Nachgefragt

Wie fit ist Ihr Krisenmanagement?

Die Katastrophe in Japan hat es wieder einmal gezeigt: Auch die besten Sicherheitsmassnahmen haben ihre Grenzen. Doch wie lässt sich das viel zitierte «Restrisiko» noch weiter minimieren? Und machen sich Unternehmen über einen GAU in ihrem Haus überhaupt Gedanken?

VON THOMAS BERNER

Die Fukushima-Katastrophe bewegt und hat viele Risikodiskussionen wieder in Gang gesetzt. Dies stellt auch Sicherheitsexperte Beda Sartory, Geschäftsführer von GU Sicherheit AG in Wil SG, fest. Neu ist ein erhöhtes Risikobewusstsein in Unternehmen für ihn jedoch nicht: «Die Risikosensibilisierung in Unternehmen hat schon vor zwei bis drei Jahren verstärkt eingesetzt. Allerdings wurden die Risiken zu oft nur isoliert betrachtet. Fukushima zeigt nun, wie sich einzelne Risiken unglücklich verketten können. Und gerade diesbezüglich beginnen nun viele Unternehmen umzudenken.»

Krisen haben nur kurzen Lerneffekt. Ins gleiche Horn stösst auch Uwe Müller-Gauss, Inhaber von Müller-Gauss Consulting in Hinwil. «Anfragen für Beratungen nehmen zu, die Leute sind aufgeschreckt», so seine Feststellung. Allerdings halte dieser Effekt nicht für lange an. «Die Lernfähigkeit aus Krisen ist leider schlecht», so Müller-Gauss. «Trotz Erfahrung etwa aus der Finanzkrise von 2008 geht das Leben genauso weiter wie vorher. Man vergisst dabei, dass ein solches Ereignis jederzeit wieder auftreten kann.»

Risikomanagement: Viel ist oft noch nicht genug. Doch nicht nur die unglückliche Verkettung mehrerer Umstände zeigt sich exemplarisch anhand der Katastrophe in Japan. «Auch die Krisenkommunikation wird oft vernachlässigt», moniert Sartory. Er nennt folgendes Szenario: «Ein Unternehmen ist gerade dabei, einen Grossauftrag an Land zu ziehen. Nun kommt es zu einem Unfall im Betrieb. Wie muss nun ein Unternehmen kommunizieren, damit es trotz dieses Ereignisses seine Reputation nicht verliert?» Was eine ungenügende Informationspolitik bewirken kann, zeigt sich gegenwärtig am Beispiel von Tepco in Japan oder vor ein paar Monaten bei BP während der Ölkatastrophe im Golf von Mexiko. Beide Unternehmen sind beileibe keine KMU und hätten eigentlich die Ressourcen für eine adäquate Krisenkommunikation.

Jedem Unternehmen seine Risikopolitik. Beda Sartory rät allen Unternehmen zu einem integralen Risikomanagement. «Es geht darum, die Risiken zu erkennen, diese zu beurteilen und die möglichen Auswirkungen festzustellen. Bei unseren Schulungen weisen wir die Unternehmen zudem explizit auf die Möglichkeit hin, dass sich mehrere Risiken auch verketten können. Jedes Unternehmen sollte neben einem praxisgerechten vorbereiteten Krisenmanagement auch auf die Krisenkommunikation gegen «innen» und «aussen» vorbereitet sein. Es gilt, eine unternehmenseigene Risikopolitik zu formulieren und sich daran zu halten.» Sartory warnt allerdings auch vor einer zu detaillierten Notfallplanung. «Eine grobe Planung reicht in der Regel aus, und es empfiehlt sich, mit Checklisten und vorbehaltenen Entschlüssen zu arbeiten.»

Das Risikomanagement in KMU hält Uwe Müller-Gauss sogar für eher besser ausgebaut als in Grossunternehmen. Ein Inhaber, der viel eigenes Geld in seine Firma hineingesteckt hat, hat ein lebhaftes Interesse daran, dass das Unternehmen überlebt. «Firmen, die im Besitz der Geschäftsleitung sind, sind häufig besser abgesichert als andere», so die Einschätzung von Müller-Gauss.

Das ominöse Restrisiko. Katastrophen lassen sich nun mal nicht kalkulieren. Eine absolute Sicherheit gibt es nicht. Jedes Unternehmen muss sich klar darüber werden, welche Risiken es bereit ist, zu tragen. Uwe Müller-Gauss: «Das Restrisiko sollte so kalkuliert werden, damit es einem Unternehmen nicht den sprichwörtlichen Rest gibt.»

CHECKLISTE KRISENMANAGEMENT

Folgende Fragen sollten Sie sich – adaptiert auf Ihr Unternehmen – zwischendurch stellen:

1. Bestehen Massnahmen zur Prävention von Krisen?
2. Ist ein Krisenstab vorgesehen und sind dessen Mitglieder definiert?
3. Wird der Krisenstab regelmässig geschult?
4. Besteht ein aktuelles Alarmmanagement (wer muss wann kontaktiert werden)?
5. Sind die wichtigsten Krisenszenarien bekannt?
6. Besteht ein Konzept für die Krisenkommunikation?
7. Sind die Mitarbeitenden für Notfälle ausgebildet?
8. Ist ein Handbuch für das Krisenmanagement vorhanden und wenn ja, wo?
9. Besteht ein Konzept für die Nachbearbeitung von Krisen?
10. Sind Tools (z.B. IT-basiert) für das Krisenmanagement implementiert und funktionsfähig?

				
	Thomas Gasser ist Geschäftsführer der Gasser Felstechnik AG in Lungern mit 280 Mitarbeitenden. **Gasser Felstechnik AG** Walchistrasse 30 6078 Lungern Tel. 041 679 77 77 Fax 041 679 77 75 gasser@felstechnik.ch www.felstechnik.ch	**Franz Grüter** ist CEO der green.ch AG in Brugg mit 90 Mitarbeitenden. **green.ch AG** Badstrasse 50 5201 Brugg Tel. 056 460 23 23 Fax 056 460 23 00 franz.grueter@green.ch www.green.ch	**William Aupée** ist Leiter «Qualität, Umwelt, Sicherheit, Normen» der Schmid Rhyner AG in Adliswil mit 47 Mitarbeitenden. **Schmid Rhyner AG** Soodring 29 8134 Adliswil Tel. 044 712 64 00 Fax 044 709 08 04 infopf@schmid-rhyner.ch www.schmid-rhyner.ch	**Max Rindlisbacher** ist Leiter Produktion und Facility Management der Tagblatt Medien AG in St.Gallen mit 652 Mitarbeitenden (Vollzeitstellen). **Tagblatt Medien AG** Fürstenlandstrasse 122 9001 St. Gallen Tel. 071 272 74 50 Fax 071 272 75 79 m.rindlisbacher@tagblattmedien.ch www.tagblattmedien.ch
Wie sieht ein Worst-Case-Szenario, d.h. der «unwahrscheinliche Fall» für Ihr Unternehmen aus?	Solche Fälle wären etwa im Untertagebau der Einsturz eines Tunnels, ein unerwarteter Felsabbruch während Fels-Sicherungsarbeiten oder der Zusammenbruch einer Baugrube.	Ein Super-GAU besteht in einem teilweisen oder kompletten Ausfall unserer Server, z.B. infolge Elementarschäden (Feuer, Wasser usw.), Sabotage, Stromunterbruch oder einem physischen Unterbruch der Internetverbindung während längerer Zeit. Aber auch Spionage oder Datenverluste sind mögliche Szenarien.	Als Chemieunternehmen sind wir mit verschiedenen Risiken konfrontiert. Unter die grössten Risiken fällt sicher ein Grossbrand.	Ein besonderes Gefährdungspotenzial besteht eigentlich nicht. Folgenschwer wäre etwa ein Brand bzw. ein Maschinenschaden gekoppelt mit Produktionsausfall oder ein grossflächiger Ausfall der IT-Systeme.
Wie sind Sie bzw. Ihr Unternehmen auf einen solchen Worst Case vorbereitet?	Unser Unternehmen verfügt über zertifizierte Managementsysteme in den Bereichen Qualität, Umwelt und Arbeitssicherheit. Darin sind auch Prozessorganisationen für Krisenfälle vorgesehen, wie z.B. Krisenstäbe.	Dem Bau unserer Rechenzentren gingen intensive Risiko-Analysen gemäss ISO voraus. Wir verfügen über redundante Systeme wie Dieselgeneratoren für die Überbrückung von Stromunterbrüchen, Löschanlagen und rigorose Zutrittskontrollen. Für das Krisenmanagement besteht eine komplette Organisation mit Krisenstäben.	Im Rahmen des Risikomanagements werden die Risiken regelmässig erfasst und bewertet. Daraus folgend werden Massnahmen zur Vermeidung und Verminderung von Risiken getroffen.	Es bestehen Brandschutzmassnahmen, Zutrittskontrollen, regelmässige Rundgänge durch Sicherheitspersonal, direkte Alarmierung der Blaulicht-Organisationen, ebenso sind Notabkommen mit anderen Unternehmen vereinbart, um Produktionsausfälle zu überbrücken. Die IT-Abteilungen verfügen über Sicherheits- und Notfallkonzepte.
Wann haben Sie das Risk Management bzw. die Krisenorganisation zum letzten Mal angepasst und was war der Anlass dazu?	Die Krisenorganisation wird einmal jährlich angepasst, jeweils im Rahmen der Ausarbeitung von neuen Businessplänen.	Jährlich erfolgt ein Sicherheits-Audit. Aufgrund von real aufgetretenen Ereignissen werden zudem die Prozesse laufend optimiert. So haben wir kürzlich für Notfälle eine eigene Krisen-Hotline eingerichtet, weil sonst die Gefahr besteht, dass unsere Callcenter überlastet werden. Ebenso werden Kundeninformationssysteme für Krisenfälle laufend ausgebaut.	Wir machen dies grundsätzlich jährlich in den Monaten März/April respektive ad hoc, wenn Ereignisse zu neuen Erkenntnissen führen	Anpassungen erfolgen laufend, so werden regelmässig Fluchtwege kontrolliert und brandschutztechnische Elemente überprüft und wenn nötig ersetzt. Die Erfahrungen anlässlich eines IT-Systemausfalls führten zu punktuellen Anpassungen der Notszenarien.
Wie oft schulen Sie die Belegschaft für Notfälle?	Auf unseren Werkhöfen führen wir regelmässig Übungen durch. Ferner finden immer im Januar ausgiebige Sicherheitsschulungen für unsere Mitarbeitenden statt.	Mindestens zweimal jährlich wird eine Alarmübung durchgeführt, in der die gesamte Krisenorganisation involviert ist.	Unsere Belegschaft wird ebenfalls jährlich für Notfälle trainiert.	«Katastrophen-Übungen» finden zwar nicht statt, doch der interne Sanitätsdienst schult und übt regelmässig. Ebenfalls werden Mitarbeitende in Brandbekämpfung als Ersteinsatzelement ausgebildet.