Mund gelegt; das ist eine zwar liebenswürdige, letztendlich aber eher fatale Begriffszuschreibung, weil seither hierzulande die Meinung vorherrscht: „Es kann uns eh nix passieren!“ Zweifellos ist es nicht opportun, von (potentiellen) Katastrophen zu reden, aber man kann die Augen auch nicht davor verschließen - es wäre Ausdruck höchster Unprofessionalität.**

Soweit eine Kurzdiagnose zur österreichischen Befindlichkeit, auch wenn man sie nicht auf alles und jedes umlegen darf. Doch kehren wir zur Frage in der Überschrift zurück. Ohne in Paranoia oder Hysterie zu verfallen, muss die kurze und eindeutige Antwort auf die eingangs gestellte Frage „**Ja**“ lauten. Österreich, und vor allem die österreichische Wirtschaft, sind Teil eines vernetzten, gesamteuropäischen Systems, bei dem es nicht möglich ist „sich abseits zu stellen“. Erinnern wir uns an BSE, SARS, Stromausfälle, oder auch Überschwemmungen und Hochwasser, wodurch unzählige Produktionsbetriebe zumindest temporär zum Stillstand kamen. Krankheitsbedingte (etwa im Falle einer Pandemie) oder durch Streiks bedingte Ausfälle von Schlüsselpersonal und Schlüsselfunktionen können ein Übriges tun, Unternehmen in ihrer Leistungsfähigkeit zu beeinträchtigen und „supply chains“ (= Logistikketten) lahmzulegen. Das nun folgende Beispiel bezieht sich auf einen konkreten Fall aus der europäischen Infrastruktur – ist aber in seiner Signalwirkung und in den aufgedeckten Planungs- und operativen Mängeln beispielgebend für **alle** Industriezweige:

Es war der 4. November 2006. Im Netz des deutschen Energiekonzerns E.ON wird eine Höchstspannungsleitung über die Ems in Norddeutschland abgeschaltet, um ein Kreuzfahrtschiff passieren zu lassen. Etwa eine halbe Stunde später kommt es zu einem der größten Stromausfälle Europas, von den Niederlanden bis nach Italien und Spanien. Was war passiert? Andere europäische Netzbetreiber waren nicht informiert worden. E.ON Mitarbeiter hatten die potentiellen Auswirkungen unterschätzt – es kam zu einer Kettenreaktion. Der nachfolgende Expertenbericht der EU Kommission stellte gravierende Sicherheitsmängel fest. Investitionen in die Zuverlässigkeit und den Netzbetrieb seien „unzureichend“ gewesen. Daher sei die Versorgungssicherheit nicht gegeben. Die EU Kommission pochte auf eine Entflechtung der Netzbetreiber. Gerade dieser Tage erfahren wir, dass sich E.ON von seinem Übertragungsnetz trennen wird.

Hier die Interpretation zu diesem „case“: Es gab gravierende interne Mängel im Krisenmanagement, sogenannte mission-critical functions (= Schlüsselfunktionen) waren nicht ausreichend abgesichert, trigger (= klar definierte Auslöser, z. B. von Alarmplänen) und back-up Funktionen nicht rasch genug einsatzfähig, die interne Kommunikation, aber auch die externe Kommunikation mit europäischen Businesspartnern war unzureichend. Die Folgen, wie wir sehen, sind schwerwiegend.

Zurück nach Österreich. Man muss den Österreichern allerdings auch bescheinigen, dass das operative Management im Katastrophenfall auf einem hohen technischen und organisatorischen Niveau funktioniert: Feuerwehr, Rettung, Polizei und andere (freiwillige) Einsatzkräfte sind in hohem Maße effektiv.

Aber wie sieht es mit der strategisch-vorbeugend orientierten Gesamtsicht bezogen auf das **einzelne Unternehmen** aus? Und **vor allem**, wie sind Krisenmaßnahmen von Unternehmen **intern** (zwischen headquarters und Teilbereichen, oder zwischen essentiellen Teilbereichen) - aber auch nach außen **mit dem Krisenmanagement der öffentlichen Hand** (Blaulichtorganisationen, Zivilschutz, Katastrophenreferenten u.a. Behörden) für einen optimierten Einsatz verschalten und integriert? Hier findet in den letzten Jahren ein in den USA entwickeltes Konzept in Europa immer mehr Beachtung, welches sich dem Verständnis eines „**all hazards approach**“ (= für alle Krisenfälle gewappnet zu sein) verpflichtet fühlt, im Fachjargon „**Business Continuity Planning**“ (**BCP**) genannt. Was verbirgt sich nun hinter diesen Worten, die in unseren Breitengraden bis dato eher nur „Eingeweihten“ ein Begriff sind ?

Ein **umfassendes und strategisches Business Continuity Planning (BCP)-Programm** stellt einen „**all hazards approach**“ dar, der in einem systematischen Ansatz einen umfassenden Grad an Krisenvorsorgemaßnahmen für alle risikoanfälligen Aspekte eines Business einführt. **Das Ziel** eines umfassenden strategischen BCP-Programmes ist es, **die Kontinuität aller mission-critical functions in einem Unternehmen zu wahren** und so die **organisatorische Widerstandsfähigkeit zu stärken**. Als mission-critical functions bezeichnet man jene Funktionen, die für die grundsätzliche Betriebsfähigkeit eines Unternehmens unverzichtbar sind. Das bezieht sich auf alle Management- Funktionen wie auch auf die Funktionen des operativen Geschäftes und deren support functions. All das wird auf „International Best BCP- Practices“ standardisiert. Nur so kann sich die österreichische Wirtschaft gegen neu auftretende Bedrohungen wappnen.

Das heißt konkret, dass der Begriff „all hazards approach“ auch und vor allem unter der Zukunftsperspektive „neuartige Bedrohungen“ zu verstehen ist. Darunter fällt ein weites Spektrum an potentiellen betriebsinternen, als auch externen Bedrohungen: z.b. Naturkatastrophen verursacht durch sich verändernde klimatische Bedingungen, und Bedrohungen durch ansteckende Human- und landwirtschaftliche Pathogene, die sich in einer hochmobilen Welt bekanntlich exponentiell rascher ausbreiten. Darunter fallen ebenso technisches Versagen und durch Menschenhand verursachte Katastrophen, wie beispielsweise Unfälle in der Gefahrgüterindustrie, Sabotage, transnationaler Terrorismus, und ganz besonders Bedrohungen aus Makroverkettungen - nicht nur in Bezug auf „cyberthreats“ und Datensicherheit, sondern mit besonderem Augenmerk auf die Logistikketten.

Neuartige Bedrohungen unterscheiden sich in ihren Dimensionen maßgeblich von den bisher gewohnten, sozusagen traditionellen Notfällen. Damit ergibt sich ein Potential für Panik unter Mitarbeitern, Entscheidungsträgern, aber auch in der Öffentlichkeit. Das könnte zu wirtschaftlicher und politischer Destabilisierung führen, weil grundlegende Strukturen nicht mehr funktionieren.

Um dem entgegenzutreten, braucht die österreichische Wirtschaft robuste BCP-Programme für ihre Betriebe und Industrien. Dadurch schafft man **pro-aktive** Effizienzerhöhung in allen mission-critical functions und damit eine **Erhöhung der operativen Widerstandsfähigkeit** eines Unternehmens **gegenüber einem weiten Spektrum an potentiellen internen und externen Bedrohungen**. Damit werden Mitarbeiter, Prozesse und Unternehmenswerte gesichert und Stillstandzeiten verringert. Umfassende Maßnahmen zur Absicherung der betrieblichen Infrastruktur sowie IT- und Datensicherheit sind ebenso selbstverständliche Voraussetzungen innerhalb eines wohl konzipierten BCP-Programmes. Umfassende Kommunikationspläne und klare Schnittstellendefinitionen gewährleisten essentielle

Kooperationsschienen sowohl innerhalb des Betriebes, als auch nach außen hin, etwa mit den Einsatzkräften der öffentlichen Hand oder mit den Medien. Spezielle Appendices, wie Pandemiepläne („was tun, wenn prognostizierte 20-60% der Belegschaft oder Schlüsselpersonal krank sind?“) können angegliedert werden. Komplikationen, die verdeutlichen was passiert, wenn derartige proaktive Maßnahmen fehlen traten beispielsweise vor einigen Wochen in Deutschland während der groß angelegten Streiks auf. Desgleichen vor einigen Jahren während des Vogelgrippeausbruches in Norddeutschland, als Desorientierung der zuständigen Stellen auf allen Ebenen zu mangelnder Koordination und peinlichen Widersprüchen in den Medien führten.

Es würde, so pflegt man für gewöhnlich zu schreiben, den Umfang eines Beitrages sprengen, ein bestimmtes Konzept im Detail auszuführen. Im konkreten Fall des BCP trifft dies in besonderer Weise zu, da es ein komplexes Gesamtkonzept aus **systematischen und standardisierten Methoden, Instrumenten und Techniken** ist, aber auch eine Fülle von „intangible elements“ umfasst: der „**people factor**“, die Motivation von Top-Management, Vorsorge für das Unternehmen zu treffen, ist genauso Teil des Systems wie die Motivation und Schulung von Schlüsselpersonal für den Krisenfall und danach. Ein strategisches BCP heißt aber auch Loszulösung von funktionell isolierten „organisatorischen Silos“ – hin zu einer „**unified planning platform**“, der Basis für **robuste organisatorische Widerstandsfähigkeit!**

Weitere Informationen unter [www.kaldas-consulting.com](http://www.kaldas-consulting.com).

**Dr. Ines M. Kaldas, MPA** forschte nach dem Doktoratsstudium (Salzburg) an den Universitäten Chapel Hill und Stanford zu Neuroanatomie, Neurochemie und Biotechnologie. Ausgezeichnet mit dem National Research Service Award des US Institute on Aging, 1999 Master of Public Administration (Harvard); 2001 Mitglied des BW-Expertenrates im BM für Landesverteidigung, Konsultantin und Korrespondentin für transatlantische Sicherheitspolitik, Zivilschutz. 2006 Gründung der Kaldas Consulting GmbH – Zentrum für Krisen- und Konsequenzmanagement, einer Berater-Plattform internationaler Spitzenkräfte aus Sicherheitspolitik, Zivilschutz, IT-Sicherheit.