Management der integralen Sicherheit ist möglich

Die Themen der integralen Sicherheit sind vielfältig. Umso wichtiger ist es, sich auf die Wesentlichen zu konzentrieren und diese effizient umzusetzen. Mit einem integrierten Managementsystem (IMS) ist das möglich. Wie kann das gehen und wo sind die Grenzen?

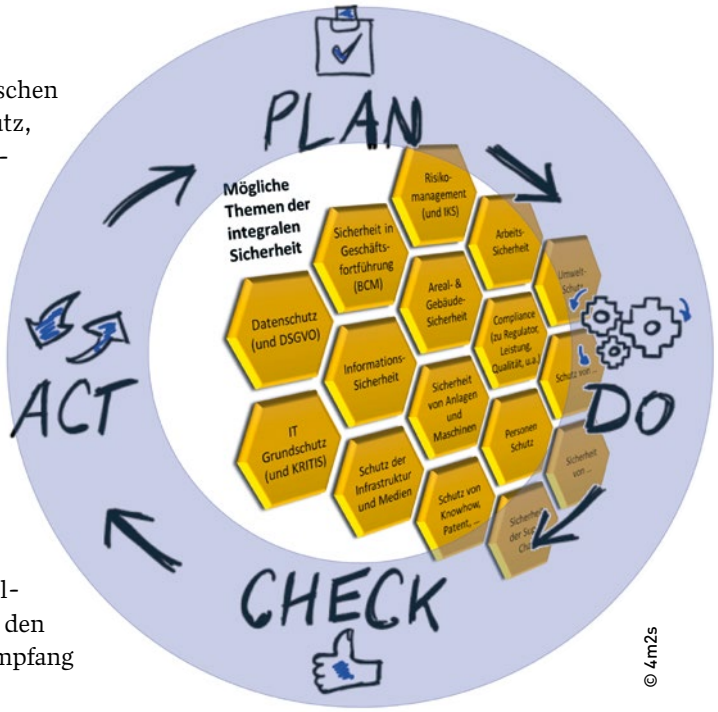
Almut Eger

Im Artikel «Worthülse oder grosser Nutzen» (SF-Ausgabe 3/20, ab S. 33) haben wir dargelegt, warum es wichtig ist, Anforderungen an «die Sicherheit im Unternehmen» integral zu verstehen, also den unterschiedlichen Bedarf an Schutzmassnahmen und Konzepten in einer Gesamtsicht zu verstehen und zu koordinieren. «Was» getan werden könnte, wurde damit ersichtlich. Auf das «Wie» gehen wir in der Folge ein.

Das Themenfeld «integrale Sicherheit» will zielgerichtet die unterschiedlichen Anforderungen an einen Schutz von Werten und Gebäuden, Menschen, Gütern, Lieferwegen usw. erreichen. Der Schutz all dieser Assets ist in verschiedenen Unternehmenseinheiten verankert, wird von mehreren Menschen ernst genommen und gesteuert. Damit sich Vorgaben nicht wiedersprechen, nicht gegenläufige Ziele verfolgt werden oder Dinge nicht drei Mal gemacht werden, ist es wichtig, ein koordinierendes Management der integralen Sicherheit zu leben. Denn schliesslich geht es um die korrekte Leistung gegenüber dem Kunden.

Das Management der integralen Sicherheit besteht aus einem Konglomerat von ineinandergreifenden Faktoren und Akteuren. Hierzu gibt es ein prominentes Beispiel: Covid-19. Die grosse Herausforderung in der jetzigen Zeit ist unter anderem eine erweiterte Quersicht zu Themen der integralen Sicherheit – wir greifen in der Folge zwei Themen heraus, um das Management der integralen Sicherheit beispielhaft zu erläutern.

1. Physische Sicherheit von Gebäuden und Arealen: Es geht nun nicht mehr «nur» um die klassischen Themen wie Brandschutz, Zutrittsfragen, Informationssicherheitsmassnahmen, sondern zusätzlich um die Frage «Wie lassen wir das Virus draussen vor der Tür?». Einem Thema, zu dem nun weitere Verantwortliche beigezogen werden müssen, zum Beispiel für Arbeitssicherheit und Gesundheitsschutz, für Personalmanagement/HR, für den Kundenbereich und Empfang etc.



© 4m2s

Ein effektives Managementsystem zeichnet sich durch einen immerwährenden Zyklus aus.

Und somit hat man eine Vielzahl von Verantwortlichen, die parallel aktiv sind und für eine integrale Sicherheit koordiniert werden müssen. Relevante Fragestellungen können sein:

- Wer verantwortet was, mit welchen Zielsetzungen?
- Wissen wir voneinander, wer was tut respektive eben nicht tut? Wer ist im Thema zusätzlich aktiv, intern im Unternehmen und extern?
- Sind die gegenseitigen Erwartungen bekannt und konsistent, damit insgesamt die Sicherheitsanforderungen erfüllt werden können?
- Und last but not least: Wer steuert die Prioritäten und die Wichtigkeit, wenn sich Ziele widersprechen oder nicht für alle Aktivitäten ausreichend Ressourcen zur Verfügung stehen sollten?

Wichtig sind alle Aspekte, sie sind gleichwertig und im Kontext der integralen Schutzforderung für die integrale Sicherheit der Unternehmung zu verstehen.

Es ist also entscheidend, eine koordinierende Stelle zu haben, die obige Fragen steuern und Friktionen stufengerecht zur Entscheidung und Lösung bringen kann.

Und somit wäre es auch zielführend, ein(!) integriertes Managementsystem zu haben, in dem die unterschiedlichen Anforderungen der physischen Sicherheit koordiniert und Schutzmassnahmen so getroffen werden können, dass alle Bedürfnisse angemessen abgedeckt werden.

2. Einhalten eines Lieferversprechens, inklusive der qualitativen und rechtlichen Vorgaben: Die Covid-19-Situation hat gezeigt, dass spezifische Vorgaben zu einem Lieferversprechen nicht einseitig

verstanden werden können. Es ist die ganze Wertschöpfungskette, die ins Gewicht fällt. Mit dem Wegfallen von Lieferanten mussten beispielsweise neue Rohstoffe auf dem Markt bezogen werden von Quellen, die mangels verfügbarer Zeit nicht wie gewohnt getestet werden konnten. Es war ein Managemententscheid, eine neue Bezugsquelle dennoch zuzulassen. Dieser Entscheid kann jedoch auch eine tickende Zeitbombe für das Unternehmen sein: Was, wenn das Material die erforderliche Belastung nicht aushält? Die Qualität kann zwar primär sichergestellt werden, hält aber im Zeitverlauf das Versprechen nicht.

Ein integriertes Managementsystem der integralen Sicherheit kann das Auftreten heikler Situationen nicht verhindern. Aber es kann dazu beitragen, dass alle relevanten Faktoren, die für eine Entscheidung berücksichtigt werden müssten, auch bekannt sind und in der richtigen Priorität und Gewichtung einfliessen können. Dass also in unserem Fall die relevanten Faktoren, die zu ausreichender Lieferqualität führen, abgerufen werden können und als Entscheidungsgrundlage in der Quersicht und der gegenseitigen Abhängigkeit vorliegen. Zum Beispiel zu Material, Fertigungs- und Lieferprozess, Know-how und Ausbildung, erforderlichen Zertifikaten für Ausgangsmaterialien, Zwischenprodukten, Arbeitsschritten und Endprodukten etc.

Zertifikate sind zum Beispiel an die Leistungserbringung in einem ganz bestimmten Prozess gebunden. Ändert dieser Prozess, weil in der Bearbeitungs- und Lieferkette wegen Covid-19 andere Player/Partner mitwirken, so kann deshalb ein Zertifikat/Gütesiegel wegfallen. Auch das muss via integriertes Managementsystem erkannt werden, bevor daraus ein Compliance-Fall wird.

IMS als steuernde Einheit der integralen Sicherheit

Ein integriertes Managementsystem, das relevante Informationen auch für solch entscheidende Momente vorhalten kann, ist enorm viel wert, muss aber im Alltag im Unternehmen voll implementiert sein. Die Basis für diese Implementierung sind häufig Prozessmanagementsysteme, in denen alle weiteren Informationen verankert oder verlinkt werden können. So können auch stufengerecht Informationen zur Verfügung gestellt werden: von der operativen, stark granularen Sicht pro Prozessschritt bis zur End-to-End-Betrachtung über Prozesse und Abteilungen hinweg. Verankert sind dann nicht nur Anweisungen und Arbeitsvorhaben, sondern auch Hinweise zu kritischen Prozessschritten, Ressourcen und Abhängigkeiten. Im Detail kann es da auch um Vorgaben wie zum Beispiel für Alleinarbeit gehen, um Temperatur und Feuchtigkeit für eine qualitativ einwandfreie Verarbeitung der Materialien. Werden diese Dinge nicht eingehalten, so entsteht relativ schnell ein Garantiefall, reputativ heikle Situationen oder gar eine heikle Governance-/Compliance-Situation.

Aus Tabelle 1 ist eine kurze, unvollständige Zusammenstellung ersichtlich, woher die Informationen zu integraler Sicherheit stammen können und wer dafür zuständig sein könnte. Die Themen und Rollenbezeichnungen sind «schematisch» zu verstehen und müssen auf die eigene Unternehmenssituation adaptiert werden.

Integriertes Managementsystem im PDCA-Zyklus

Ein integriertes Managementsystem der integralen Sicherheit soll für alle spezifisch einbezogenen Akteure gelten. Es soll Auskunftsbasis sein für den Alltag – und ebenso für schwierige, ausserordentliche Situationen, in denen verstanden werden muss, welche Ressourcen, Prozessschritte und Abhängigkeiten nun in Gefahr sind und womit die optimale Sicherheit der Unternehmung fokussiert werden kann, im Einzelnen wie in der Gesamtheit der erforderlichen Sicht, eben der integralen Sicherheit.

Um das sicherstellen zu können, empfiehlt sich die Steuerung in einem integrierten Managementsystem im PDCA-Zyklus: Ein effektives Managementsystem zeichnet sich durch einen immerwährenden Zyklus aus, in dem Planung (P), Umsetzung (D), Überprüfung (C) und darauf basierende Korrekturmassnahmen und erneute Zielsetzungen (A) die kontinuierliche Weiterentwicklung über die Jahre auszeichnet. Mit diesem Zyklus, auch Demingkreis oder PDCA-Zyklus genannt, kann Bestehendes verbessert und Neues kontinuierlich eingebracht werden. Und genau das ist nötig für ein effizientes und effektives Steuern der integralen Sicherheit.

Im Folgenden zeigen wir beispielhaft, was pro Schritt getan respektive welche Ergebnisse erzielt werden sollen:

Plan:

1. Erkennen der Anforderungen an eine Lieferleistung, ein Produkt, einen Verarbeitungsschritt. Und zwar von allen Themen der integralen Sicherheit (siehe SF-Ausgabe 3/20, ab S. 33)

2. Erkennen der kritischen Prozesse und/oder Ressourcen, um diese Leistung, dieses Produkt, diesen Verarbeitungsschritt in erforderlicher Qualität und Zeiteinheit erbringen zu können.

3. Erkennen und Planen von Massnahmen, um das georderte Sicherheitslevel, Schutzlevel, Lieferversprechen usw. erbringen zu können.

Ergebnis: Mit diesen Schritten wird im Unternehmensalltag bekannt, aus welchen Disziplinen und Verantwortungen welche Anforderungen gestellt werden.

Beispiel physische Sicherheit eines Hauptgebäudes mit Empfang: Vorgaben aus Facility Management, Arbeitssicherheit, HR und Projektplanung für den neuen Kundenbereich koordinierenn.

Hinweis: Mit der Methodik des Business Continuity Managements können diese Fragestellungen einfach und rasch beantwortet werden.

NUTZEN EINES IMS FÜR DIE INTEGRALE SICHERHEIT

Nutzen eines integrierten Managementsystems IMS für die integrale Sicherheit: Änderungen bestimmen unser Leben und dasjenige der Kunden, Lieferanten, Provider, Zulieferer und Regulatorien. Je besser ein Unternehmen die Gesamtheit der Anforderungen an eine sichere Lieferleistung kennt, umso rascher und besser können diese auch in schwierigen Zeiten unterstützt und geschützt werden. Und umso effizienter können erforderliche Veränderungen erkannt, nötige Massnahmenfelder aus dem IMS abgerufen und mit den zuständigen Stellen bearbeitet werden.
Mit integriertem Managementsystem werden also Erkenntnisse aus Business Continuity Management, Riskmanagement, Facility Management, Arbeitssicherheit und Gesundheitsschutz, Informationssicherheit, Governance- und Compliance-Anforderungen und vieles mehr koordiniert und zielgenau zur Verfügung gestellt.

Thema	Beispiele	Verantwortliche
Business Continuity Management BCM	Kritische Prozessschritte, Ressourcen, Abhängigkeiten intern und extern	BC-Manager/in
Arbeitssicherheit & Gesundheitsschutz	Vorgaben pro Arbeitsgattung	• AS/GS-Verantwortliche/r • HR • Führungskräfte spezif. Einheiten (Bsp. Empfang)
Facility Management, Gebäudesicherheit	Vorgaben Zutrittslösungen, in Abhängigkeit von Badges, Zeiterfassung etc.	• Facility-Manager/in • SiBe
Produktmanagement	Compliance-Vorgaben für Produkteinsatz (Verkauf, Transport, Montage, Betrieb, Entsorgung)	• Produktmanager/in • Führungskräfte spezif. Einheiten (Bsp. Montagegruppe)
Informationssicherheit	Schutz von Daten, Zugriff auf Applikationen, Schutz von Dokumenten	• CISO • ISMS-Beauftragte/r • ...
Umweltschutz und Nachhaltigkeitsmanagement	Vorgaben für Produkte, Arbeitsarten etc.	• UMS-Beauftragte/r
Compliance und /oder Governance	Einhalten von Lieferversprechen, Marktaktivitäten etc.	• Legal & Compliance Manager/in

Tabelle 1: Ein Alleingang einer dieser Disziplinen würde zu unkoordinierten Massnahmen führen, womit sich getroffene Schutzmassnahmen auch wieder gegenseitig aufheben können.

Do:

1. Umsetzen von Massnahmen zum Schutz eines Gebäudes vor unberechtigtem Zutritt, zum Beispiel wenn wegen Homeoffice die normale Besetzung nicht da ist, inklusive Empfang. Wie können Kunden bedient werden – einfach auf anderen Kanälen? Der Ideen sind viele, aber welche ist auch konform zu allen Anforderungen? Inklusive der erforderlichen Schulungen, Einweisungen und Einhaltung von gesetzlichen Vorgaben? Spielt auch Datenschutz eine Rolle?

2. Festlegen der Verantwortlichkeiten für die einzelnen Themen, aber auch für die Gesamtsicht der Umsetzung.

Check:

1. Testen und messen: «Wer misst, misst Mist.» Dieser geläufige Spruch muss sehr ernst genommen werden. Getestet werden sollen Massnahmen, die dazu gedacht sind, die integrale Sicherheit zu erhöhen. Folglich muss der Test eine Antwort darauf liefern, ob die Massnahmen auch wirklich dieses Ziel erreichen. Und der Test soll erkenntlich machen, was weiter zu tun ist, um integrale Sicherheit im gewünschten Mass zu erreichen.

Dasselbe gilt für Messkriterien und -ergebnisse: Sie sollen ein Gradmesser sein, ob die angestrebte integrale Sicherheit erreicht werden kann, wo am häufigsten Fehler auftreten usw.

Test- und Messergebnisse sind eine Basis für die Steuerung der integralen Sicherheit.

2. Beüben: «Nur wer übt, findet die versteckten Fehler.» Integrale Sicherheit kann nicht vollends geplant werden. Sie hat zwar einen hohen Planungsteil, aber einen ebenso wichtigen Erfahrungsteil, der in heiklen Situationen ein enormes Gewicht bekommt. Die Erfahrung, was nun wichtig und prioritär ist, kann nicht gänzlich erarbeitet oder eingeplant werden. Geplant werden können oftmals nur die Hinweise darauf. Deshalb sind die Übungserkenntnisse enorm wichtig und dienen ebenso der Steuerung der integralen Sicherheit. Insofern gilt: keine integrale Sicherheit ohne Tests und Übungen.

Act:

1. Das Heikelste der integralen Sicherheit sind die versteckten Mängel, Minderleistungen und Beinahe-Unfälle. Sie passieren täglich und werden damit auch als «normaler Bestandteil des Alltags» eingestuft. Die Herausforderung ist deshalb, sie zu erkennen, bevor ein Sicherheitsrisiko daraus entsteht. Das ist möglich mit der Quersicht auf die integrale Sicherheit der gesamten Wertschöpfungskette, mit den relevanten Akteuren und Ergebnissen aus Messungen, Tests und Übungen.

Sicherheit kostet Geld. Fehler kosten in der Regel noch mehr Geld. Die Steuerung der integralen Sicherheit soll so ausgestaltet sein, dass via die Schritte in Plan, Do und Check ausreichend Erkenntnisse vorliegen, um hier, im letzten Schritt «Act» erkennen zu können, ob die getroffenen Massnahmen der integralen Sicherheit greifen und ein möglichst hoher Schutz der kritischen Leistungseinheiten besteht. Aber auch, wo allenfalls Korrekturmassnahmen nötig sind.

2. In einem Management Review sollen alle Erkenntnisse zusammengefasst werden, um auf Stufe Gesamtverantwortung das Erreichte reflektieren und neue Ziele für die nächste Periode setzen zu können.

Fazit

Mit einem integrierten Managementsystem (IMS) können die Vorgaben für integrale Sicherheit der Unternehmung erstens in der Quersicht aller Anforderungen erkannt werden, zweitens im Alltag wie in heiklen Situationen spezifisch zusammengezogen und daraus priorisierte Massnahmen abgeleitet werden.

Für die Pflege und Weiterentwicklung dieser Anforderungen bleiben die jeweiligen Abteilungen und beauftragten Stellen verantwortlich. Die Steuerung erfolgt zentral koordiniert.

Das IMS sollte im PDCA-Zyklus aufgebaut werden. Damit besteht die Möglichkeit, Änderungen einfliessen zu lassen – ohne das System per se überarbeiten zu müssen.

Ein IMS schafft die übergeordnete Quersicht über alle Anforderungen der integralen Sicherheit und damit eine schlanke Methode, um all die unterschiedlichen Vorgaben koordinieren und bei Bedarf priorisieren zu können. ■

ALMUT EGER
BCM-Managerin, Krisenmanagerin
Geschäftsleitung
4 Management 2 Security GmbH