

Zukunft der Sicherheit: prozessorientierte Managementsysteme

AUTOR: DR. JUR. KLAUS BOCKSLAFF

Die Einordnung der Unternehmenssicherheit innerhalb der Unternehmenshierarchie ist in Bewegung geraten. Als Ergebnis von Reorganisationsprojekten wird die Unternehmenssicherheit zunehmend in dem Bereich Compliance oder Risikomanagement angesiedelt. Damit geht ein befürchteter Bedeutungsverlust der Unternehmenssicherheit einher: Werden insbesondere die Leiter der Unternehmenssicherheit einen erheblichen Bedeutungs- und auch Bezahlungsrückgang erfahren? Insgesamt stellt sich hier nicht weniger als die Frage nach der Zukunftsfähigkeit der Unternehmenssicherheit in ihrer heutigen Form.

In vielen Unternehmen ist das Thema „Konzernsicherheit“ oder „Unternehmenssicherheit“ historisch gewachsen. Einzelne operative Bereiche der „Sicherheit“ sind für sich genommen gut ausgeprägt. Gleichzeitig fehlen allerdings häufig

- (1) ein klarer Bezug zur Unternehmensstrategie,
- (2) eine Herleitung der Anforderungen aus den Geschäftsprozessen und
- (3) der Risikoanalyse sowie
- (4) eine eindeutige Definition und Aufbau der Planungs-, Führungs- und Steuerungsprozesse der Sicherheit.

Anders gesagt: Der Stärke auf der operativen Umsetzungsebene der Sicherheit steht das Fehlen eines durchgängigen, prozessorientierten Managementsystems der Sicherheit gegenüber.

Hinzu kommt: In vielen Unternehmen wird in Sachen Sicherheit ein erheblicher Aktionismus nach Großereignissen (leider) von einer geringen Akzeptanz im Alltag begleitet. Erheblicher Stellenabbau bzw. große Fluktuation bei den Mitarbeitern und eine inhaltliche und organisatorische „Abspaltung“ der IT-Sicherheit kommen hinzu. Neben einer gedanklichen Trennung zwischen Safety und Security – mit „Kasten“-Denken auf beiden Seiten – finden wir schließlich in vielen Unternehmen ein „Beauftragten“-Unwesen.

Sicherheitsmanagement als unternehmensweiter Gesamtanspruch

All diese Befunde zusammengekommen sind nicht zuletzt auch ein Ausdruck eines mangelnden Gesamtanspruchs der Sicherheit. Die Folge ist mangelnde Akzeptanz des Wertschöpfungsbeitrages der Unternehmenssicherheit. Mit dem fatalen Ergebnis, dass in Sachen Sicherheit allzu gerne die Aussage vorherrscht: „Dafür haben wir jetzt kein Geld!“ Eben weil der Wertschöpfungsbeitrag von Sicherheit nicht messbar gemacht wird.

In einem Teil der Literatur wird in dieser Situation vorgeschlagen, den Bereich des Business Continuity Managements zu einem „integrierten Krisenmanagement“ auszubauen und so der Unternehmenssicherheit als „Kontinuitätsmanager“ einen stärkeren inhaltlichen Rahmen zu geben. Dazu wird mit dem BSI-Standard 100-4 ein Werk des Bundesamtes für Informationssicherheit bemüht, das maßgeblich von einem IT-Beratungshaus geschaffen wurde und das sicherlich wertvolle Erkenntnisse aus der IT-Betrachtungsebene enthält.

Für den Bereich der Sicherheitsmanagementsysteme liegen allerdings – außer den Überlegungen in Österreich (ONK 252 Corporate Security Management) – derzeit noch keine anerkannten Normen vor. Als Vorbild für ein umfassendes Sicherheitsmanagementsystem lassen sich die ISO 27000 ff. zur Informati-

onsicherheit oder der BS 25999 „Code of Practice for Business Continuity Management“ bzw. der ONR 49000 „Risikomanagement“ heranziehen.

Wie kann ein unternehmensweiter Gesamtanspruch des Sicherheitsmanagements geschaffen und umgesetzt werden? Und wie kann damit der Wertschöpfungsbeitrag von Sicherheit im Unternehmen messbar gemacht werden?

Eine Antwort: Viele Unternehmen besitzen ein ausgeprägtes Qualitätsmanagement. Was liegt also näher, als diese bereits etablierten Methoden – u. a. den PDCA-Zyklus – auf den Sicherheitsbereich zu übertragen sowie Sicherheitsmanagement analog zum Qualitätsmanagement zu entwerfen und später in einem integrierten Managementsystem zu verbinden? Damit könnte zugleich auch der Weg gegangen werden, der in der ONR 49000 und der ISO 31000 hinsichtlich der Einrichtung eines integrierten Managementsystems unter Einbeziehung der Bereiche Qualität, Umwelt, Informationssicherheit sowie Gesundheit und Sicherheit angedeutet wurde.

Verfolgen wir diesen Ansatz weiter, wird es in der Praxis darauf ankommen, zunächst die Sicherheitsziele und die Sicherheitspolitik des Unternehmens festzulegen. In der folgenden Ausarbeitung der erforderlichen Dokumente auf den verschiedenen Ebenen werden die zu behandelnden Themenbereiche abgegrenzt, Verantwortlichkeiten festgelegt und die Sicherheitsprozesse definiert. Neben den organisatorischen, übergreifenden Strukturen werden die einzelnen Themen anschließend mit den verantwortlichen Mitarbeitern dezidiert bearbeitet bis hin zu einzelnen Prozessbeschreibungen. Vorhandene Strukturen, Organisationen und Maßnahmen werden überprüft und soweit möglich in das neue Sicherheitsmanagementsystem überführt.

Bis das vollständige System schließlich implementiert ist, durchläuft es mehrere Qualitätsmanagementzyklen. Der modulare Aufbau stellt

sicher, dass jedes Unternehmen, das diesen Weg geht, tatsächlich ein individuelles, auf seine konkreten Sicherheitsbedürfnisse abgestimmtes System erhält, unter Einhaltung der „Best Practice“-Standards. Damit wird ein Beitrag zur Beantwortung der obigen Frage geleistet, der Wertschöpfungsanteil der Sicherheit wird deutlich, und die Akzeptanz der Sicherheit im Unternehmen wird zumindest nicht weiter sinken. Und nicht zu vergessen: Letztendlich wird bei diesem Ansatz klar, in welchem Anforderungsumfeld sich der erfolgreiche Sicherheitsmanager in der Zukunft bewegen müssen.

Ein Projektbeispiel – die LIFE AG

Wie man bei der Einführung eines prozessorientierten Sicherheitsmanagementsystems vorgehen kann, beschreibt das folgende fiktive Projekt:

Bei unserem Musterunternehmen, der LIFE AG, handelt es sich um ein mittelständisches Familienunternehmen mit ca. 780 Mitarbeitern, davon ca. 640 in der Produktion. Der einzige Produktionsstandort liegt in unmittelbarer Nähe zum Main bei Frankfurt. Das Unternehmen beschäftigt sich mit Entwicklung, Produktion und Vertrieb von elektrisch angetriebenen Werkzeugen für Heim-/Handwerker (z. B. Bohrmaschinen). Der Katalogfertiger mit globalem Vertriebsnetz (70% Vertrieb) hat Tochtergesellschaften in verschiedenen Ländern und unabhängige Importeure in weiteren Staaten. Der gute Markterfolg wird durch hohe Qualität und Lieferfähigkeit erreicht. Termintreue ist auf umkämpften Märkten von hoher Bedeutung.

Dieses Unternehmen hatte in verschiedenen Situationen sehr negative Erfahrungen mit Krisen und insbesondere mit der Presse gemacht. Es war zu weltweiten Produktrückrufen gekommen. Schwierigkeiten bereiteten auch Plagiate und ein Hochwasser des Mains.

Nach diesen Erfahrungen hat die LIFE AG das komplette Sicher-

heitsmanagementsystem prüfen lassen. Dabei wurde festgestellt, dass die vorhandene Sicherheitsorganisation nicht über eine strategische Ausrichtung verfügte, sondern operative Einzellösungen im Vordergrund standen.

Ziel eines umfassenden Projektes ist nun eine Neuausrichtung des Sicherheitsmanagementsystems unter Berücksichtigung strategischer und operativer Komponenten. Die strategische Fachführung für den Hauptsitz und alle betroffenen Tochterunternehmen soll einer zentralen Koordinations- und Fachstelle Sicherheit zugesprochen werden. Die operative Fachführung und Umsetzung bleiben bei den einzelnen betroffenen Bereichen.

Ziel des Projektes ist der Neuaufbau einer Unternehmenssicherheit innerhalb eines prozessorientierten Ansatzes. Dabei wird von folgenden Grundannahmen ausgegangen:

- „Sicherheit“ ist die Voraussetzung für einen effizienten und erfolgreichen Ablauf aller Geschäftsprozesse entlang der gesamten Wertschöpfungskette (Verdeutlichung des Wertschöpfungsbeitrages der Sicherheit).
- Neben dem Schutz von Menschen und anderen wichtigen Schutzgütern ist die möglichst störungsfreie Fortführung des Geschäftsbetriebes (Business Continuity) ein wesentliches Ziel der Sicherheit.
- Eine unternehmensweite Festschreibung von Sicherheitsgrundsätzen ist Voraussetzung für ein gemeinsames Verständnis von „Sicherheit“ und die unternehmensweite Umsetzung.
- „Sicherheit“ ist im geltenden Regelwerk definiert und steht in Einklang mit den Werten der LIFE AG. Vor allem die Werte „Vertrauen“ und „Zuverlässigkeit“ liegen der Sicherheitsphilosophie zugrunde.
- Unternehmensweite Sicherheitsgrundsätze, die diesem Grundverständnis folgen, leisten einen direkten Wertbeitrag für das Unternehmen und bieten klare Orientierung in allen Märkten: den Mitarbeitern der LIFE AG sowie den Kunden, Geschäftspartnern und Lieferanten.

Das unternehmenseinheitliche Sicherheitskonzept ist die Vereinigung aller entscheidenden Stellen in der Sicherheitsarchitektur eines Unternehmens. Statt additiver Konzepte und Teillösungen wird ein ganzheitlicher Ansatz mit einer gemeinsamen Philosophie in allen Ebenen und Bereichen generiert. Sicherheitsmanagement in einer solchen unternehmensweit ausgerichteten Sicherheitsorganisation bedeutet:

- Transparenz über Unternehmensrisiken und die damit verbundenen Chancen unter Einbeziehung aller mit der Bewältigung von Risiken verbundenen Kosten.
- Aufbau von Sicherheitsmanagement als Führungsprozess im Unternehmen, damit die notwendige Transparenz über Organisation, Verantwortlichkeiten, Kompetenzen und Standards sowie Erreichung der notwendigen Führungs- und Mitarbeiterverantwortung durch Richtlinien und Sensibilisierung gewährleistet wird.
- Schaffung von Qualitäts- und Sicherheitsgrundsätzen als Leitfaden für Entscheidungen und persönliches Verhalten sowie Schaffung eines Handlungsrahmens für sicherheitsrelevante Vorgänge oder Vorfälle auf Basis von Standards, mit nachvollziehbaren und wiederholbaren Ergebnissen.
- Kommunikation zwischen Fachbereich und Sicherheitsverantwortlichen mit einem gemeinsamen Verständnis von Geschäftsanforderungen und Sicherheitszielen.
- Optimale Umsetzung von Sicherheitsbelangen, indem angemessene, wirksame und nachhaltige Sicherheitsmaßnahmen ausgewählt werden und diese insbesondere hinsichtlich Gebrauchstauglichkeit unter Berücksichtigung von Kosten-Nutzen-Aspekten an Unternehmens- und Mitarbeiterbedürfnisse angepasst werden.
- Abgrenzung und Zuordnung von Verantwortung hinsichtlich neuer Gefahrenfelder und Vermeidung von Sicherheitsmaßnahmen für subjektiv wahrgenommene Bedrohungen, die kein bedeutendes Risiko für das Unternehmen darstellen.

Konkretisiert man diese grundsätzlichen Ziele auf die konkrete Aufgabe, so ergeben sich Anforderungen in folgenden Punkten:

- Abgestimmte Ausrichtung zwischen den Sicherheitsbelangen und den Business-Anforderungen und damit die Ausrichtung der Sicherheit an der Geschäftsstrategie des Unternehmens.
- Vernetzung von Corporate Governance, Qualitätsmanagement, Risikomanagement, Interner Revision und Unternehmensplanung.
- Aufzeigen und Bewerten von Sicherheitsrisiken und Ableiten von geeigneten Maßnahmen.
- Förderung/Verpflichtung der Kostentransparenz für Sicherheitsanforderungen.
- Frühzeitige Einbeziehung der Sicherheitsinteressen in allen Konzept-, Projekt- und Betriebsphasen.
- Flexibilität der Weiterentwicklung von Lösungen bei gleichzeitiger Gewährleistung eines stabilen Sicherheitsniveaus.

An Geschäftszielen orientiertes Sicherheitsmanagement

Aus diesem Ansatz ergibt sich ein Sicherheitsmanagement, das mit dem Risikomanagementprozess verbunden und somit ein an den Geschäftszielen ausgerichteter Führungsprozess ist. Dieses Sicherheitsmanagement gewährleistet die definierten Sicherheitsstandards bei allen Produkten und Dienstleistungen des Unternehmens.

Aus diesem Grundprozess ergeben sich aber insofern auch Anforderungen aus begleitenden Prozessen. Denn nur ein integrales Sicherheitsmanagement, welches

- (1) sowohl das Risikomanagementsystem des Unternehmens als Frühwarnsystem für die präventive Herleitung und Bestimmung der notwendigen Sicherheitsmaßnahmen nutzt als auch
- (2) auf das Notfall- und Krisenmanagementsystem setzt, um auch bei besonders zeitkritischen oder krisenhaften Situationen die Hand-

lungsfähigkeit des Unternehmens sicherzustellen, ist eine geeignete Basis, um die Geschäftskontinuität langfristig zu sichern. Und schließlich ergibt sich eine besondere Anforderung

(3) bei den Umsetzungsprozessen der Unternehmenssicherheit aus Kosten- und Effizienzgesichtspunkten. Damit wird ein wesentlicher Beitrag zur Reduzierung der Gesamtkosten erbracht, die zur Risikobehandlung ausgegeben werden müssen (total cost of risk).

Für die Ausgestaltung des hier dargestellten Modells für den Ausbau der Unternehmenssicherheit ist eine Vielzahl von Schritten erforderlich: Ausgegangen wird dabei von der Erstellung eines Handbuchs für die Unternehmenssicherheit, in dem u. a. die entwickelte Sicherheitspolitik und die Sicherheitsstrategie ebenso festgehalten werden wie die grundsätzliche Organisation, die Ablauforganisation, die Verantwortungen und die Kompetenzen. Auf dieser Basis werden dann die vielfältigen weiteren Module umgesetzt, die für die Implementierung erforderlich sind. Dazu gehören, um einzelne Elemente zu benennen:

- ein klar gegliedertes System für die Dokumentenstruktur,
- ein ausgeprägtes Berichtssystem,
- ein definiertes Meldesystem für die Erfassung kritischer Ereignisse,
- eine klare Definition von Sicherheitsstandards unterschiedlicher Gefährdungsklassen und
- ein auswertbares Erfassungssystem für etwaige Abweichungen von den Sicherheitsstandards.

Angesichts der hohen Bedeutung des Risikofaktors Mensch sollte dieses Gesamtprogramm auch Elemente zur Verbesserung des Risikobewusstseins enthalten.

Vorgehensweise mit den klassischen Phasen des Projektmanagements

Für die hier vorgesehene Weiterentwicklung des unternehmensweiten Sicherheitsmanagements (SMS) bei

der LIFE AG würden die klassischen Phasen aus dem Projektmanagement verwendet:

Phase 1: Studie

Bei einer grundlegenden Studie wurden zunächst eine Ist-Aufnahme und die Beurteilung des geplanten Soll-Zustandes vorgenommen. Der abschließende Bericht sollte eine Darstellung des Ist-Zustandes und Würdigung der vorgesehenen Maßnahmen für den Soll-Zustand enthalten. Weiter sollten mögliche Lösungsansätze dargestellt und ein Antrag für die Umsetzung der besten Variante formuliert werden.

Phase 2: Projektierung

In der Projektierung wird nun ein Plan für die Umsetzung der zukünftigen Soll-Prozesse dargelegt. Dazu werden in verschiedenen Workshops zunächst ein Grobkonzept für die Aufbau- und Ablauforganisation, die erforderlichen Instrumente, Hilfsmittel und Ressourcen sowie ein Modell für eine Alarmorganisation entwickelt. Für dieses Grobkonzept wird dann eine konkretere Umsetzungsplanung mit den Inhalten Vorgehen, Termine, Inhalte, Kosten und Projektqualitätsmanagement erstellt und schließlich in einen Projektplanungsantrag umgesetzt.

Phase 3: System- und Organisationsaufbau

Auf der Basis des verabschiedeten Grobkonzeptes erfolgt nun die Erarbeitung des Detailkonzeptes mit den Spezifikationen der Sicherheit und der entsprechenden Prozesse, einer Detailplanung für die Implementierung, die Umsetzung der Prozesse und mit der entsprechenden Schulung für die verantwortlichen Mitarbeitenden.

Phase 4: Umsetzung Systemaufbau, Ablauforganisation

Die Umsetzungsphase ist davon geprägt, dass nunmehr die einzelnen Elemente für den Systemaufbau

und die Ablauforganisation umgesetzt werden. In internen Workshops werden die Prozesse der Unternehmenssicherheit ausgearbeitet. Weiter werden die notwendigen Schnittstellen zu anderen Fachbereichen bestimmt, ein risikoorientiertes internes Kontrollsystem mit geeigneten Kontrollpunkten, welche in das Berichtswesen zu integrieren sind, konzeptioniert sowie das generelle Berichtswesen und die Kommunikationswege Top-down und Bottom-up organisiert.

Phase 5: Organisations- und Systemüberführung in die ordentliche Ablauforganisation

Bei der Überführung der entwickelten Organisation und des Systems in die ordentliche Ablauforganisation werden die erforderlichen Maßnahmen koordiniert und die zuständigen Mitarbeitenden unterstützt und geschult. Etwaige bei der Einführung auftretende Qualitätsmängel des Systems werden dokumentiert und ein Maßnahmenkatalog für die Beseitigung der Mängel erstellt.

Die Ergebnisse werden in einem Projektbericht zusammengefasst und in einer entsprechenden Präsentation werden Meilensteine für das weitere Vorgehen definiert.

Phase 6: Nachbereitung / Abschluss

Der Abschluss des Projektes erfolgt durch eine Erfolgsanalyse mit einer Erhebung der Kundenzufriedenheit, einer Nachbesserung der erkannten Schwächen des Systems und der Erstellung eines Vorgehenskonzeptes für die nachhaltige Pflege und Systemfortführung.

Fazit

Solange es sich die Unternehmen leisten können, die Corporate Security und die Safety in getrennten Bereichen zu organisieren, scheint der wirtschaftliche Druck noch nicht hoch genug zu sein. Gut beraten ist derjenige Sicherheitsverantwortliche, der nicht versucht, diesen klassischen Widerspruch aufzulösen.

Die Widerstände bei einem solchen Unterfangen sind erheblich, sie zeigen jedoch, dass die handelnden Personen auch weiterhin in den klassischen operativen Anforderungen verhaftet sind und sich einem prozessorientierten Denken noch nicht geöffnet haben. Nur durch das Klarstellen der Prozesse der Unternehmenssicherheit und deren verbindliche Implementierung in alle betroffenen Bereiche können erhebliche Vorteile bei den Prozesskosten realisiert werden, ohne dass die Qualität der Sicherheit nachlässt.

Dabei liegt ebenfalls auf der Hand, dass ein Sicherheitsverantwortlicher, der diesen Weg einschlägt, über weitergehende fachliche und persönliche Kompetenzen verfügen muss, als dies heute häufig der Fall ist. Neben sehr guten Sicherheitskenntnissen wird es insbesondere auf eine sehr gute Beherrschung des Prozess- und Projektmanagements ankommen. Zudem sind sehr gute Kenntnisse der anwendbaren nationalen und internationalen Standards und insbesondere des Risikomanagements erforderlich.

Auf dieser Basis kann dann ein Sicherheitsmanagementsystem geschaffen werden, bei dem die handelnden Personen den kritischen kollegialen Dialog mit der Internen Revision, dem Controlling, dem Risikomanagement oder dem Business Continuity Manager nicht scheuen müssen, sondern darauf bestehen werden.

Es wird für Sicherheitsverantwortliche darauf ankommen, sich auch mit Themen zu beschäftigen, die auf den ersten Blick nicht im unmittelbaren Zusammenhang mit den klassischen Sicherheitsthemen stehen. Damit kann der Beitrag der Sicherheit zur Wertschöpfung deutlich gemacht und der Stellenwert der Sicherheit im Unternehmen gefestigt werden.



Der Autor dieses Beitrags, **Dr. jur. Klaus Bockslaff, LL.M.**, ist Gründer und Managing Partner der Verismo GmbH, Küsnacht (Schweiz) und der Verismo Consulting GmbH, Hassloch (Deutschland). Er arbeitet als Wirtschaftsberater und Management Coach. Vorher war er als Vorstand und Risikomanager in der Versicherungswirtschaft und als Senior Manager bei Arthur Andersen tätig. Seine Schwerpunkte sind die Einrichtung und Vertiefung integrierter Managementsysteme, speziell auf den Gebieten des Risiko-, Sicherheits- und Krisenmanagements.

Kontakt:
klaus.bockslaff
@verismo.ch