

Die Relevanz der Trennung von Governance & Management in der Sicherheitsorganisation

von Franziska Englert
04. Januar 2023

Die Führung der Sicherheitsorganisation und das Sicherheitstagesgeschäft wird in den meisten Unternehmen von, durch die Unternehmensführung bestimmten, Sicherheitsexperten unter der Leitung eines Chief Security Officer (CSO), Head of Global Security oder Leiter Unternehmenssicherheit übernommen.

In der Praxis findet an dieser Stelle häufig, weder in der IT-Sicherheit noch im Sicherheitsmanagement (Safety- und Securitybereich), eine klare Trennung der Verantwortlichkeiten, Aufgaben und Instrumenten von Governance und Management (Führung und Umsetzung) statt.

Hier besteht in den meisten Unternehmen Optimierungsbedarf zur Steigerung des Wirkpotenzials der Sicherheitsorganisation und für die Vermeidung von Effizienz- sowie Effektivitätsverluste um im Ergebnis mehr Resilienz im Unternehmen zu erreichen.

Haben Sie Governance und Management bisher synonym betrachtet ?

Damit sind Sie nicht alleine, die Verschmelzung der Verantwortlichkeiten und Aufgaben sowie Vermischung der Methoden und Werkzeuge aus beiden Welten findet in Unternehmen fachübergreifend statt. Mit entsprechenden Folgen.

Nachstehend sind die ursächlichen Faktoren für die Vermischung der Zuständigkeiten im Sicherheitsbereich und häufige negative Auswirkungen beschrieben:

- **Keine wissenschaftlich fundierte Herangehensweise an Sicherheitsmanagement allgemein, in Kombination mit Unkenntnis über die Funktion und Wirkung von Governance & Management sowie ihrer Trennung.**

Das Wirkpotenzial der Sicherheitsorganisation und der notwendige Durchgriff sind eingeschränkt. Die Kosten sind häufig versteckt: Ressourcenverschwendung (Doppelarbeit, Einsatz wirkungsloser Sicherheitstechnik und hohe Kosten), unerkannte oder nicht zu behebende Sicherheitslücken, mangelhaftes Krisenmanagement mit Reputationsschäden,

...

- **Sicherheit wird von der Unternehmensführung kein Stellenwert (z.B. in Form einer Stabsstelle und Managementfunktionen) eingeräumt.**

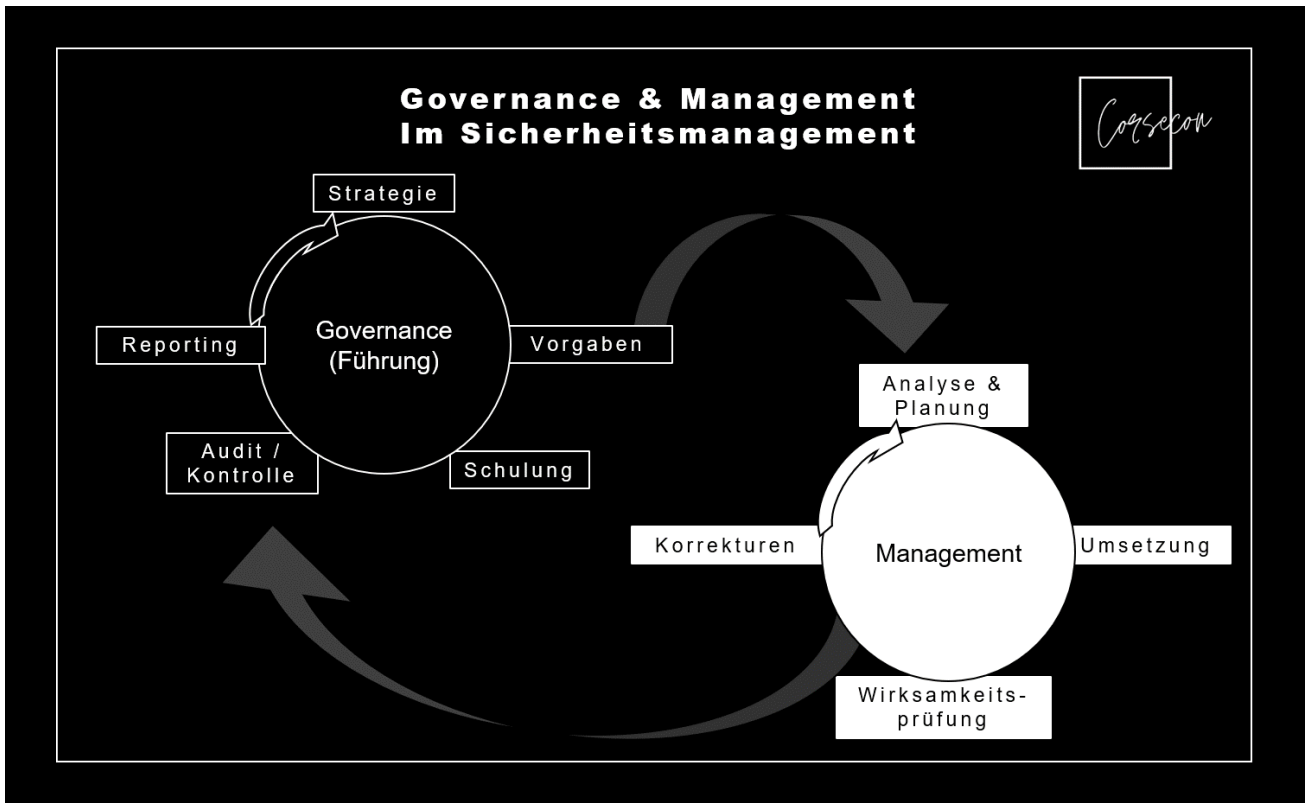
Damit fehlt die Basis für Sicherheitskultur im Unternehmen sowie ausreichend Ressourcen und Budget für die Sicherheitsorganisation. Die direkte Folge ist die Vermischung der Zuständigkeiten und Aufgaben aus den Bereichen Governance und Management, alles muss und wird, teilweise wider besseren Wissens, von den wenigen Sicherheitsexperten in einer Abteilung und in Funktionsunion übernommen.

- **Sicherheitsverantwortliche haben keine Weisungsbefugnisse.**

Häufig herrscht ein geringes Kompetenzniveau in der Sicherheitsorganisation. Zusammengewürfelte „gewachsene“ Sicherheitsabteilungen aus ehemaligen und nicht adäquat qualifizierten aber „günstigeren“ Mitarbeitern anderer Abteilungen, sind in Kombination wenig leistungsfähig und den komplexen Anforderungen häufig nicht gewachsen. Auch hieraus resultiert häufig geringes Vertrauen der Unternehmensführung in die Organisation. Den Verantwortlichen wird in Folge lediglich eine reine Beratungsfunktion zugestanden. Das führt zu unterschiedlicher Interpretation, Varianzen in der Umsetzung, Zuständigkeitsvakua und Kompetenzgerangel.

Die Prinzipien der allgemeinen guten Unternehmensführung verlangen die Trennung von Steuerung und Umsetzung in allen Bereichen.

Der Reifegrad der Prozess- und Führungsstrukturen hängt maßgeblich davon ab inwieweit eine Unterscheidung der Funktionen und entsprechende Ausgestaltung des Aufbaus- und der Abläufe vorliegt.



Governance

Governance ist als gute Unternehmensführung im Rahmen der ESG-Kriterien (Environment, Social und Governance) bekannt, lässt sich aber auch auf kleinerer Ebene auf die Führung eines Geschäftsbereichs, wie beispielsweise der Sicherheitsorganisation, beziehen.

Sie bildet den rechtlichen und faktischen Rahmen zur Organisation und Überwachung der Sicherheit im Unternehmen.

Die Verantwortlichkeit dafür liegt grundsätzlich bei der Unternehmensführung und kann nicht delegiert werden, die Zuständigkeit für die Aufgaben jedoch auf eine oder mehrere andere Funktionen übertragen werden.

Im Governanceprozess wird auf Basis der Geschäftsanforderungen und allgemeinen Unternehmensstrategie die Sicherheitsstrategie definiert sowie die notwendigen Vorgaben für die Organisation, z.B. Sicherheitsverantwortliche oder (lokale) Abteilungen mit Sicherheitsaufgaben definiert. Dazu zählen beispielsweise die Gestaltung der Aufbau- und Ablauforganisation und ergänzende Melde- und Berichtswege. Risikoanalyse-Methoden und Sicherheitskonzeptgrundlagen werden in Richtlinien und Leitfäden definiert um ein einheitliches Sicherheitsniveau zu schaffen. Die Sicherheitsverantwortlichen und Mitarbeiter werden durch Schulungen in die Lage versetzt die Vorgaben umzusetzen.

Die Auditierung der Umsetzung des Sicherheitsmanagements bildet den Ist-Stand und Fortschritt zur Erreichung der Ziele objektiv ab und zeigt Optimierungspotenziale und Sicherheitslücken auf. Diese werden im Reporting an die Unternehmensführung übermittelt...

So kann durch die Unternehmensführung, respektive den CSO, steuernd eingegriffen werden um die gesetzten Ziele zu erreichen und die Vorgaben durchzusetzen. Ziel ist die Reduktion von

Haftungsrisiken, Schäden und Missmanagement und die Sicherstellung der Erreichung der allgemeinen Geschäftsziele.

Management

Das Management setzt die Vorgaben um und steuert das operative Tagesgeschäft, beispielsweise Prävention, Fallbearbeitung und Problemlösung vor Ort. Es bedient sich dabei der geschaffenen Strukturen und geschulten Sicherheitsexperten.

Im Managementzyklus wird klassisch die Differenz zwischen den gesetzten Anforderungen und dem Ist-Zustand analysiert und darauf aufbauend passende Maßnahmen zur Umsetzung geplant. Dies umfasst alle für das Unternehmen relevanten Sicherheitsbereiche wie z.B. Business Continuity Management (BCM), Bedrohungsmanagement oder Reisesicherheit.

Die Wirksamkeitsprüfung, welche meist jährlich anhand der gewonnenen Daten über Vorfälle und entstandene Kosten, Tests und Übungen durchgeführt wird, identifiziert die Maßnahmen bei denen zur Erreichung der Ziele Korrekturen vorgenommen werden müssen.

Nachteile häufiger Praxis

Gibt es für Sicherheit lediglich eine Abteilung, erstellt diese meist sowohl die für sie geltenden Vorgaben und führt im Anschluss die Kontrolle der Einhaltung durch. Als Konsequenz ist das Phänomen zu beobachten, dass unbewusst die Vorgaben an die (voraussichtlichen) Ergebnisse angepasst oder die Ergebnisse passend zu den Vorgaben ermittelt werden, statt die erreichten Fortschritte anhand gesetzter Vorgaben objektiv zu messen.

Erschwerend hinzu kommt, dass meist nur einzelne Elemente aus dem Aufgabenspektrum umgesetzt werden.

In der Governancepraxis werden überwiegend die Bereiche Schulung, Audit und Reporting vernachlässigt, im Management finden Wirksamkeitskontrolle und darauf basierende Korrekturen wenig Beachtung.

Letzteres geschieht häufig in Ermangelung der Definition valider Messgrößen für Sicherheitsmaßnahmen (KGIs und KPIs), wiederum einem Versäumnis der Führung.

Reporting muss von der, für aus Sicherheitslücken resultierende Schäden haftenden, Unternehmensführung eingefordert werden. Nur so bleibt sie über Risiken des Unternehmens und die Wirksamkeit der teuer installierten Sicherheitsorganisation informiert und hat die Möglichkeit steuernd einzugreifen und Missmanagement zu erkennen.

Für unregelmäßige (Sonder-)audits von Sicherheitsmaßnahmen oder Strukturen wird üblicherweise die interne Revision beauftragt, die jedoch nur diesen isolierten Part übernimmt und somit lediglich Objektivität suggeriert, statt sie tatsächlich zu bieten.

Beispielsweise wird im Fall der zur Prüfung angelegten Maßstäbe bei näherer Betrachtung klar, dass sie aus der zu prüfenden Organisation stammen. Bei der Betrachtung aller Führungsaufgaben wird deutlich, dass die Revision keine anderen, insbesondere sich einem Audit anschließende Führungsaufgaben, übernehmen kann und damit etwaig ermittelte Ergebnisse nicht als Korrektiv im Governancezyklus wirken (können). Alle Führungsaufgaben müssen, ebenso wie die Managementaufgaben, heute zwingend von Personen mit Sicherheitssachverstand übernommen werden, was die Auslagerung einzelner Kernaufgaben verbietet.

Entwurf einer praxistauglichen Sicherheitsorganisation

Eine gelungene wirksame Sicherheitsorganisation kann von einer, durch die Unternehmensführung eingerichtete Stabsstelle für Sicherheit, unter der Leitung eines CSO, gestaltet werden, die je nach Unternehmensgröße mit mehreren Mitarbeitern ausgestattet ist. Sie übernimmt die Governancefunktion.

Dem Bereich Schulung kommt dabei große Bedeutung zu. Die Teilaufgaben reichen von der Vorgabe und Bewertung der Kompetenz der in der Organisation eingesetzten Sicherheitsexperten, über die Umsetzung von Awareness-Programmen zur Förderung einer Sicherheitskultur für alle Mitarbeiter, hin zu Schulungen für Fachspezialisten und der besonderen Aufbauorganisation Krisenstab.

So werden die für Management und operative Umsetzung Zuständigen, durch die Vermittlung von Methodenkompetenz, des aktuellen Stands der Wissenschaft, der Anwendung der Richtlinien und Leitfäden sowie Wissen zur Umsetzung von Best Practices und Erkenntnissen aus der Organisation, unterstützt.

Das Management kann, abhängig von der Unternehmensgröße und Präsenz in den Regionen der Welt, unterschiedlich ausgestaltet werden.

- Eine Option ist die Funktion zentraler Sicherheitsmanager, in Ergänzung zu Standortsicherheitsverantwortlichen oder benannten Sicherheitsverantwortlichen in relevanten Abteilungen (z.B. Travel- und Eventmanagement, ...), zu schaffen. Die zentralen Sicherheitsmanager zeichnen für verschiedene Regionen der Welt verantwortlich und koordinieren die Umsetzung der Governancevorgaben für alle Sicherheitsbereiche. Nebenbei bilden sie die Schnittstelle zwischen Governance und Sicherheitsmanagement vor Ort.

Als Anlaufstelle zur Beratung unterstützen sie die Standortverantwortlichen bzw. Sicherheitsexperten der Fachabteilungen im operativen Geschäft vor Ort. Nebenbei werden Bedarfe (z.B. Schulung, Budget) und Herausforderungen (z.B. in der Umsetzung) erfasst und an die Führung zurückgespielt, die diese Punkte bei der Ausführung ihrer Aufgaben berücksichtigt.

Mit Standortverantwortlichen oder Sicherheitsexperten in Fachabteilungen wird gewährleistet, dass alle Sicherheitsaspekte über die Tätigkeiten der Organisation hinweg berücksichtigt werden. Die Mitarbeiter verfügen über die erforderliche Nähe zum operativen Kerngeschäft und neben wertvollem Wissen aus der Praxis über ein gutes Netzwerk, welches die Sicherheitsinteressen unterstützen kann.

- Alternativ ist auch die Schaffung einer klassischen und zentralen Abteilung für Sicherheitsmanagement denkbar, die die einzelnen Sicherheitsthemen wie Objektschutz, Reisesicherheit und BCM umsetzt, erste Anlaufstelle und Dienstleister für alle Abteilungen und Standorte des Unternehmens in Sicherheitsfragen ist.

Auch eine Kombination aus den beschriebenen Gestaltungen der Aufbauorganisation ist möglich. Über alle Ebenen und Regionen hinweg sind klare Zuständigkeiten und Abläufe durch die Sicherheitsführung vorzugeben und durch das Management umzusetzen.

Einige wenige international tätige Großkonzerne haben ihre großen Sicherheitsorganisationen wie beschrieben (um-)strukturiert und erfolgreich etabliert.

Selbstverständlich setzt der Aufbau der beschriebenen Struktur und Trennung von Governance und Management Investitionen in und eine Priorisierung der Sicherheitsorganisation, bei der erforderlichen Abänderung bereits vorhandener Strukturen auch ein Changemanagement, voraus. Im Gegenzug bewirkt er, konsequent umgesetzt, eine schlagkräftige, schlanke und effektive Sicherheitsorganisation, die wesentlich zu einem resilienten zukunftssicheren Unternehmen beiträgt.



Weitere Fachartikel unserer Experten erhalten Sie mit unserem Sicherheitsbriefing.