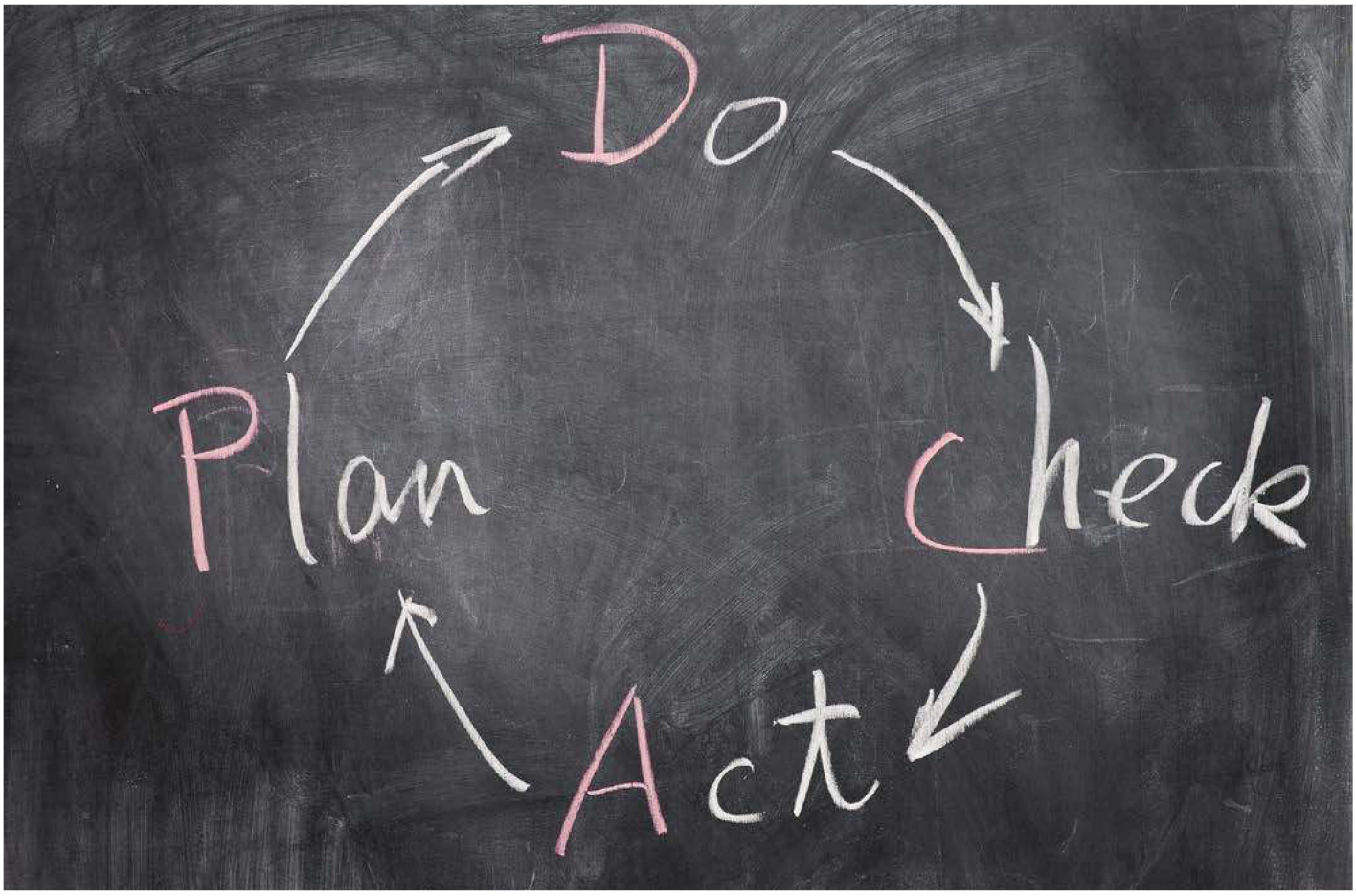


Sicherheit als Managementprozess

Das Thema Sicherheitsmanagement kommt in Unternehmen und Organisationen mehr und mehr da an, wo es hingehört, nämlich auf der Ebene der Entscheidungsträger, Unternehmenslenker und Führungskräfte.

Jörg Schulz

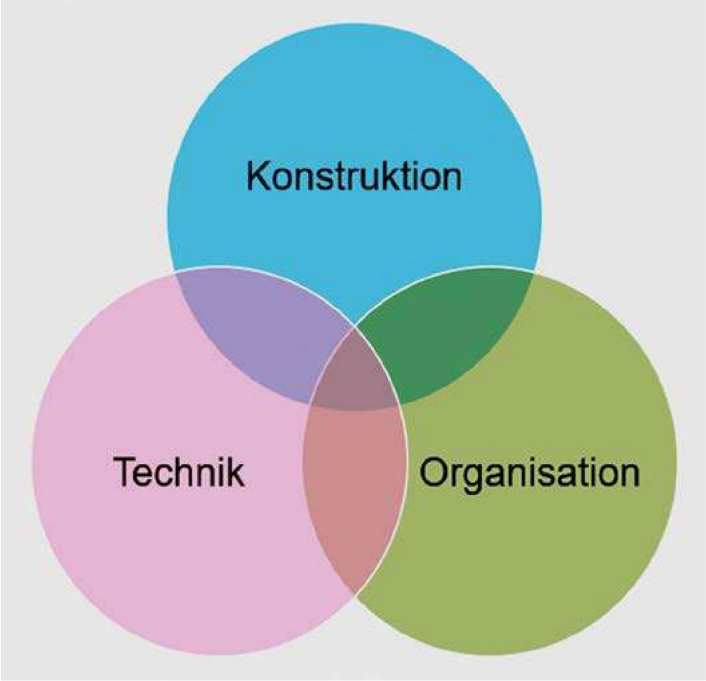
Dies ist das Resultat eines jahrelangen Prozesses der Bewusstseinsbildung, die das Thema Sicherheit herausholt aus Ebenen der Belanglosigkeiten und der Nebensächlichkeiten, ein Wandel hin zu einem wichtigen Business Enabler für reibungslose Geschäftsprozesse. Entscheider wollen sich jedoch nicht mit jedem einzelnen Magnetkontakt beschäftigen, vielmehr wollen sie strategische Entscheidungen auf Metaebene treffen und Vorgaben für Massnahmen formulieren, die dann durch Fachabteilungen weiter zu vertiefen sind. Der vorliegende Beitrag zeigt auf, wie man das Thema Sicherheit auf dieser Flughöhe erfolgreich angehen kann und welche Werkzeuge und Methoden es braucht.

Homogene Betrachtungsweise: Weg von Einzelmassnahmen, hin zu Ganzheitlichkeit

Der gesamte hier behandelte Themenkomplex muss von Beginn an durch Ganzheitlichkeit geprägt sein. Jede Technik und jedes System hat ihre resp. seine Stärken, aber auch ihre resp. seine technologisch bedingten Grenzen. Diese sind mit anderen Lösungen aufzufangen, und hier darf keineswegs nur über Technik nachgedacht werden. Denn die Basis für alles Weitere sind nach wie vor bauliche und konstruktive Massnahmen. Und damit aus Konstruktion und Technik ein erfolgreicher Prozess wird, sind personelle und organisatorische Massnahmen obligatorischer Bestandteil einer erfolgreichen Gesamtlösung.

Ganzheitlichkeit heisst das Stichwort. Jedoch kann nie irgendeine Sicherheitstechnik eine fehlerhafte bauliche Situation entschärfen, genauso wie organisatorische Massnahmen nicht dazu dienen dürfen, mangelhafte bauliche und technische Umstände zu kompensieren.

Stellen wir uns beispielsweise ein mechanisch hochwertig ausgerüstetes Fenster vor, das nun mit einer entsprechenden Sicherungstechnik kombiniert werden soll. Würde man innerhalb des Raumes quasi hinter dem Fenster einen Bewegungsmelder installieren, so würde dieser bei einem Überwindungsversuch erst eine Meldung abgeben, wenn das Fenster bereits durchbrochen wäre. Die hohe Widerstandszeit, die ein hochwertiges Fenster mit sich bringt, wäre ungenutzt abgelaufen und man hätte keinen Mehrwert davon. Ein besserer Weg wäre es, bereits die erste Annäherung zu detektieren, sodass man die Widerstandszeit der Barriere dazu nutzen kann, die Intervention einzuleiten und weitere schädigende Ereignisse abzuwenden. Dieses kleine Beispiel ist nicht das Ergebnis jahrelanger akademischer Forschungsarbeit, sondern lediglich das Resultat von logischem Denken.



Risiko, Schutzziel, Massnahme: Eine klare Strategie für zielgenaue Ergebnisse

Wer Massnahmen plant, braucht Schutzziele, die ihm die Angemessenheit der Massnahmen aufzeigen und ein ständiges Überprüfen bzw. Plausibilisieren der Massnahmen ermöglichen.

Wer Schutzziele formulieren will, muss dies im Bewusstsein der individuellen Risikolage tun, um die Schutzziele nicht an der Bedrohungslage vorbeizudefinieren. Dies ist bekannt und bewährt. Und diese bewährte Strategie gilt es definitiv weiter anzuwenden und mit modernen Werkzeugen fortzuschreiben.

Eine erste Methodik dazu wäre der Deming-Kreis mit seinem Zyklus PLAN – DO – CHECK – ACT. Diese in vielen Bereichen bereits anerkannte und bewährte Methodik kann man ohne Weiteres im Kontext Sicherheitsmanagement anwenden. Hierbei muss man keineswegs das Rad neu erfinden, denn die beschriebenen systematischen Schritte lassen sich innerhalb des Deming-Kreises zuordnen und um den wichtigen Schritt der ständigen Evaluierung erweitern. So kann Bewährtes weiter angewendet und um zeitgemässe Aspekte erweitert werden, indem man innerhalb der einzelnen Schritte die folgenden Handlungen durchführt:

PLAN:

- Risiken und Bedrohungen sind zu analysieren, indem man Eintrittswahrscheinlichkeit und potenzielle Schadenshöhe auf einer Skala beispielsweise von 0 bis 5 einsortiert und aus dem Produkt der beiden Aspekte eine objektivierte Risikoeinschätzung vornimmt. Anhand dieser Betrachtung kann relativ unmissverständlich erkannt werden, welchem der beiden Aspekte mit Massnahmen am wirkungsvollsten entgegengewirkt werden kann.

- Ziele sind zu benennen, indem man aus den Ergebnissen der Risikoanalyse heraus die Schutzziele definiert und sie gewissermassen als Vision für alle weiteren Planungen ganz oben anstellt. Verbleibende Restrisiken müssen benannt und ins Bewusstsein gerückt werden, damit Entscheidungsträger in der Lage sind, abzuwägen. Wer Investitionen scheut, kann oft ein bestimmtes Schutzziel nicht erreichen und wirkt somit einem bestimmten Risiko nicht entgegen. Diese Bewusstseinsbildung hilft, bei Investitionsentscheidungen Budgets zu plausibilisieren und zu begründen.
- Sicherheitsvorgaben und Standards sind zu formulieren, indem man aus den Schutzzielen bestimmte, immer wiederkehrende allgemeingültige Definitionen ableitet und detaillierter benennt.
- Konkrete Massnahmen sind zu planen, indem auf dieser Ebene Lösungen mit Einzeltechniken und Sensoriken entwickelt werden, die den Risiken entgegenwirken, sei es durch baulich-mechanische Härtung, meldetechnische Signalisierung und Überwachung oder personelle, organisatorische Prozesse.

DO:

- Massnahmen sind umzusetzen, indem durch Fachplaner bauliche und technische Lösungen ausführungsreif geplant und ausgeschrieben und diese dann durch Fachunternehmer umgesetzt werden. An dieser Stelle bietet sich die Option einer Proof-of-Concept-Phase an, die nicht immer zwingend notwendig ist, jedoch gerade bei komplexen Anwendungen vor dem grossen Roll-out Stärken und Schwächen aufzeigen kann.
- Systeme sind zu aktivieren, indem die installierten Lösungen in Betrieb genommen, getestet und an den Betreiber übergeben werden.

CHECK:

- Die Wirksamkeit der Massnahmen ist zu prüfen, indem ein Abgleich der zuvor definierten und vereinbarten Schutzziele vorgenommen wird und die Erreichung der Schutzziele überprüft wird. Abweichungen sind hierbei festzustellen und zu beheben, indem ein laufendes Verfahren der Erfassung und Kontrolle etabliert wird.

ACT:

- Die Zielerreichung ist permanent zu prüfen, indem die vorgenannten Aktivitäten nicht nur nach der Inbetriebnahme ausgeführt werden, sondern als kontinuierlicher Prozess und als wiederkehrende Handlung.
- Ziele sind permanent zu prüfen, indem ebenfalls als wiederkehrende Handlung festgestellt wird, ob die Schutzziele noch richtig definiert sind oder ob durch veränderte innere oder äussere Einflüsse eine Anpassung notwendig ist. Sollten hierbei grössere Abweichungen festgestellt werden, gilt es, den PDCA-Zyklus neu zu starten und den Gesamtprozess erneut zu durchlaufen.

Bemerkenswert an dieser Betrachtung ist, dass sich an die initiale Phase, die durch Risikoanalyse, Schutzzieldefinition und schlussendlich das Umsetzen von Massnahmen geprägt ist, eine Phase des Betriebes und der Instandhaltung anschliesst.

1. Weiter aufgedröselt, meint Evaluierung hierbei zuerst, dass sich an die genannten Phasen ein Schritt der interoperablen Funktionstests anschliesst. Innerhalb solcher Tests ist nachzuweisen, dass die Integration unterschiedlicher Lösungen, Systemtechniken und Gewerke erfolgreich umgesetzt wurde und sich so aus einer Vielzahl von Einzeltechniken eine homogene Gesamtlösung ergibt.

   Geprägt sind solche Tests durch eine Sichtweise, die nicht in Systemtechniken oder Anlagen denkt, sondern in Prozessen und Szenarien. Dies können Angriffs-, Sabotage- oder Bedrohungsszenarien sein, deren Abwendung bereits in den Schutzzielen definiert sein müsste. Nun gilt es, diese Szenarien so realitätsnah wie möglich darzustellen und auch auszuführen, um die Wirksamkeit der Massnahmen als Ganzes zu prüfen und zu beurteilen. Dem Verfahren vorauszugehen hat natürlich ein 1:1-Test der einzelnen Anlagen als Nachweis der vollen Funktionsfähigkeit und Einsatzbereitschaft. Bestenfalls gelingt es so, mit den Integrationstests eine ganzheitliche Wirkungsweise sowohl der baulichen Anlagen, der technischen Systeme sowie der folgenden organisatorischen Massnahmen nachzuweisen.

   Es versteht sich aber von selbst, das hier, von Ausnahmen abgesehen, nur zerstörungsfrei prüfbare Systeme und Anlagen berücksichtigt werden können. Kaum einer würde innerhalb eines solchen Tests auf die Idee kommen, eine Scheibe einzuschlagen oder eine Tresorwand zu durchbrechen. Auch Blitzschutzsysteme lassen sich kaum mit solchen Methoden prüfen.

2. Sind interoperable Funktions- und Integrationstests erfolgreich abgeschlossen, begibt man sich in die wohl längste Phase einer Sicherheitslösung, nämlich die Betriebsphase. Gewöhnlich werden sicherheitstechnische Anlagen und Systeme durch Instandhaltungsleistungen gepflegt und über Jahre funktionsfähig gehalten. Diese Instandhaltungsleistungen können vorbeugenden oder korrektiven Charakter haben und gliedern sich üblicherweise in Inspektion, Wartung, Instandsetzung und Verbesserung. Erweiternd kann auch hier der Gedanke eines kontinuierlichen Zyklus dazu genutzt werden, einen Schritt weiterzugehen: Nicht nur die Technik an sich muss am Leben erhalten werden, sondern auch die Erreichung der ursprünglich gesteckten Schutzziele ist permanent zu hinterfragen. Ebenso gehört eine ständige Fortschreibung sowie Anpassung der Ziele durch veränderte Risiko- und Gefährdungslagen dazu.

Wenn man also, wie beschrieben, eine erfolgreiche Initialphase in einen laufenden Prozess überführt, hat man beste Chancen, dass die Lösung für lange Zeit die gesteckten Ziele erreicht und zum Unternehmenserfolg beiträgt.

Sicherheitstechnik und ISMS: Wenn aus Meldeanlagen IT-Systeme werden

Fast nahtlos lässt sich das Vorgenannte fortschreiben, wenn man etwas tiefer in die einzelnen technischen Systeme eintaucht. Zahlreiche Sicherheitssysteme sind heute reinrassige IT-Systeme. Anlagen benutzen oft keine eigenen Leitungswege oder proprietären Übertragungsverfahren mehr, sondern kommunizieren über anwendungsneutrale Kommunikationsverkabelungen, wie sie auch in der IT genutzt werden. Die Komponenten sind oft keine Einzelsensoren oder Melder mehr, sondern kommunizieren gewissermassen als kleine Webserver direkt im Netz. Und die Zentralen sind keine anlagentypischen Kisten mehr, sondern kommen als Server daher.

Eine solche Architektur erfordert per Definition dann ein angemessenes Mass an IT-Sicherheit und Datenschutz. So etwas schreibt man üblicherweise in einem Informationssicherheitskonzept nieder. Ein solches Werk beschreibt dann IT-sicherheits- und datenschutzrelevante Inhalte für sicherungstechnische Systeme und Leitstellen entsprechend den Regeln bzw. dem Stand der Technik. Wie man dieses Werk und den Gesamtprozess gestaltet, beschreibt am besten die Normenreihe ISO 27000.

Die Struktur der ISO 27000 ist wiederum geprägt von:

- einer Phase der Konzeption,
- einer Phase der Planung,
- einer Phase der Umsetzung und schlussendlich
- einer Phase der ständigen Überwachung.

Die Parallelen zur oben beschriebenen Anwendung des Deming-Kreises sind offenkundig. Dies vereinfacht es, die Methodik auf die Gesamtlösung anzuwenden.

Halten wir also fest, dass Sicherheit ein Prozess ist, der für den Unternehmenserfolg essenzielle Bedeutung hat. Um nun die Problemstellungen im Management zu platzieren und dort damit umgehen zu können, sind Methoden der Komplexitätsreduktion und der Abstrahierung vonnöten. Niemand kann und wird sich mit differenzierten Gefahren auf Objektebene auseinandersetzen. Vielmehr geht es hier um das Grosse und Ganze. Wie gezeigt, können solche Methoden sehr pragmatisch angewendet werden und erleichtern so den Umgang mit vielerlei Problemstellungen. Wenn es dazu noch gelingt, zyklische Betrachtungsweisen zu etablieren, stehen die Chancen gut, dass eine sicherheitstechnische Lösung lange Zeit erfolgreich bleibt. ■

JÖRG SCHULZ
BBA Business Security, Berater und Fachplaner bei der VON ZUR MÜHLEN'SCHE (VZM) GmbH; technische Ausbildung und anschliessende Tätigkeit im Bereich Elektro- und Sicherheitstechnik