VfS-Handbücher

Handbuch
Gefahrenmanagement-Systeme (GMS)

Wirtschaftliche Fragestellungen – Nutzeranforderungen – Lösungskonzeptionen

3. Auflage

Verband für Sicherheitstechnik e. V.

Inhaltsübersicht

Inhaltsverzeichnis

I.1 Bedeutung eines umfassenden Sicherheitsmanagements

I.1.1 Wertschöpfung aus dem Sicherheitsmanagement

In einigen Branchen wie auch kritischen Verwaltungseinrichtungen wird bereits heute ein effizientes Sicherheitsmanagement als zentrales Vorsorge-Element wahrgenommen. Hierzu gehören Banken und Versicherungen ebenso wie Schlüsselindustrien der Grundstoffherstellung, große Produktions- und Fertigungsbetriebe, Logistik- und Verkehrsunternehmen usw. Auch in wesentlichen Bereichen der öffentlichen Verwaltung, wie Innenministerien, Polizeien, Landeskriminalämtern, der Justiz, der Finanzverwaltung usw. wurden den hohen Sicherheitsanforderungen entsprechende Maßnahmen ergriffen.

In vielen weiteren Unternehmen der Produktion und Dienstleistung steht die Sicherheit in der Werteskala zur Absicherung des Unternehmenserfolgs und Erzielung eines Wettbewerbsvorteils aber immer noch auf einer niedrigen Stufe; die möglichen Auswirkungen eines nicht vorhandenen oder nur rudimentär aufgesetzten Sicherheitsmanagements werden gar nicht erst in Erwägung gezogen, obwohl dessen Fehlen die Existenzgrundlage der Unternehmen gefährdet. Viel zu wenig wird ein effizientes Sicherheitsmanagement als wichtiger Teil der Wertschöpfung des Unternehmens wahrgenommen.

Trotz einer hohen Bedeutung der Gefahrenerkennung und -abwehr gelingt es den Sicherheitsverantwortlichen selten, aus dem Wissen um Risiken den „Business-Nutzen“ aus der Vermeidung von Gefahrenlagen nachzuweisen. Das Augenmerk der Entscheider richtet sich fast immer wieder nur auf die Kosten der Sicherheitstechniken und eines zugehörigen wirkungsvollen Sicherheitsmanagements, das dann auch noch qualifiziertes, und damit teures, Personal erfordert. Unbeachtet bleibt dabei die Tatsache, dass gerade ein Gefahrenmanagement-System den Personal- und Technikeinsatz optimiert, Folgekosten vermeiden hilft und die mit der Anschaffung entstehenden Kosten durch die nachfolgenden Einsparungen und sonstigen Vorteile fast immer überkompensiert werden.

Die Sicherheit muss „aus der Kostenecke“ herausgeholt und in die Unternehmensstrategie eingebunden werden. Dazu gehört auch, dass Sicherheitsverantwortliche mit entsprechenden Kompetenzen auszustatten sind.

Jedem Unternehmen ist unter Beurteilung von Eintrittswahrscheinlichkeiten eine detaillierte Risiko- bzw. Sicherheitsanalyse anzuraten, untrennbar verbunden mit der Bewertung von Schadensszenarien. Bei letzteren ist fallbezogen der voraussichtliche materielle Schaden ebenso

abzuwägen wie ein Ansehensverlust (Imageschaden), der die direkten Kosten der Schadensbeseitigung bei weitem übertreffen kann.

Bei potenziellem Personenschaden gibt es keinen Ermessensspielraum; Schutz von Leib und Leben hat immer absoluten Vorrang. Es erübrigt sich fast der Hinweis, dass bei Personenschäden die Berufsgenossenschaften und letztlich auch der Staatsanwalt die Ursachen ermitteln und ggf. auch haftungsrechtliche Konsequenzen für das verantwortliche Management einleiten.

Wesentlich ist auch die Erkenntnis, dass Sicherheit allein über Technik nur in Ausnahmefällen erreichbar sein wird. Sicherheit verlangt einen ganzheitlichen Prozess, der sich letztlich in einem umfassenden Sicherheitsmanagement abzubilden hat.

Im Sicherheitsmanagement sind dann in Anpassung an internationale Standards (z.B. ISO 27001) allgemeine Regeln und Erkenntnisse ebenso abzubilden, wie individuelle Maßnahmen aus der Bewertung der zu schützenden Personen, von potenziell gefährdeten Geschäftsprozessen und Objekten.

Ein umfassendes **Sicherheitsmanagement** stützt sich auf vier wesentliche Elemente, die letztlich eine Einheit bilden müssen, um daraus **Mehrwert und Nutzen** ziehen zu können:

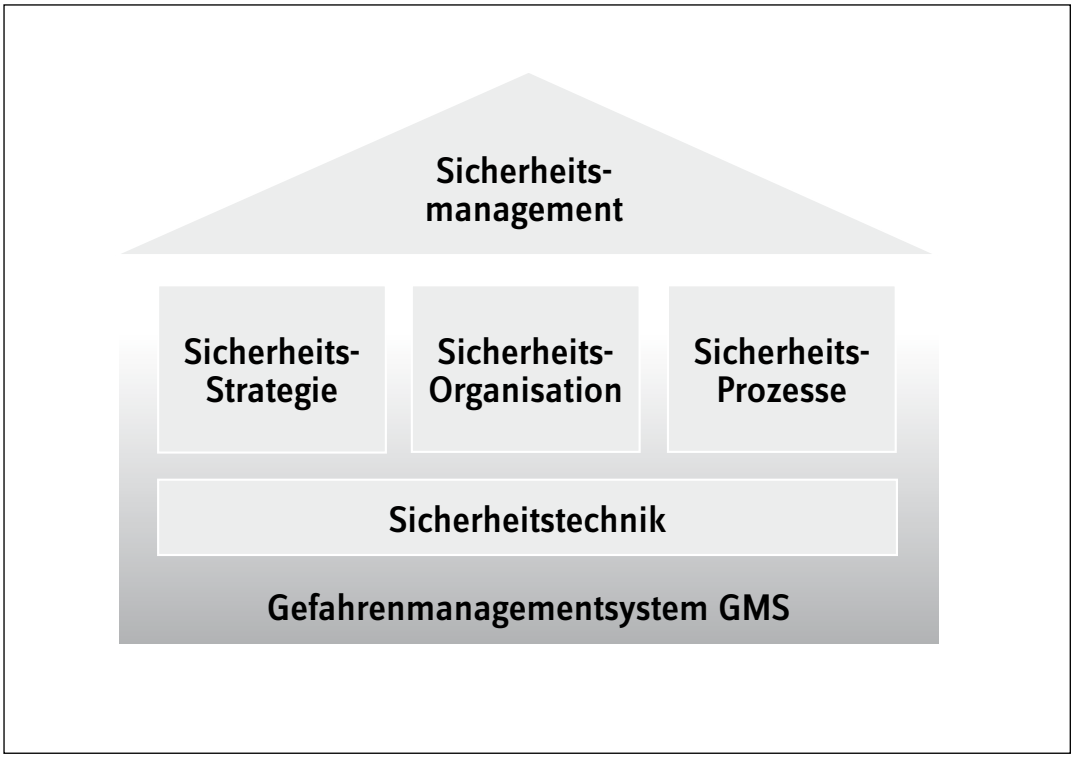

Abb. 1.1 Elemente eines Sicherheitsmanagements

I.1.2 Risikoerkennung und Schadensabwehr

Alle vernetzten Prozesse sind erhöhten Risiken ausgesetzt, was am Beispiel des „just-in-time“ am einfachsten zu beschreiben ist: Reißt ein Glied der Kette, ist meist nur unter erheblichen Aufwendungen größerer Schaden zu vermeiden.

Ein GMS überwacht alle eingebundenen technischen Subsysteme wie z.B. Brandmeldeanlagen, Frisch- und Abwasser, Heizung, Klima und Lüftung. Das GMS überwacht aber auch die Zutrittskontrolle im Rahmen der Diebstahls- und Sabotageprävention, häufig in Kombination mit Video-Beobachtung einschließlich Sensorik in allen sensiblen Bereichen.

Bisher meist übersehen, bzw. in separate Überwachungsprozesse eingebunden, wurde der Gesamtbereich der Informations- und Kommunikationstechniken (IuK). Eine Fertigungssteuerung mit systemgestützter Qualitätskontrolle im eigenem Unternehmen wie aber auch „remote“ beim Zulieferer ist durch technische Ausfälle ebenso gefährdet wie durch Virenattacken, und sei es „nur“ auf Übermittlungsstrecken zwischen zwei Standorten, wenn der Übertragungsweg beispielsweise im Internet ungesichert „getunnelt“ wird.

Das GMS leistet in einem solchen Umfeld wesentliche Unterstützungsarbeit für das Fachpersonal und die Unternehmensleitung:

Es bietet Vorwarnung vor und Früherkennung von Gefahrensituationen mit der Möglichkeit der Intervention vor Eintritt des Schadensfalles bzw. Reaktion in der Frühphase der Gefährdung mit meist noch geringer Wirkungsbreite und -tiefe von sich entwickelnden Schadensereignissen.

Im Alarmfall sind die betrieblichen und außerbetrieblichen Einsatzkräfte aufgrund detaillierter Lagebilder mit entsprechender Ausrüstung auf kurzem Wege einsatzbereit.

Protokollierung und Archivierung des Schadensablaufes wie auch der Aktionen/Reaktionen der Einsatzleitung wehren Haftungsansprüche ab und entlasten das Management; dies insbesondere im Fall von Personenschäden.

I.1.3 Abbau von Haftungsrisiken

Das bereits seit 1998 gültige „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich“ KonTraG verpflichtet Aktiengesellschaften und große GmbH zum Risikomanagement. Im § 91 Abs. 2 AktG war durch das KonTraG beispielsweise aufzunehmen, dass der Vorstand geeignete Maßnahmen zur Risikovorsorge zu treffen hat. Das heißt, dass er insbesondere in der Verpflichtung steht, ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen frühzeitig erkannt werden.

Der Geltungsbereich dieser Forderung erstreckt sich nach aktueller Rechtsprechung allgemein auf große Kapitalgesellschaften und wird voraussichtlich auch auf große Einheiten/Körperschaften des öffentlichen Rechts zu übertragen sein.

Ein Risikomanagementsystem (RMS) nach KonTraG beinhaltet nicht nur Offenlegungspflichten der wirtschaftlichen Verhältnisse; einzubeziehen sind alle Leitungsaufgaben des Vorstands/der Geschäftsführung, so auch die Pflicht zur Erkennung und Abwehr latenter Risiken im Rahmen der operativen Geschäftsführung.

Das GMS wird somit zwangsläufig Bestandteil des gesetzlich geforderten Risikomanagements.

Die sich häufig aus der Struktur und Komplexität des operativen Geschäfts ergebenden immanenten Bedrohungen unterschiedlicher Natur, z.B. in den Bereichen Produktion, Lager, Vorstoffe/Zulieferteile, IT/EDV und Umwelt erstrecken sich von technischen Risiken bis hin zu Betrug und Sabotage.

Welche Risiken wie zu überwachen sind, schreibt der Gesetzgeber nicht vor; die Rechtsprechung wird im Schadensfall die Verantwortung des Managements aber sehr genau analysieren und zumindest bei Kapitalgesellschaften heute bereits die Verantwortlichen zur Haftung heranziehen.

Der Einsatz eines leistungsfähigen GMS mit klaren betrieblichen Regelungen im Rahmen eines Notfallmanagements kann haftungsbefreiend wirken.

I.1.4 Elemente eines effizienten Sicherheitsmanagements

I.1.4.1 Sicherheitsstrategie

Die frühzeitige Erkennung und Abwehr von Gefahrenlagen bilden die Schwerpunkte und Ziele einer erfolgreichen Sicherheitsstrategie, die sich wiederum aus den Geschäftsgrundlagen und geschäftlichen Anforderungen ableiten muss. Ergänzend ist immer auch das potenzielle Verhalten der Kunden eines Unternehmens in Krisensituationen desselben zu bewerten.

Das Vorhandensein einer Sicherheitsstrategie sollte vorausschauend als Marketinginstrument mit eingesetzt werden, insbesondere wenn es darum geht, Kundengruppen über Vertrauensbildung zu gewinnen. Nicht zu vergessen sind auch die Hausbanken, deren Rating zu den sogenannten „weichen Faktoren“ Kreditvergaben nach Basel II maßgeblich beeinflusst. Insgesamt lassen sich daraus Chancen und Potenziale für erfolgreiche Geschäftsstrategien entwickeln.

Zur Sicherheitsstrategie gehört auch, dass diese aktiv gelebt, in eine Sicherheitsorganisation und in betriebliche Sicherheitsprozesse umgesetzt wird:

- Wenn nur zur einmaligen Untersuchung und Bearbeitung interner sicherheitsrelevanter Fragestellungen und ggf. auch externer Anforderungen „Paper-/Schrankware“ erstellt wurde, war dieses ein vielleicht erforderlicher, aber insgesamt doch teurer Vorgang. Der momentane Zweck mag erreicht sein, dem Unternehmen hilft es aber selten weiter.
- Eine Sicherheitsstrategie beinhaltet als Kernbestandteile die unternehmensindividuelle

Gefährdungsanalyse und einen entsprechenden Maßnahmenkatalog zur Risikoerkennung und Gefahrenabwehr. Auf die Gefährdungsanalyse wie auf den daraus abzuleitenden Maßnahmenkatalog ist angemessen in der Organisation und mit technischen Maßnahmen zu reagieren.

- Ein wesentlicher, häufig aber vernachlässigter Teil des Sicherheitskonzeptes ist ein sogenannter Alarmplan. Dieser muss lageabhängig Alarmierungs- und Meldewege, Evakuierungs- und beispielsweise auch Interventionsmaßnahmen aufzeigen.
- Der Notfallplan bzw. das Continuity-Management dürfen in keinem Fall ausgelassen werden; die jeweilige Maßnahmentiefe ist individuell festzulegen.

Die Sicherheitsstrategie ist kein statisches Instrumentarium. Diese muss in Anpassung an sich wandelnde Geschäftsprozesse, Kundengruppen, neue interne und externe Bedrohungen, Fortschritt in den Sicherheitstechniken usw. einer periodischen Revision unterworfen werden. Während z.B. Qualitätssicherung nach ISO 9000 mit jährlichen Überwachungsaudits eine allgemein akzeptierte Vorgehensweise geworden ist, fehlt in der Anerkennung von Sicherheitsstrategien Vergleichbares; der Marktwert einer zertifizierten Sicherheitsstrategie lässt vielfach noch auf sich warten.

Ansätze sind im Segment der IuK-Technologien über Zertifizierungen von Sicherheitsmaßnahmen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu beobachten; eine Plattform für allgemeine Anerkennung von Sicherheitsstrategien scheint aber zu fehlen.

Unabhängig von allgemein gültigen Zertifikaten kann und sollte jeder seine Sicherheitsstrategie entwickeln und nach innen und außen wirkend umsetzen.

I.1.4.2 Sicherheitsorganisation

Ein wesentlicher Aspekt für den Aufbau und die werteorientierte Ausrichtung der Sicherheitsorganisation betrifft die in der Regel ganzheitliche Betrachtung zwischen enger Verzahnung von Geschäftsprozessen und der Sicherheit im Unternehmen. Beide Seiten, Business- und Sicherheitsverantwortung, müssen aufeinander zu gehen, ihre Anforderungen formulieren, ggf. auch priorisieren und in die Betriebsorganisation einbringen.

Sicherheitsstrategische Sichten und Vorgehensweisen müssen sich in der Gesamtorganisation des Unternehmens mit entsprechenden Kompetenzen und Durchgriffsmöglichkeiten wiederfinden. So weit erforderlich, ist ein eigenständiger Fachbereich Sicherheit aufzusetzen, der sowohl in die innerbetrieblichen Informationsflüsse und Berichtswege als auch bei der Planung neuer Geschäftsprozesse entsprechend verantwortlich einzubinden ist.

Personell muss die Sicherheitsverantwortung nicht zwingend Vollzeit wahrgenommen werden; die Gefahr der Interessenkollision im Jobsharing ist jedoch zu vermeiden.

Wesentlicher Bestandteil einer jeden Sicherheitsorganisation ist deren Kommunikation nach innen, das heißt die angemessene Einbindung des Personals, weitergehend möglicherweise auch die Verpflichtung auf die Umsetzung der Sicherheitsorganisation im Alltag mit den jeweiligen Sicherheitsprozessen.

I.1.4.3 Sicherheitsprozesse

Die strategische Bedeutung der Sicherheit hat sich in der Verankerung und Verzahnung mit den Prozessen der jeweiligen Betriebs- und Ablauforganisation wiederzufinden. Vorgangsabhängig ist im Prozesshandbuch eines jeden Unternehmens oder einer jeden Behörde festzulegen, dass Freizeichnungen bestimmter Vorgänge auch die Zustimmung der Sicherheitsverantwortlichen erfordern. So weit erforderlich, muss der Sicherheit Vetorecht eingeräumt werden, welches nur durch die Geschäftsführung oder die Behördenleitung aufgehoben werden kann; dann aber auch im Bewusstsein der Akzeptanz von potenziellen Risiken in den Folgeschritten.

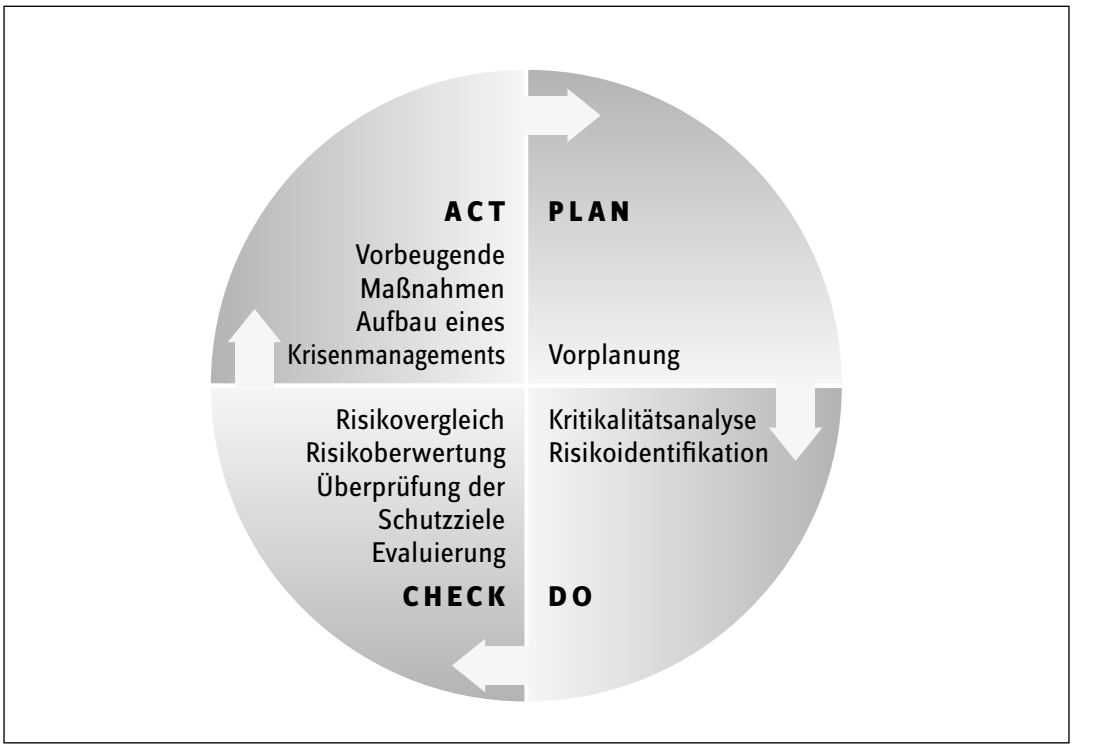

Abb. 1.2 Plan-Do-Check-Managementzyklus

In vielen Fällen wird eine verantwortliche Geschäftsführung oder Behördenleitung vor kritischen Entscheidungen eine Nutzwertanalyse durchführen lassen und Mehrwert gegen Risikofaktoren angemessen bewerten.

Sicherheitsprozesse unterliegen gewisser Allgemeingültigkeit im Rahmen internationaler Standardisierung, z.B. nach ISO 27001 für den Bereich IT. Allgemein gültige Standards treffen aber

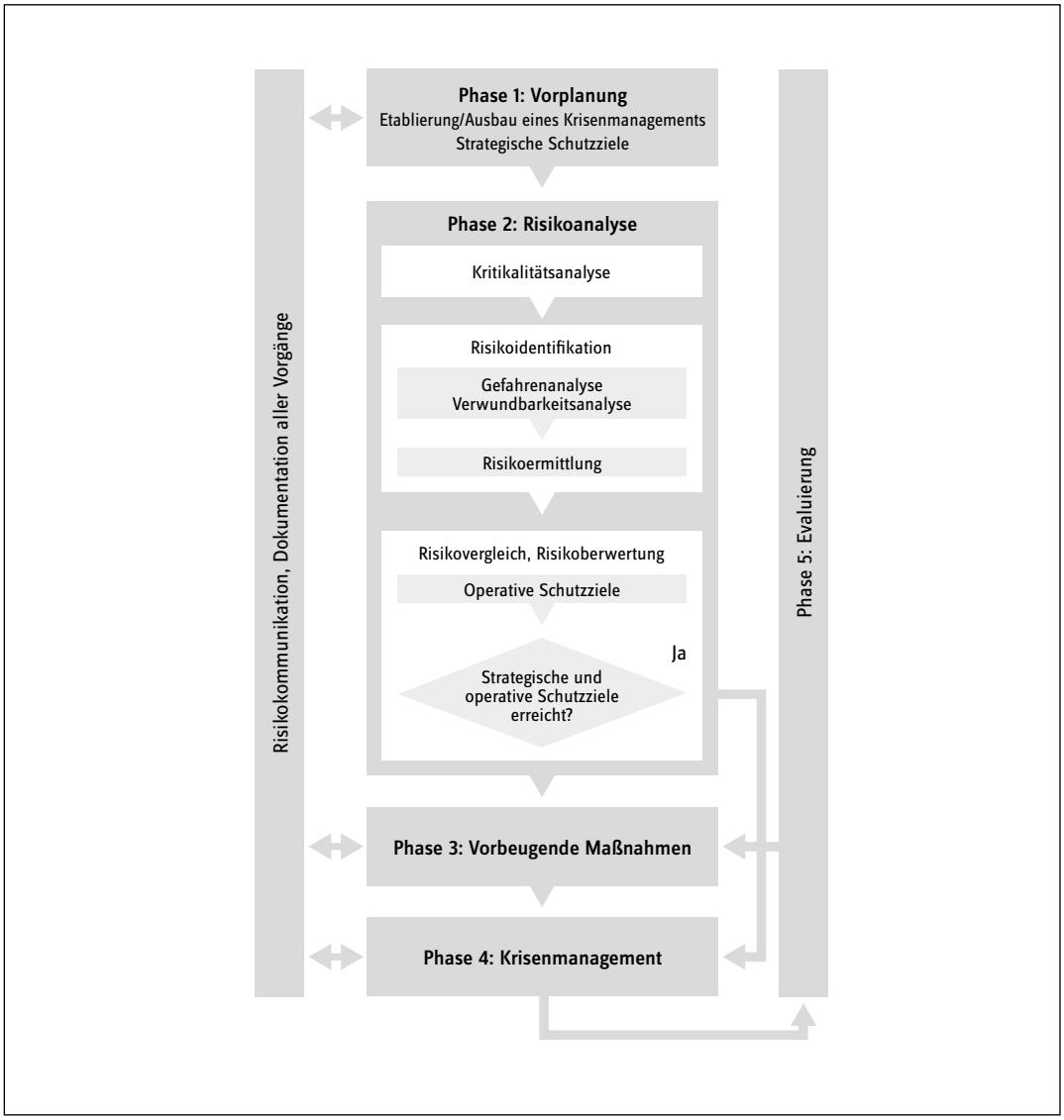

Abb. 1.3 Sicherheit als dynamischer Optimierungsprozess[1]

selten die spezifischen Sicherheitsbedürfnisse eines Unternehmens/einer Behörde und sind somit in jedem Fall auf die betrieblichen Anforderungen abzustimmen. Damit ist der gesamte Sicherheitsprozess der betroffenen Einheit auf individuell erstellten Sicherheitsrichtlinien zu betreiben.

Von wesentlicher Bedeutung ist auch nicht der zitierte Standard allein, sondern die innerbetriebliche Verpflichtung aller Beteiligten, sich an den einmal verabschiedeten Prozess zu halten. Dessen Umgehung aus Termindruck oder anderen scheinbar zwingenden Gründen wird sich in vielen Fällen als fataler Fehler erweisen.

[1] Quelle: BMI/Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, Leitfaden für Unternehmen und Behörden/Stand: 2007

Die Realisierung der Sicherheitsprozesse und damit Umsetzung der Sicherheitsrichtlinien kann tiefgreifende Änderungen im strukturellen Umfeld des Unternehmens oder der Verwaltungseinheit zur Folge haben. Hierbei ist es von entscheidender Bedeutung, dass bei der Planung des Sicherheitsprozesses auch alle sicherheitsrelevanten Bereiche des Unternehmens einbezogen werden.

Im laufenden Betrieb müssen die realisierten Sicherheitsrichtlinien einem ständigen Verbesserungs- und Anpassungsprozess unterliegen. Gewonnene Erkenntnisse sind innerhalb eines kontinuierlichen Prozesses erneut in die Planung und Realisierung einzubeziehen. Dieses sollte nach einer im Risiko- und Krisenmanagement allgemeinen anerkannten Prozessfolge im Rahmen eines „Plan-Do-Check-Managementzyklusses“ (PDCA) durchgeführt werden.[2]

Einzelmaßnahmen zur Erkennung und Abwehr bestimmter Gefahren sind normiert bzw. können normiert werden und unterliegen allgemein anerkannten Standards (s.o.); der gesamte Sicherheitsprozess eines Unternehmens, meist auch einer Behörde, beinhaltet eine Vielzahl gegenseitiger Abhängigkeiten. Er ist damit immer individuell und hängt maßgeblich von der Bewertung des Risikopotenzials ab; die Risikoanalyse ist unverzichtbar!

Postulat: Sicherheit ist ein wesentlicher Bestandteil der Qualitätssicherung und als Marketinginstrument häufig unterbewertet.

I.1.4.4 Sicherheitstechnik

Neue Sicherheitstechnik kostet Geld, veraltete Technik kostet durch Nichtleisten der an sie gestellten Forderungen im Ernstfall meistens ein Vielfaches dessen, was an Aufwendungen für einen Innovationszyklus in der Sicherheitstechnik erforderlich gewesen wäre. Technik allein macht es auch nicht; diese will eingesetzt, betrieben und überwacht/gewartet werden.

Die Frage ist somit immer, inwieweit Kenngrößen mit quantitativen und qualitativen Indikatoren eine Kosten-Nutzen-Analyse über die Gesamtheit der betroffenen Bereiche des Unternehmens ermöglichen, z.B.

- Infrastruktur (Hoch-/Tiefbau, Verkehrswege/Logistikketten, Perimeter, Schleusen, Ver- und Entsorgungseinrichtungen usw.)
- Hard-/Software (Sicherheitstechnik, Kommunikationswege/-verbindungen, IT-Infrastrukturen usw.)
- Orga-Lösungen (Überwachungs-, Kontroll- und Revisionsmaßnahmen, Schließsysteme usw.)
- Personal für Planung und Betrieb sicherheitstechnischer Einrichtungen

[2] Quelle: BMI/Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement, Leitfaden für Unternehmen und Behörden/Stand: 2007

I.1.5 Mehrwert und Nutzen des Sicherheitsmanagements

I.1.5.1 Schlüsselfaktoren

Im Rahmen zusehends knapperer Budgets sind auch die Sicherheitsverantwortlichen gezwungen, jeden investierten Euro zu rechtfertigen. Unternehmensleitungen wollen mittlerweile genau wissen, ob die für ihre Sicherheit auszugebenden Gelder richtig bemessen, zu knapp angesetzt sind oder eventuell auch überzogen sein könnten. Wie kann man das richtige Maß für die sicherheitstechnischen Ausgaben finden?

Der erste Schritt liegt in der Fragestellung, welches Sicherheitsniveau das Unternehmen insgesamt oder in wesentlichen Bereichen benötigt oder auch mit wie viel potenzieller Bedrohung man leben kann oder will. Diese Risikoabschätzung ist gleichermaßen Kunst wie Wissenschaft, befreit die Verantwortlichen jedoch nicht von einem systematischen Vorgehen. Allein auf das Glück zu bauen, dass die Gefahrensituationen nicht eintreten, ist wie ein „russisches Roulette".

Der Weg zum Ziel führt über Schlüsselfaktoren, die sogenannten „Key Performance Indicators" (KPIs) in den nachfolgend aufgeführten Schritten:

- Sicherheitsstrukturanalyse mit Schutzbedarfsfeststellung, ggf. mehrstufig, beginnend mit einer Stärken-Schwächen-Analyse (SWOT, siehe unten)
- erste Modellierung eines Sicherheitskonzeptes
- Durchführung von Basis-Sicherheitschecks
- Aufsetzen einer umfassenden Risikoanalyse
- Erarbeitung einer Sicherheitsrichtlinie für das Unternehmen
- gefolgt von Dienstvereinbarungen, Mitarbeiterverpflichtungen
- Einbindung von Sicherheitsfachpersonal und ggf. externer Interventionskräfte
- „last but not least": Planung beziehungsweise Aktualisierung der Notfallvorsorge

1.5.2 Risikoanalyse

Die Risikoanalyse resultiert im Erkennen der Schutzziele und der Definition der Maßnahmen mit Priorisierung von Einzelmaßnahmen bzw. deren Kombination zur Minderung des Gesamtrisikos. Für den Schadensfall sind entsprechende Notfallpläne, d.h. Back-up-Szenarien, vorzubereiten.

II.A.1 Leitfaden zur Planung von GMS

II.A.1.1. Ausgangslage und Voraussetzungen zur Planung von GMS

II.A.1.1.1 Zielsetzung

Die wichtigste Voraussetzung für die Planung eines Gefahrenmanagement-Systems ist die **ganzheitliche Betrachtung** des zu schützenden Bereiches inklusive aller Teilbereiche.

Insbesondere bei der Vernetzung von sicherheitstechnischen Einrichtungen spielen übergeordnete Managementsysteme eine zunehmend zentrale Rolle. Es gilt, Gefahrenmeldeanlagen, Warn- und Signalisierungsanlagen, Kommunikationseinrichtungen sowie die betriebstechnischen Einrichtungen über Datenschnittstellen mit dem Managementsystem zu verbinden. Die Integration dieser Teilsysteme einer sicherheitstechnischen Infrastruktur macht jedoch nur dann Sinn, wenn möglichst viele Funktionen der verbundenen Systeme über eine **einheitliche Benutzeroberfläche** des GMS genutzt werden können und der Anwender damit einen erweiterten Nutzen erzielt.

Für den **Planer** solcher Systeme gilt es, die Funktionalitäten unter Berücksichtigung bestehender Vorschriften, Richtlinien und Normen zu erfassen, zu strukturieren, auszuschreiben und in die Umsetzung zu begleiten (Objektüberwachung in der Leistungsphase 8 der HOAI; siehe nachfolgend).

Grundsätzlich besteht für GMS und deren Betrieb ein weitgehender Gestaltungsspielraum, andererseits sind z.B. konkrete Vorschriften einzuhalten.

Gerade auch die jeweils für die verbundenen Systeme geltenden Richtlinien haben in der Regel Einfluss auf diesen Gestaltungsspielraum.

Eine weitere Aufgabe des Planers ist es, in die Gewerke übergreifende Planung eine ergonomisch-ökologisch optimierte Koordination aller Funktionen einzubinden.

Dieser Leitfaden soll u.a. Planern, Anwendern, Herstellern und Errichtern sowie Systemintegratoren eine Hilfestellung bei der Ausschreibung, Angebotserstellung und Projektabwicklung geben. Aufgrund der Vielschichtigkeit sicherheitstechnischer Anforderungen kann dabei kein Anspruch auf Vollständigkeit erhoben werden.

Die nachfolgende Abbildung 1 (Hierarchiemodell) weist darauf hin, dass ein GMS ganzheitlich „top down“ zu planen ist:

Im Rahmen des **Management-Levels** ist das Einsatzumfeld mit den zu erreichenden Zielsetzungen zu bestimmen.

Im **Automation-Level** ist zu klären, welche Teilsysteme, letztlich als sogenannte verbundene Systeme, zusammen zu schalten sind und wie Alarme aus diesen erfasst, ggf. gefiltert und an den Management-Level zur Ausgabe, Visualisierung usw. übergeben werden sollen.

Im Field-Level werden die einzelnen Melder und Sensoren beschrieben (z.B. Typen, Platzierungen, Zusammenschaltung zu Melderketten usw.).

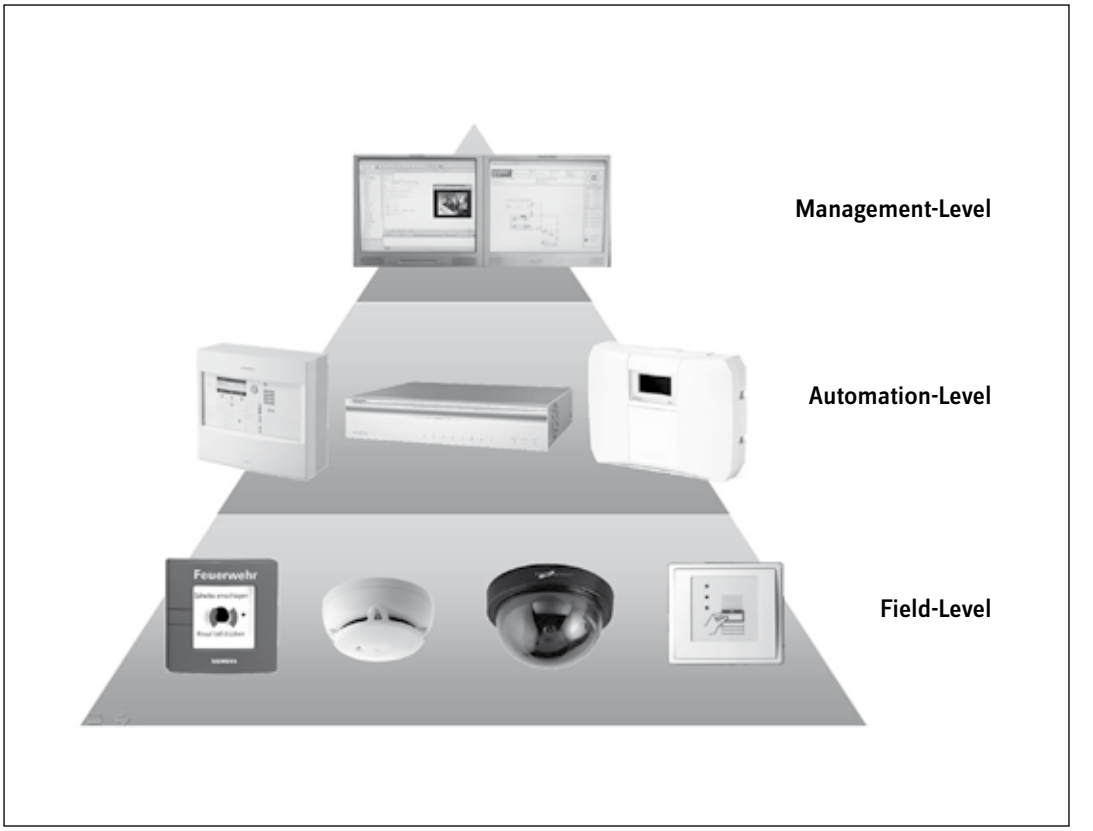

Abb. A.1.1 Hierarchiemodell zum Gefahrenmanagementsystem

II.A.1.1.2 Richtlinien und Vorschriften zu Planungsleistungen (Auszug)

Der Planer selbst ist in seiner Aufgabenstellung und Vorgehensweise in den meisten Fällen in Vorschriften und Richtlinien eingebunden, die letztlich auch den Vertrag zwischen ihm und seinem Auftraggeber bestimmen.

- Häufig zur Anwendung kommt die **Honorarordnung für Architekten und Ingenieure HOAI** in ihrer jeweils aktuellen Fassung mit zugehörigen Musterverträgen. Dieses gilt für den privaten wie auch öffentlichen Auftraggeber.
- Überwiegend im Bereich des öffentlichen Auftragebers kommen, je nach **Aufgabenstellung an den Planer** wie auch die zu erbringenden Leistungen bzw. die erstellenden Gewerke, mehrere Regelwerke in Betracht:

  - **VOL** („Vergabe und Vertragsordnung für Leistungen“) mit
    - VOL/A (Verfahrensrichtlinien), Abschnitte 1 oder 2, letzterer für die Vergabe von Leistungen im Anwendungsbereich der Richtlinie 2004/18/EG (VOL/A-EG)
    - VOL/B (Allgemeine Vertragsgrundlagen zur Erbringung von Leistungen)
  - **VOB** („Vergabe und Vertragsordnung für Bauleistungen“) mit
    - VOB/A (Verfahrensrichtlinien), Abschnitte 1 (Basisparagrafen) oder 2 (Basisparagrafen mit zusätzlichen Bestimmungen nach der Richtlinie 2004/18/EG)
    - VOB/B (Allgemeine Vertragsbedingungen zu Bauleistungen)
    - VOB/C (DIN/EN)
  - **VOF** (Verdingungsordnung für freiberufliche Leistungen)
- Abhängig von den Aufgabenstellungen kommen ggf. Anforderungen hinzu wie z.B.
  - Einhaltung datenschutzrechtlicher Bestimmungen (BDSG, Landesdatenschutzgesetze, Sozialgesetzbuch usw.)
  - Umweltschutzgesetzgebung mit einschlägigen Rechtsverordnungen
  - Zertifizierungsnachweise, z.B. nach ISO 9001 und ISO 27001
  - Nachweise zu Sicherheitsüberprüfungen
  - Auflagen der Berufsgenossenschaften bzw. des Arbeitsschutzes
- **Hinweis:** Die aufgeführten Regelwerke unterliegen einem ständigen Wandel, maßgeblich verursacht durch Regulierungsvorgaben der EU im Rahmen von in nationales Recht zu überführenden Dienstrichtlinien, aber auch durch den technischen Wandel. Vor Anwendung der Regelwerke ist in jedem Fall sicherzustellen, dass auf die aktuell gültigen Fassungen zugegriffen wird.

II.A.1.1.3 Aspekte der Sicherheit

Ein gewerkeübergreifendes Sicherheitsmanagement stellt dem Betreiber eine für die Arbeitserfordernisse optimierte Bedienerunterstützung zur Verfügung.

Um diese Unterstützung bei Systemausfällen oder Anlagenfehlern aufrecht zu erhalten, ist eine stufenweise Sicherheitskonzeption vorzusehen. Diese könnte folgende Kriterien aufweisen:

- Modularer Aufbau in Hardware und Software:
  Ein modularer Aufbau der Hard- und Software erlaubt eine strukturierte Teststrategie sowie ein schnelles und logisches Erkennen von Fehlern und somit einen zielgerichteten Austausch der defekten Komponenten.

- Backup-Fähigkeit:
  Zeitzyklisches Speichern der Datenbestände, mindestens aber nach Änderungszyklen, versetzt den Betreiber bei Datenverlusten wieder in die Lage, auf einer weitgehend aktuellen und konsistenten Betriebssituation neu aufzusetzen.
- Spiegelplattenbetrieb:
  Bei Spiegelplattenbetrieb werden die aktuellen Betriebsdaten parallel und quasi zeitgleich auf zwei eigenständigen Speichermedien geführt. Dadurch wird einem Datenverlust vorgebeugt, d.h. in einem Fehlerfall arbeitet das System ohne Unterbrechung mit dem gespiegelten Datenbestand weiter.
- Hot-Standby-Rechner:
  Bei Hot-Standby-Konzeptionen arbeiten zwei Rechnersysteme zeitgleich. Bei Ausfall des aktiv arbeitenden Systems erfolgt in der Regel ohne Bedienereingriff eine automatische Umschaltung auf das Redundanz-System; die Anwendungen laufen weiter. Zur Sicherung der Datenbestände ist eine Festplattenkonzeption nach RAID zu empfehlen.
- RAID-Konzeption:
  Bei einer RAID-Konzeption steuert ein eigener Controller die Platten- und/oder Speicherzugriffe und die Verteilung der Datenbestände ohne Beeinflussung der Arbeitsauslastung des Anlagen-Steuerrechners. Je nach Anforderung sind Lösungen nach unterschiedlichen RAID-Levels zu konzipieren. Bei RAID Level 5 (oder höher) mit mindestens 3 Festplattenlaufwerken lässt sich z.B. die defekte Festplatte im laufenden Betrieb ohne Rückwirkung austauschen.

II.A.1.2 Projektphasen

II.A.1.2.1 Übersicht

Im Rahmen der Realisierung von Gefahrenmanagementsystemen (GMS) gilt es (in Anlehnung an die HOAI) einzelne Projektphasen zu beachten, die unterschiedliche Inhalte, Zuständigkeiten und Verantwortungen aufweisen:

Leistungsphase 1/Grundlagenermittlung mit u. a.

- Klärung der Ausgangssituation
- Ermittlung der Anforderungen an das Projekt
- Zieldefinition und
- damit Erstellung eines Pflichtenheftes

Leistungsphasen 2 und 3/Vor-, Entwurfsplanung mit u.a.

- Klärung aller Rahmenbedingungen
- Kostenschätzungen/-rechnungen (z.B. nach DIN 276)

Leistungsphase 4/Genehmigungsplanung (so weit erforderlich, möglichst vor Erstellung der Ausführungsplanung)

Leistungsphase 5/Ausführungsplanung

Leistungsphase 6/Vorbereitung der Vergabe (Ausschreibung) mit

- Erstellung der Ausschreibungsunterlagen
- Durchführung der Ausschreibung

Leistungsphase 7/Mitwirkung bei der Vergabe mit

- Angebotsauswertung
- Vergabe

Leistungsphase 8/Objektüberwachung (Bauüberwachung)

- Projekt-/Ausführungsüberwachung
- Kostenkontrolle
- Abnahme

Leistungsphase 9/Objektbetreuung und Dokumentation

II.A.1.2.2 Grundlagenermittlung

Hinweis: Checklisten zur Grundlagenermittlung sind Bestandteil des Kapitels II.A.1.4 dieses Kapitels.

II.A.1.2.2.1 Klärung der Ausgangssituation und Anforderungen

Mit Klärung der Ausgangssituation und Anforderungen an das Projekt sind die Voraussetzungen zur Aufnahme der Planungsarbeiten möglichst umfassend sowie gleichzeitig auch eingegrenzt auf die Aufgabenstellung herbeizuführen. Häufig ist die Frage zu beantworten, inwieweit bestehende Verträge des Auftraggebers mit Dritten die Planungsarbeiten beeinflussen werden.

II.A.1.2.2.2 Zieldefinition

Die Zieldefinition muss durch den Auftraggeber/Nutzer vorgegeben werden und dient als Grundlage für die Erarbeitung eines Pflichtenheftes. Die Zieldefinition beinhaltet u.a. folgende Elemente:

- Umfang der zu integrierenden Sicherheits-, Kommunikations- und Haustechnikanlagen/-systeme

- Definition der Integrationsschritte in z.B. bestehende Infrastrukturen
- erwartete Verbesserungen gegenüber einer Einzelsystemlösung
- Beschreibung der Arbeitsplätze, Betriebsabläufe und Aufgaben der Mitarbeiter an den Arbeitsplätzen (Prozessbeschreibung)

Der Auftraggeber muss seine Anforderungen (Zieldefinition) erfassen und verständlich darlegen. Je umfassender die Darstellung ist, desto detaillierter können die beteiligten Partner auf den gemachten Angaben aufbauen.

Aus der Aufgabenstellung muss z.B. eindeutig hervorgehen:

- Welchen Umfang das GMS als Gesamtsystem haben soll
- was in einem GMS zu integrieren ist
- welche Funktionen ein GMS erfüllen muss
- welche übergreifenden Verknüpfungen zwischen dem zu planenden GMS und den unterschiedlichen, weiteren Systemen gefordert werden
- wie die integrierten Einzelinformationen im Rahmen des dann übergeordneten Systems dargestellt werden sollen
- Definition, wie Einzelinformationen innerhalb des Gesamtsystems behandelt und welche weiteren Aufgabenstellungen an diese geknüpft werden sollen
- Ansprechpartner des AG
- vom AG bereitgestelltes Material

II.A.1.2.2.3 Pflichtenheft

Aus der **Zieldefinition** ist ein Pflichtenheft in Zusammenarbeit Nutzer/Planer zu erstellen.

Im Rahmen des Pflichtenheftes wird die Vollständigkeit und Klarheit der Zieldefinition überprüft. Folgende Angaben müssen u. a. konkretisiert werden:

- Welche Anlagen/Systeme sind im Bestand vorhanden und in das Gesamtsystem einzubinden (mit Angabe des Softwarestandes)?
- welche Anlagen/Systeme müssen neu angeschafft werden? Fabrikate bzw. Beschreibung der Systeme und der erwarteten Schnittstelle für die Integration
- Datenpunktumfang
- funktionale Beschreibung (Alarmpläne, Automatisierungswünsche, Maßnahmenpläne, Grafiken, Bedienungskonzepte etc.)
- Definition der erwarteten Leistungsmerkmale