Compliance und Sicherheitsmanagement

Die Notwendigkeit zur Einhaltung gesetzlicher Regeln durch Unternehmen ergibt sich aus dem Grundsatz, dass Gesetze - auch durch juristische Personen - einzuhalten sind. Unternehmen und Unternehmensverantwortliche sind per Gesetz verpflichtet, dafür Sorge zu tragen, dass aus dem Unternehmen heraus keine Gesetzesverstöße erfolgen. Das Erkennen und Managen der vielfältigen Risiken, denen ein Unternehmen ausgesetzt ist, gehört ebenso zu den Rechtspflichten der Unternehmensverantwortlichen. Versäumnisse können zu wirtschaftlichem Schaden, Reputationsverlust und Haftung des Managements führen (in der Regel liegt Organisationsverschulden vor). Bereits der erste Schritt zu einem rechtssicheren und gerichtsfesten Sicherheitsmanagement, Gefahren und Bedrohungen sowie die damit verbundenen Risiken zu identifizieren, birgt Brisanz in sich, da häufig unrealistische Betrachtungen zugrunde liegen.

Gesetze, Richtlinien, Verordnungen und normative Anforderungen

Das natürliche Bedürfnis nach Sicherheit und Risikominimierung wird zusätzlich von gesetzlichen und normativen Regelwerken bestimmt. „Organisationsverpflichtung“, „KonTraG“, „Basel III“, „Kommunikations- und Datenschutz“, „Arbeitsschutz“, „Umweltschutz“, Versicherungsbedingen u.v.m. sind eng miteinander verknüpft und verpflichten das Management zum vorbeugenden Handeln: „Die Gefahr von Verlusten und Schäden, die in Folge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge externer Ereignisse eintreten, angemessen einzuschränken oder gar zu verhindern“. Letztendlich läuft es darauf hinaus, ein funktionierendes Sicherheitsmanagementsystem einzurichten, welches alle auf das Unternehmen oder Objekt zutreffende Gefahren und Bedrohungen berücksichtigt. Neben den wirtschaftlichen Risiken sind auch technischen und organisatorische Risiken zu identifizieren und zu bewerten. Zu den technischen Risiken gehören z.B. Risiko aus Forschung und Entwicklung, Produktionsrisiko und Produktionsausfallrisiko. Produktionsausfallrisiko wiederum ist eng verknüpft mit Verfügbarkeit der technischen Infrastruktur, u.a. Spannungsversorgung und Informationstechnik.

Auch der Schutz kritischer Infrastrukturen (KRITIS) und deren Einrichtungen wird mittlerweile durch die EU-Richtlinie 2008/114/EG geregelt. Zusätzlich greifen Regelwerke wie z. B. ISO 31000, DIN EN31010, COSO II oder ONR 49000 ff. Nicht zu vergessen ist die DIN EN 50518, die – hinsichtlich des Anwendungsbereiches - heftige Diskussionen unter den möglicherweise betroffenen Unternehmen auslöste. Zusätzlich sind oft vielfältige Policy- und Audit-Richtlinien umzusetzen. Die Richtlinie 96/82/EG des Rates vom 9. Dezember 1996 zur Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen, die EU-Richtlinien der Luftfahrt und der Luftsicherheit, der Sicherheit im Bahnbetrieb und in der Logistik, weitere internationale Standards wie die ISO 27001 und ISO 28001 für Informationssicherheit sind in vielen Unternehmen anzuwenden. Auch die Liste der DIN EN Regelwerke

ist lang und umfänglich. Sie regelt fast alles, was im technischen Umfeld zu berücksichtigen ist.

2018 werden die Normen zum Risikomanagement (ISO 31000) und zur Risikobewertungsmethoden (ISO 31010) überarbeitet erscheinen, die überarbeitet wurden. Geplant ist auch eine gemeinsame Ausgabe für die deutschsprachigen Länder (DACH).

Das Haftungsrisiko ist erheblich aber beherrschbar

Unbestritten ist, dass Gesetze rechtsverbindlich sind. Deren Berücksichtigung und Umsetzung stehen also nicht zur Diskussion. Zuwiderhandeln zieht strafrechtliche und oft auch zivilrechtliche Folgen nach sich.

Ein wesentliches Statement zu den ISO-Normen ist: ISO-Normen sind Leitlinien, deren Verwendung freiwillig ist. Verbindlichkeit erhalten ISO-Normen dann, wenn nationale Gesetze oder Verordnungen eine oder mehrere dieser Normen zum Bestandteil von nationalen Regelwerken erklären.

Die nachfolgenden juristischen Überlegungen stellen keine Rechtsberatung dar. Sie geben lediglich Inhalte publizierter juristischer Überlegungen wieder, die sich mit der haftungsrechtlichen Bedeutung nationaler und internationaler Normen im Bereich der Sicherheit, beschäftigt hat (z. B. Fachartikel im s+s report 6 / 2010, Autorin: Rechtsanwältin Petra Menge). Hinsichtlich der DIN EN Normen ist komprimiert festzustellen:

- Normen sind grundsätzlich keine Gesetze und keine Rechtsnorm und somit nicht rechtsverbindlich. Sie sind private, technische Regelungen mit Empfehlungscharakter. Ihre Anwendung ist somit grundsätzlich freiwillig, aber sinnvoll. Das hat auch der Bundesgerichtshof explizit in einem Grundsatzurteil klargestellt.

- Normen werden erst verbindlich durch Bezugnahme in Gesetzen, in Verordnungen oder in Verträgen.

- Früher galten Normen als anerkannte „Regeln der Technik“. Heute hat eine Entwicklung dahin gehend stattgefunden, dass sie bereits den „Stand der Technik“ wiedergeben.

- Grundsätzlich bilden DIN-Normen einen Maßstab für einwandfreies technisches Verhalten und sind im Rahmen der Rechtsordnung von Bedeutung. Die Nichtbeachtung oder der nicht erfolgreich geführte Nachweis der Beachtung von DIN-Normen kann in erheblichem Umfang haftungsrechtliche Auswirkungen auf die gesetzlichen Vertreter von Unternehmen oder Organisationen haben.

Die verbindliche Berücksichtigung von Normen spiegelt sich sehr ausgeprägt im Bereich der Zertifizierungen wieder. Es beginnt mit der allgegenwärtigen ISO 9000er Reihe und endet

bei individuellen Richtlinien von Verbänden und privatwirtschaftlichen Organisationen wie z. B. VdS, BHE, BSI, usw.

Im Gegensatz zur Rechtsverbindlichkeit der Gesetze wird die Berücksichtigung von Normen und Richtlinien vom Haftungsrecht nach den Vorschriften des Bürgerlichen Gesetzbuches bestimmt. Unerlaubte Handlungen gemäß §§823 ff BGB liegen in der Regel vor:

- Bei Vertragsverletzungen und Delikthaftungen. Dies sind u. a. Nachlässigkeit bei der Auftragsdurchführung, auftragswidriges Mitarbeiterverhalten, unzureichende Organisation und unzureichende technische Ausrüstung.

- Bei Schäden an Leib, Leben und Gesundheit oder Eigentum von Kunden, Mitarbeitern oder Dritten durch eine schädigende Handlung des Unternehmens, seiner Angestellten oder seiner Führungskräfte.

Spätestens an dieser Stelle muss ein Bezug zum „gerichtsfesten Sicherheitsmanagement oder auch Risikomanagement“ und dem damit verbundenen gut strukturierten und dokumentierten Sicherheitsmanagementsystem bzw. Risikomanagementsystem hergestellt werden. Unternehmen und Führungskräfte, die nach den Regeln des Sicherheitsmanagements handeln, brauchen Haftungsrisiken durch Rechtsverletzungen nicht zu fürchten.

Die Haftungskaskade im Sicherheitsmanagement zeigt nach unten

Regelmäßig werden namhaften Unternehmen sensible Daten gestohlen. Die Täter - Mitarbeitern oder Externe - konnten offensichtlich alle Sicherheitsvorkehrungen umgehen, die Daten aus dem Unternehmen schleusen und dem begehrlichen Markt zuführen. Wo es um viele Millionen Euro geht, bedienen sich sogar – oder zu Recht – bundesdeutsche Finanzbehörden dieser dubiosen Quellen. Der Zweck heilt die Mittel, das Kosten- / Nutzenverhältnis stimmt und an Tätern wird es auch weiterhin nicht mangeln.

Die bekannt gewordenen Fälle machen nicht nur Schlagzeilen, den betroffenen Unternehmen entstanden teils erhebliche wirtschaftliche Schäden und ein bedeutender Imageverlust. Auch die straf- und zivilrechtlichen Folgen sind für einige Verantwortliche äußerst schmerzhaft. Die Unternehmen sehen sich stets als Opfer krimineller Handlungen oder sollte man nicht besser sagen Opfer krimineller Insider-Handlungen? Wurde das Risiko „Mitarbeiter oder Insider“ einfach ausgeblendet, weil nicht sein kann, was nicht sein darf? Lässt man sich vom Satz leiten: So etwas hat es bei uns noch nicht gegeben?

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 werden die Schwachstellenanalysen und die Risikobewertungen erstellt. Hier werden die De-

tails der technischen und der baulichen Maßnahmen erarbeitet und umgesetzt. Hier werden die Verfahren und Sicherheitsprozesse 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 auch direkt zuzuordnen.