

## Sicherheitsmanagement auf dem Prüfstand

**Abgesehen von „Global Player“ mit hohem Bedrohungspotenzial, spielt das Thema „Terror“ für deutsche Unternehmen noch eine untergeordnete Rolle. Aber auch bezüglich der vielfältigen anderen Risikopotenziale wie z.B. Einbruch, Sabotage, Diebstahl, Wirtschaftskriminalität, Wirtschaftsspionage oder ganz normales technisches Versagen, verhalten sich viele Unternehmen und Sicherheitsverantwortliche bemerkenswert selbstsicher.**

**Gesetze und Regelwerke bestimmen zwar das Handeln – Selbstzweifel ist aber die beste Basis**

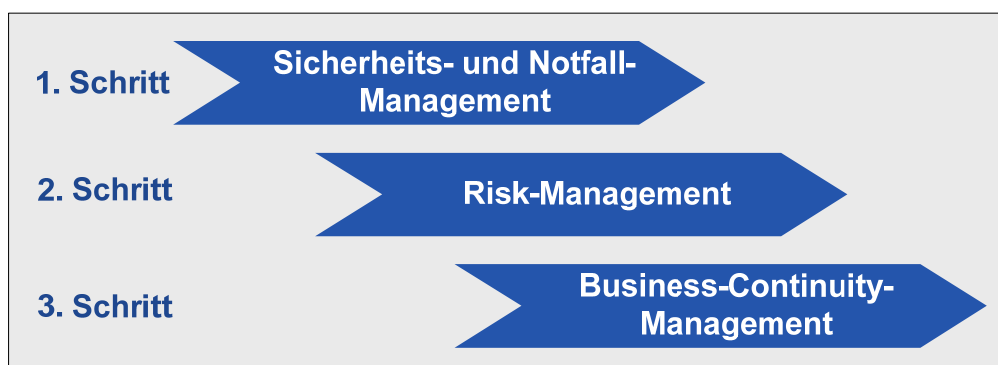
Curt Emmerich, deutscher Arzt und Schriftsteller sagte einmal: „Ich war meiner Sache ganz sicher und gerade diese Sicherheit war es, der alle Zweifel entsprangen“. Ein Satz, den sich jeder Sicherheitsverantwortliche merken sollte, denn konsequentes Sicherheitsmanagement ist der ständige Prozess „Bestehendes kritisch zu prüfen, zu optimieren und den Realitäten zeitnah anzupassen“.

Sicherheits- und Notfallmanagement wird von gesetzlichen und wirtschaftlichen Regelwerken bestimmt. „Organisationspflicht“, „Sorgfaltspflicht“, „KonTraG“, „Kommunikations- und Datenschutz“, DIN ISO 27001, „Arbeitsschutz“, „Umweltschutz“, Versicherungsbedingungen u.v.m. sind eng miteinander verknüpft und verpflichten zum vorbeugenden Handeln.

Auszug KonTraG:

„Die Gefahr von Verlusten und Schäden, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder in Folge externer Ereignisse eintreten, angemessen einzuschränken oder gar zu verhindern.“

Ein Satz mit weitreichender Bedeutung, dessen Realisierung mit dem Sicherheits- und Notfallmanagement beginnt. Teilweise überdeckend schließen sich Risk-Management und Business-Continuity-Management an.



Quelle: KRAISS SECURITY CONSULT

## Sicherheitsmanagement auf dem Prüfstand

### Die Haftungskaskade zeigt nach unten!

Die Haftungskaskade zeigt gefühlsmäßig nach oben. Bedrohungsbild, Schutzzieldefinition und Leitlinien müssen zwar auf der strategischen Ebene erarbeitet und entschieden werden. In der Regel wirkt die Haftungsverantwortung aber auf die operative Ebene. Hier erfolgt die Schwachstellenanalyse und die Risikobewertung, hier werden die Details der technischen und der baulichen Maßnahmen umgesetzt, hier werden die Verfahren und Prozesse für den Fall des Eintretens (Was ist Wenn?) entwickelt. Hier muss der Detaillierungsgrad hoch verdichtet und gerichtsfest dokumentiert werden. Organisationsfehler auf dieser Ebene können sich im Ereignisfall katastrophal auswirken und sind in der Regel den Sicherheitsverantwortlichen dann direkt zuzuordnen.

### Die Realität ist bedenklich

Eine Aussage wie: „Die Ursache war eine Verkettung unglücklicher Umstände“ deutet in der Regel auf Fehler im Sicherheitsmanagement hin und ruft automatisch Versicherung und Staatsanwaltschaft auf den Plan. Der Vorwurf „Organisationsverschulden“ ist schnell erhoben und trifft in der Regel auch zu.

Wurden Fehler bei der Bewertung von Schwachstellen und Risikopotenzial gemacht? Stimmte die Aufbau- und Ablauforganisation nicht, da ständig umorganisiert wurde? Lag es an fehlenden, falschen oder nicht aktualisierten Leitlinien, Richtlinien, Verfahrensanweisungen oder Arbeitsanweisungen? Lag es an fehlenden oder falschen Aufgaben- und Arbeitsplatzbeschreibungen? Lag es an inkonsequenter Überwachungs- und Gefahrenmeldetechnik. Hat man etwas davon und etwas hiervon genommen und waren deshalb die Sicherungslinien lückenhaft und nicht auf die notwendigen Widerstandszeitwerte für eine erfolgreiche Intervention und Schadensabwehr abgestimmt? Mangelte es an einer funktionierenden Gefahrenabwehrorganisation? Hat man nicht definiert wann ein Ereignis zu einem Notfall oder einer Krise eskaliert? Lag es an unklar oder gar nicht definierten Ablaufprozessen, an unklaren Vorgaben bezüglich Gesamtverantwortung, Durchführungsverantwortung, Mitwirkungsverantwortung und Informationspflicht? Fehlte es an regelmäßigen Schulungen und Übungen? Die Liste der Mängel und Fehler kann beliebig fortgeführt werden. Die Revisionspraxis zeigt, dass bereits auf der Ebene Security- und Notfallmanagement elementare Mängel vorhanden sind. Offensichtlich bleibt ungeachtet, dass bereits auf dieser Ebene der größte Teil des Risikopotenzials im Fall des Eintretens abgefangen werden kann.

### Risikobewertung und Wertschöpfungspotential rechtfertigen Investitionen

In Zeiten eng geschnürter Budgets und breit gestreuter Sparmaßnahmen kommt auch die Sicherheit nicht ungeschoren davon. Viele bereits verabschiedete Maßnahmen werden verschoben oder gestreckt, teilweise oder ganz gestrichen. Sicherheitsmängel werden bewusst in Kauf genommen. Der Sicherheitsverantwortliche steckt in der Zwickmühle. Nimmt er die Sicherheitsmängel billigend in Kauf, übernimmt er ein persönliches Risiko. Zeigt er die Sicherheitsmängel auf, muss er die Notwendigkeit zu deren Beseitigung nachvollziehbar belegen und dokumentieren. Die Risikobewertung (Risikopotenzialwert ohne Maßnahme und Risikopotenzialwert mit Maßnahmen) ist dafür ein geeignetes Mittel und dokumentiert gerichtsfest, dass Mängel erkannt, bewertet und

## Sicherheitsmanagement auf dem Prüfstand

den Verantwortlichen angezeigt wurden. Die Frage „Darf es etwas mehr oder etwas weniger sein“ ist auf das „notwendige Muss“ relativiert.

### Früh erkannt – Gefahr gebannt

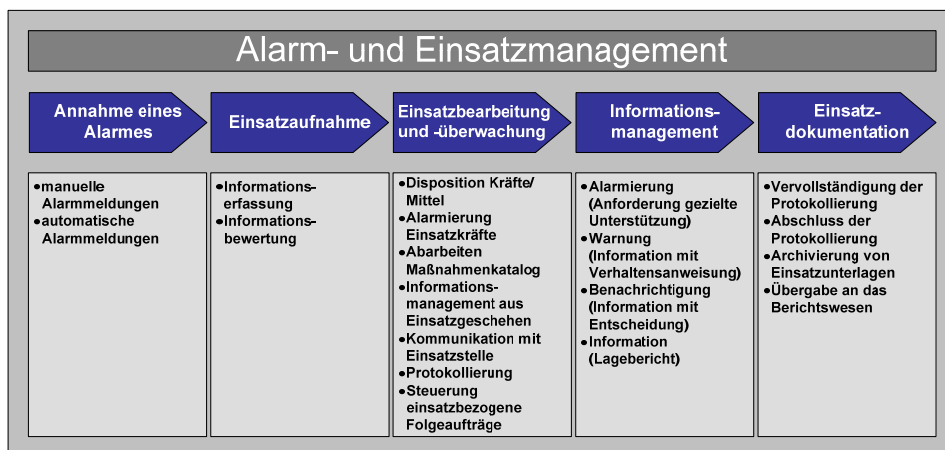
In der Regel werden die Kenngrößen Eintretenswahrscheinlichkeit (A) und Schadensausmaß (B) zur Bewertung des Risikopotenzials verwendet. Eine wichtige Kenngröße wird oft vernachlässigt und nicht in die Bewertung einbezogen: die Entdeckungswahrscheinlichkeit (C). Gerade an dieser Kenngröße lässt sich die Reduzierung des Risikopotenzials und somit der getätigten bzw. geplanten Investitionen sehr gut nachweisen. Die Gegenüberstellung von „Risikopotenzial Alt“ und „Risikopotenzial Neu“ sowie das verbleibende Restrisiko ist daher grundsätzlich zu empfehlen und belegt das Wertschöpfungspotenzial von Sicherheitsmaßnahmen.

### Strukturiertes Ereignis- und Notfallmanagement

Investitionen in technische, bauliche und personell-/organisatorische Maßnahmen verlieren an Wirkung, wenn die Ereignis- und Notfallorganisation im Fall des Falles nicht funktioniert. Die Ereignis- und Notfallorganisation hat zwar höchste Bedeutung, zeigt aber oft gravierende Mängel. Die Komplexität und der Detaillierungsgrad der Aufbau- und Ablauforganisation ist von Art und Größe eines Unternehmens abhängig. Der Aufwand für die durchgängige Konzipierung und Aktualisierung ist erheblich und wird aus Zeitmangel und Kostengründen oft vernachlässigt.

Die Kernanforderungen sind grundsätzlich gleich. Die damit verbundenen Sicherheits- und Ablaufprozesse müssen in jedem Fall eindeutig und lückenlos sein. Regelmäßige Trainings und Schulungen sind regelmäßig durchzuführen und zu dokumentieren.

Am Beispiel „Alarm- und Einsatzmanagement einer Sicherheitsleitstelle“ sind u.a. nachfolgende Aufgaben, Kernprozesse und Teilprozesse zu erarbeiten und gerichtsfest zu dokumentieren:



Quelle: KRAISS SECURITY CONSULT

## Sicherheitsmanagement auf dem Prüfstand

### Fazit:

**Sicherheits- und Notfallmanagement darf nicht von der Frage „etwas weniger oder etwas mehr“ bestimmt werden. Die beste Basis ist die Bereitschaft zu Selbstzweifel und systematischem Vorgehen.**

KRAISS SECURITY CONSULT  
Sandeldamm 16  
63450 Hanau  
Telefon 06181 / 78 05 35  
Telefax 06181 / 78 05 65  
Email [kontakt@kraiss-consult.de](mailto:kontakt@kraiss-consult.de)  
Website [www.kraiss-consult.de](http://www.kraiss-consult.de)