Warum Sicherheitsplanung?

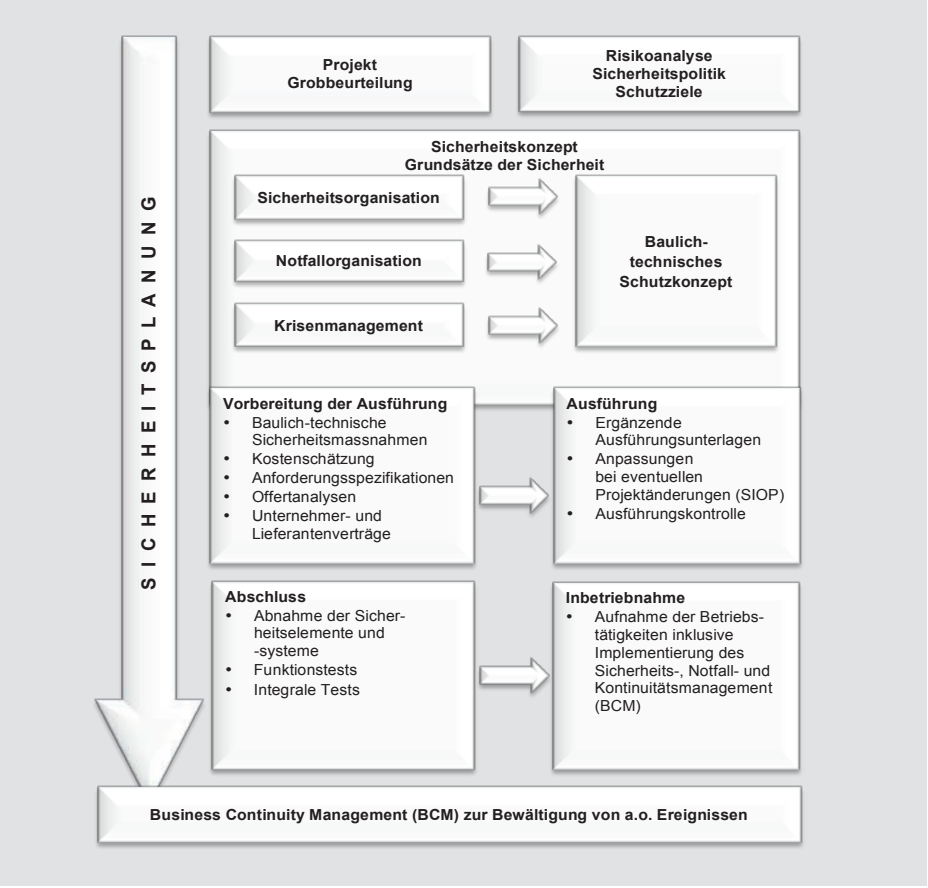
Veränderungen beherrschen heisst, insbesondere Risiken richtig zu beurteilen und in den Griff zu bekommen. Eine immer komplexer werdende Umwelt, gesellschaftliche Entwicklungen, verschärfte Gesetze, aber auch innerbetriebliche Abläufe, Technologien und daraus resultierende Abhängigkeiten, wachsender Wettbewerbsdruck und sich integrierende Märkte erhöhen die Risiken für ein Unternehmen.

Von Uwe Müller-Gauss

Schon kleinere Störungen können zu Schäden führen, die Unternehmensziele, Ertragssicherung oder gar die Existenz einer Firma ernsthaft gefährden. Sie müssen rechtzeitig erkannt und zielgerichtet angegangen werden. Präventive Sicherheitsmassnahmen schaffen die Grundlage, mit Schäden aller Art fertig zu werden beziehungsweise diese in annehmbaren Grenzen zu halten.

Methodik der Planung

In erster Priorität soll mit einem Minimum an Kosten die Risikoexposition des Unternehmens auf ein akzeptables Niveau reduziert werden. Nachfolgend wird für einen Neubau ein pragmatisches und zielorientiertes Vorgehen aufgezeigt. Die Sicherheitsplanung umfasst im Wesentlichen folgende Phasen:



Phase 1: Vorprojekt
- Risikoanalyse
- Sicherheitspolitik und Schutzziele
- Sicherheitsorientierte Bauprojektüberprüfung (SIOP)
- Sicherheits-Grobkonzept mit Vorschlägen für Massnahmen aufgrund der definierten Schutzziele

Phase 2: Bauprojekt
- Baulich-technisches Sicherheitskonzept
- Anforderungsspezifikationen für Sicherheitsanlagen und -einrichtungen als Grundlage für die Submissionen
- Sicherheitstechnische Beurteilung der Offerten von Sicherheitsanlagen und -einrichtungen
- Projektbegleitung und -koordination

Phase 3: Ausführung
- Baubegleitung und Detailbearbeitung
- Abnahmen der Sicherheitsanlagen und -einrichtungen
- Überwachung von Abnahmependenzen der Sicherheitsanlagen und -einrichtungen
- Instruktion der Nutzer mit Sicherheitsaufgaben (in Zusammenarbeit mit den Anlagelieferanten)

Phase 4: Nutzungsphase
- Implementierung der Sicherheits- und Notfallorganisation
- Sensibilisierung der Mitarbeitenden für Sicherheitsfragen
- Periodische Audits für die Überprüfung der Erhaltung der Sicherheitsvorkehrungen
- Business Continuity Management (BCM) zur Bewältigung von ausserordentlichen Ereignissen

Bemerkung: Bauprojektänderungen erfordern ein iteratives Vorgehen bei der Sicherheitsplanung. Die vier Phasen wiedergeben daher nur den ungefähren zeitlichen Verlauf der Sicherheitsplanung.

Phase 1 – Vorprojekt

Risikoanalyse: Sie umfasst die Zusammenstellung eines für den Neubau relevanten Risikokataloges. Dabei werden für die einzelnen Risiken mögliche Szenarien

beschrieben. Die einzelnen definierten Risiken werden hinsichtlich der Eintritts- und Entdeckungswahrscheinlichkeit sowie des möglichen Schadenausmasses qualitativ bewertet, wobei jeweils die betroffenen Schutzobjekte, Prozesse und möglichen Folgeschäden (Beeinträchtigung des Unternehmenserfolgs, Verlust der Marktposition) ausgewiesen werden. Die Risikoanalyse ist sodann in einem Workshop mit Vertretern des Bauherrn zu besprechen und gegebenenfalls anzupassen. Das Resultat der Risikoanalyse wird grafisch in einem Risikoportfolio zusammengefasst.

Politik und Schutzziele: Ausarbeiten einer auf die Firma zugeschnittenen Sicherheitspolitik in Zusammenarbeit mit der Geschäftsleitung, welche die im Betrieb anzuwendenden Sicherheitsstrategien definiert und die Grenzen der tragbaren, nicht tragbaren und überwälzbaren Risiken für Personen und Betrieb festlegt.

Ausgehend von der Sicherheitspolitik (Sicherheitsleitbild) sind die Schutzziele zu formulieren. Schutzziele definieren die Höhe des anzustrebenden Schutzgrades. Sie basieren auf den vorgängig bewerteten Risiken und sind durch die Geschäftsleitung zu genehmigen. Die definierten Schutzziele wirken sich direkt auf die zu treffenden baulich-technischen und organisatorischen Sicherheitsmassnahmen aus.

Bauprojektüberprüfung: Überprüfung des Projektes in Bezug auf Sicherheitskriterien anhand von Grundrissplänen, Schnitten, Fassadenansichten sowie Baubeschrieben. Aufzeigen von Schwachstellen und Formulieren von Massnahmenempfehlungen zuhanden der Projektverantwortlichen.

Grobkonzept: Erstellen eines Grobkonzeptes, welches in knapper Form aufzeigt, wie und mit welchen Mitteln die formulierten Schutzziele zu erreichen sind. Massnahmenpakete baulich-technischer und organisatorischer Art werden, unter Einhaltung objektspezifischer Randbedingungen, definiert. Das Grobkonzept behandelt unter anderem die folgenden Teilschutzbereiche.

Beispiele:
- Zutrittskonzept, enthält Perimeterschutz (Arealabgrenzung), Peripherieschutz, (Gebäudehülle), Innenschutz (Gebäudeinnenbereiche), Sicherheitszonenpläne, -beschriebe, Zonenübergänge und Zutrittskontrolle/-regelungen
- Objektschutz
- Brandschutz
- Schutz vor Ausfall betriebswichtiger Systeme
- Schutz vor Verlust betriebswichtiger Informationen
- Sicherheitsorganisation
- Notfallorganisation

> «Krisen meistert man am besten, indem man ihnen zuvorkommt.»
>
> *Walt Whitman Rostow (1916–2003), amerik. Wirtschaftswissenschaftler*

Phase 2 – Bauprojekt

Baulich-technisches Konzept: Nach Genehmigung des Grobkonzeptes durch die Projektverantwortlichen, sind – basierend auf die Sicherheitszonenpläne und Zonenübergänge – das detaillierte verbale baulich-technische Sicherheitskonzept und die entsprechenden Sicherheitskomponentenpläne zu erarbeiten.

Anforderungsspezifikationen: Der Anforderungskatalog enthält die technische und funktionelle Beschreibung der Sicherheitsanlagen und -einrichtungen. Er bildet die Grundlage für die Submissionen. Die – durch die Lieferanten – abzugebenden Dokumentationen für die Sicherheitsanlagen und -einrichtungen sind hier ebenfalls aufzuzeigen.

Beurteilung der Offerten: Die Offerten sind in technischer Hinsicht auf die Einhaltung der Anforderungsspezifikationen zu überprüfen und gegebenenfalls – wenn vom Bauherrn gewünscht – auch auf preisliche Aspekte (Offertgegenüberstellung) zu untersuchen.

Projektbegleitung und -koordination: Während der ganzen Projektdauer sind die Projektverantwortlichen in sicherheitsrelevanten Problemstellungen zu unterstützen. Insbesondere ist die Koordination zwischen den Lieferanten der einzelnen Sicherheitsanlagen und -einrichtungen zu gewährleisten, damit eine vollständige und aufeinander abgestimmte Erstellung erfolgt. Weiter ist eine termingerechte Behandlung und optimale Integration der Sicherheitsaspekte in das Gesamtprojekt anzustreben.

Phase 3 – Ausführung

Baubegleitung und Detailbearbeitung: Von der Überprüfung der Ausführung bis zu den Abnahmen respektive der Inbetriebnahme ist sicherzustellen, dass die spezifizierten Massnahmen konsequent und qualitativ den Anforderungen entsprechend realisiert werden. Die Implementierung der Massnahmen ist mittels periodischer Überprüfungen zu kontrollieren. Insbesondere die Umsetzung der Sicherheitsmassnahmen sowie die Sicherstellung der Folgerichtigkeit (z.B. bei Projektänderungen) sind laufend zu überwachen.

Dazu hat sich die Sicherheitsorientierte Prüfung von Projekten (SIOP) bewährt. Die sicherheitsorientierte Überprüfung von Projektvorhaben vergleicht (am besten von Anfang an) die Projektplanung und -ausführung auf die Folgerichtigkeit mit den Vorgaben der Sicherheit. Dieser Soll-Ist-Vergleich dient als Entscheidungsgrundlage für die Freigabe der jeweils nachfolgenden Projektphase. Die SIOP kann Bestandteil eines Internen Kontrollsystems (IKS) sein.

Die SIOP soll sicherstellen, dass Sicherheitsanforderungen im Projektvorhaben rechtzeitig berücksichtigt werden. Durch ein formalisiertes Kontrollverfahren im Sinne einer Qualitätssicherung wird sichergestellt, dass das Projektergebnis den Sicherheitsanforderungen des Benutzers genügt.

Die baulich-technische Sicherheitsprüfung vergleicht die Anforderungsspezifikationen mit der Projektausführung. Es wird also die Realisierung sicherheitsrelevanter baulich-technischer Elemente und Systeme auf Folgerichtigkeit zu den Vorgaben der Sicherheit überprüft. Dieser Soll-Ist-Vergleich dient als Entscheidungsgrundlage für die Freigabe der nächsten Phase.

Durch eine fortlaufende sicherheitsorientierte Überprüfung soll sichergestellt werden, dass die Sicherheitsmass-

nahmen folgerichtig zum Sicherheitskonzept geplant, ausführungsreif detailliert und den Anforderungen entsprechend realisiert werden.

Abnahmen: Abnahme der Sicherheitsanlagen und -einrichtungen mit Vollständigkeitskontrolle sowie integrierten Funktionstests. Die Kontrolle der Dokumentation (Betriebsanleitungen, Pläne, Schemas usw.) ist ebenfalls ein Bestandteil der Abnahme. Mängel sind in einem Abnahmeprotokoll mit Behebungstermin und Verantwortlichen festzuhalten. Die Behebung der Abnahmependenzen sowie Garantiearbeiten sind zu überwachen.

Instruktion: In Zusammenarbeit mit den Lieferanten sind die Nutzer der Anlagen und Einrichtungen anwenderorientiert zu instruieren.

Phase 4 – Nutzungsphase

Sicherheits- und Notfallorganisation: Bereits parallel zur Erarbeitung des baulich-technischen Sicherheitskonzeptes (Phase 2) ist die Sicherheits- und Notfallorganisation im Aufbau und Ablauf zu definieren. In der Phase 4 ist die Organisation in das Gesamtkonzept zu implementieren.

Sensibilisierung: Die Mitarbeitenden sind im Verhalten bei Notfällen (z.B. Brandfall, medizinischer Notfall/Unfall, telefonische Drohungen) mittels Schulung/Instruktion regelmässig zu sensibilisieren.

Periodische Audits: Periodisch ist zu überprüfen, ob die dem vorhandenen Sicherheitskonzept zugrunde liegenden Randbedingungen noch aktuell sind. Änderungen in der Bedrohung, der Nutzung von Gebäudebereichen, der Bedeutung einzelner Funktionen usw. erfordern eine Überprüfung und allenfalls Anpassung des Sicherheitskonzeptes.

Business Continuity Management: Die Geschäftstätigkeit stellt hohe Anforderungen an die Informatik und das Gebäudemanagement. Der Ausfall der Gebäudeinfrastruktur kann den Ausfall von Informatikdienstleistungen bewirken und zu einem Ausfall der Geschäftsprozesse eskalieren. Für den Krisenfall sind darum Katastrophen-, Ausweich- und Wiederanlaufpläne zu erarbeiten.

Schlussbemerkung

Nur ein Facility Management, das auf ein systematisches, nachhaltiges Risikomanagement ausgerichtet ist, stärkt nachhaltig das Vertrauen von Geschäftspartnern, Kunden und Mitarbeitenden in das Unternehmen und ermöglicht so die dringend benötigte «long-term licence to operate» sowie die Sicherstellung eines Sustainable Developments. ■

UWE MÜLLER-GAUSS
Dipl. Entrepreneur FH MBA. Inhaber der Müller-Gauss Consulting in Hinwil-Zürich.