1. Sicherheitsanalysen und -konzepte

Unternehmungen haben in den letzten Jahren durch den Einsatz hochtechnologischer Systeme eine gesteigerte Produktionseffizienz, die engere Einbindung in Netzwerkstrukturen, die zunehmende Partizipation am globalen Wettbewerb sowie auch durch die Konzentration auf Marktnischen große Risikopotentiale aufgebaut.

Die Veränderungen bei den Risikostrukturen betreffen nahezu alle Unternehmungen: Wer langfristig am Markt erfolgreich bleiben will, hat sich den wandelnden wirtschaftlichen, rechtlichen, ökologischen und sozialen Rahmenbedingungen anzupassen. Dadurch kommt es auch in den Unternehmen zu großen Veränderungen bei der Risikoqualität.

Während sich Produktionsverfahren, Marketingstrategien, Kommunikations-, Logistikkonzepte und Forschung ständig den Veränderungen anpassen bzw. diese mit bewirken und prägen, bleiben häufig die Sicherheitsstrukturen, -maßnahmen und bestehende Sicherheitskonzepte, die auf der Basis früherer Rahmenbedingungen entwikkelt wurden, unverändert weiterbestehen oder werden ohne präzise neue Sicherheitsanalyse aus wirtschaftlichen oder sonstigen Gründen reduziert.

So besteht heute in vielen Unternehmen die Notwendigkeit

- aktuelle Sicherheitsanalysen durchzuführen
- neue Sicherheitskonzepte zu entwickeln oder bestehende anzupassen
- Sicherheitsziele neu zu definieren bzw. zu aktualisieren und in der Unternehmenspolitik zu verankern.

Dieses Kapitel zeigt die Grundsätze der Sicherheitsanalyse, der Erarbeitung eines Sicherheitskonzeptes und der Realisierung von Sicherheitskonzepten mit dem Schwerpunkt der Sicherheitsplanung auf.

Der Fachmann kann Anregungen bei der Durchführung dieser Aufgabe finden, der Laie kann mit Hilfe der angefügten Checkliste Defizite und weiteren Handlungsbedarf feststellen.

Da in den Unternehmen nicht immer professionelle Security-/Sicherheitsfachleute mit umfassendem Fachwissen und umfangreichen praktischen Erfahrungen zur Verfügung stehen, ist es bei bestehendem Handlungsbedarf u. U. erforderlich, externe Sicherheitsberater mit der Durchführung der Sicherungsanalyse zu beauftragen.

Auch sollten die Vorteile einer systematischen Bewertung der betrieblichen Sicherheit, wie

- Transparente Risikolage
- Einbezug des Managements

- ausgewogene Konzepte ohne gefährliche Sicherungslücken
- keine Alibimaßnahmen bzw. unzweckmäßige Schutzvorkehrungen
- keine punktuellen, nicht bewertbare Maßnahmen, sondern wirkungsvolle Gesamtlösungen
- kontrollierbare, jederzeit anpaßbare Sicherungsmaßnahmen
- nachvollziehbare Dokumentation der Überlegungen und Grundlagen

keineswegs unterschätzt werden.

1.1 Voraussetzungen

Effiziente und wirtschaftliche Sicherheitsmaßnahmen setzen eine fundierte Sicherheitsanalyse voraus, um den standortspezifischen Sicherheitsbedarf zu ermitteln. Hierbei können zur Anwendung kommen:

- IST-Bestandsaufnahme
- Schwachstellenanalyse
- Abhängigkeitsanalyse
- Bedrohungs-/Gefährdungsanalyse
- Organisationsanalyse
- Ausbildungsbedarfsanalyse
- Effektivitätsuntersuchung

Je nach Schwerpunkten und Zielen der Analyse können alle diese Untersuchungen oder nur einzelne davon zur Anwendung kommen.

Der Ersteller einer Sicherheitsanalyse bzw. eines Sicherheitskonzeptes sollte verfügen über:

- Kreativität
- Flexibilität
- Ideenreichtum
- Reichhaltige Erfahrung
- Fähigkeit des vernetzten Denkens
- Kommunikative Fähigkeiten
- Unabhängigkeit
- Kenntnis des Sicherheitsmarktes (Markttransparenz)
- Teamorientierung
- Fähigkeit des vorausschauenden Denkens und Handelns

Auf der Basis des erhobenen IST-Zustandes mit den erkannten Schwachstellen und Risiken ist dann ein standortspezifisches Sicherheitskonzept (Beschreibung des SOLL-Zustandes) zu entwickeln sowie eine Entscheidung über die Umsetzung herbeizuführen.

Hierzu ist eine Entscheidungsvorlage und eine Realisierungsplanung mit Untersuchung der Wirtschaftlichkeit zu erarbeiten. Bei Betrachtung der Wirtschaftlichkeit im Bereich der Sicherheit muß Kostentransparenz gegeben sein; es darf jedoch kein einseitiges Kostendenken vorherrschen. Vielmehr sind die Kosten in eine ganzheitliche Betrachtung der Risiken und Folgen einzubeziehen.

Beim Ermitteln sinnvoller und ausreichender Sicherungsmaßnahmen zum Verhindern von Störfällen durch fahrlässiges oder vorsätzliches Einwirken von Personen müssen für jeden Betrieb/Anlage eine Reihe unterschiedlicher Faktoren beachtet werden. Hierbei spielen z. B. die

- Art der Produktion,
- Sensibilität des betrieblichen Know-how,
- Abhängigkeit von spezieller Infrastruktur (z. B. DV, Logistik, externe Dienstleiter),
- Lagerung von Stoffen,
- Lage des Betriebes,
- Umgebung des Betriebes,
- Art und Umfang der Bebauung,
- personelle Ausstattung,
- vorhandene Sicherheitsstrukturen und -maßnahmen
- sich aus der Sicherheitsanalyse ergebende Gefahrenpunkte sowie
- betriebsspezifische Besonderheiten

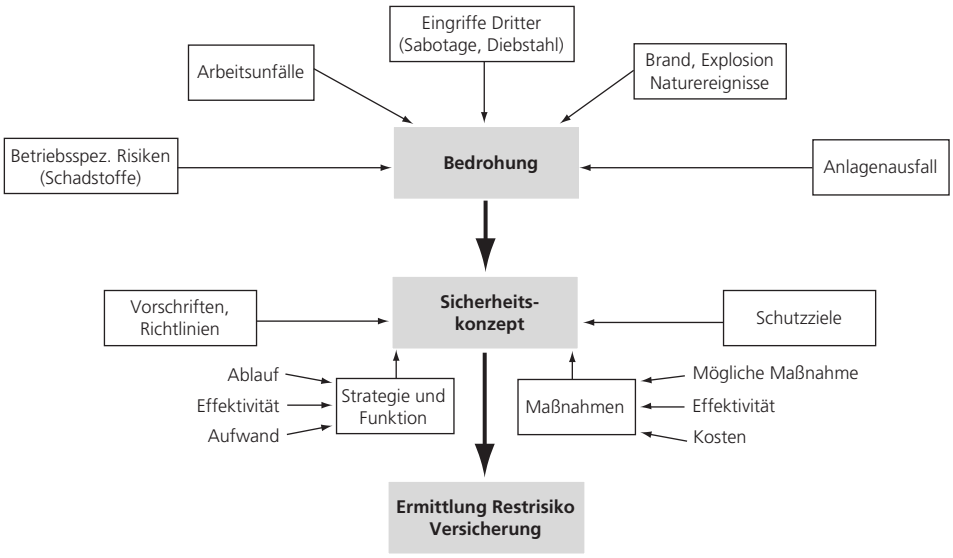
eine Rolle.

1.2 Ablauf einer Sicherheitsanalyse und Risikobewertung

Die auf einen Industriebetrieb einwirkenden Gefahren können vielfältiger Natur sein:

- Naturereignisse
- Ereignisse in der Umgebung des Betriebes

Bild 1: Einflußgrößen auf ein Sicherheitskonzept



- Eingriffe Dritter (Straftaten, terroristische Bedrohung)
- Eigentumsdelikte durch Mitarbeiter und Betriebsfremde
- Sabotage
- Spionage/Know-how-Diebstahl
- Betriebsspezifische Risiken durch Produktionsverfahren und Schadstoffe
- Arbeitsunfälle
- Brand/Explosion
- Technisches Versagen/Anlagenausfall
- Umweltbeeinflussung

Ausgelöst werden können solche Schadensereignisse durch Zufall, Irrtum oder Absicht.

Schäden können sich in allen Bereichen eines Industriebetriebes ergeben, so z. B. bei Betriebsanlagen

- Investitionsgütern (Gebäude, Anlagen)
- Produktionsmitteln (Maschinen)
- Elektronische Datenverarbeitung (EDV)
- Material
- Produktion etc.

Immateriellen Werten

- Fertigungsverfahren, Know-how, Informationen, Methoden
- Erfindungen, Patente
- Qualitätsstandards
- Organisation
- Personal
- Ansehen der Firma in der Öffentlichkeit

Zur Vermeidung von Gefahren und Minderung der Risiken sowie um den Eintritt von Schadensereignissen und/oder Schäden zu verhindern, sind Sicherungsmaßnahmen durchzuführen.

Hierbei ist vorab festzustellen, welche Gefahren und Risiken im individuellen Fall einer industriellen Einrichtung drohen und wie hoch die Eintrittswahrscheinlichkeit von Schadensereignissen ist.

Dies erfolgt im Rahmen einer **Sicherheits- oder Schwachstellenanalyse.**

Im Rahmen einer Sicherheitsanalyse müssen auch Abhängigkeiten und Ursachenketten i. S. eines vernetzten Denkens berücksichtigt werden. Die komplexen Sicherheitsprobleme in einem modernen Industriebetrieb sind nicht mit der einfachen Formel

Schwachstelle + Sicherheitsmaßnahme
= Sicherheit

zu lösen.

Aufgrund einer solchen Sicherheits- oder Schwachstellenanalyse, die man auch als Sicherheitsbeurteilung eines Betriebes bezeichnen könnte, sind die Schutzziele für das Unternehmen oder den Betrieb zu definieren, aus denen die möglichen Schutzmaßnahmen abgeleitet werden. Diese werden in einem Sicherheitskonzept zusammengefaßt.

Das Sicherheitskonzept ist eine, auf einer Schwachstellenanalyse basierende SOLL-Darstellung des Sicherheitszustandes eines Betriebes, welche i.S. eines vernetzten Denkens die komplexen betrieblichen Strukturen und Einrichtungen in ihrer Gesamtheit berücksichtigt.

Wirksame Sicherheitskonzepte erfordern die systematische Berücksichtigung einer Vielzahl von Einflußgrößen. Nachfolgend wird aufgezeigt, wie, ausgehend von der Analyse, der betreffenden Anlage hinsichtlich ihrer Struktur, ihrer Funktion und aller damit in Zusammenhang stehenden sicherheitsbezogenen Eigenschaften eine Bedrohungsanalyse durchgeführt wird.
Die einzelnen Stufen sind dabei

- Auflisten und Zuordnen der relevanten Gefahren,
- Risikobewertung,
- Zusammenfassen der Risiken in einem Bedrohungsbild,
- Auflisten und Zuordnen der relevanten Gefahren,
- Risikobewertung,
- Zusammenfassen der Risiken in einem Bedrohungsbild.

Anhand festgelegter Schutzziele wird daraus das Sicherheitskonzept als sinnvolle und effektive Kombination von baulichen Vorkehrungen, technischen Einrichtungen und organisatorischen Maßnahmen abgeleitet.

Das Diagramm (Bild 2) zeigt die Zusammenhänge auf.

Basis für die Ausarbeitung des Sicherheitskonzeptes für einen Betrieb, eine Anlage, ein System ist die **Bedrohungs- oder Risikoanalyse,** mit der man sich zunächst einen möglichst quantifizierten oder bewerteten Überblick über die Risikoverteilung verschafft. Dazu muß zunächst das betrachtete System hinsichtlich seiner Struktur, seiner Funktion und der damit verknüpften sicherheitsrelevanten Eigenschaften analysiert werden. Für die so ermittelte Objektstruktur werden die denkbaren Schadensereignisse (Gefahren) zunächst unbewertet zusammengestellt. So entsteht eine Gefahrenmatrix. Ein Beispiel für eine solche Gefahrenmatrix zeigt Bild 3.

Wichtigster Teil der Bedrohungsanalyse ist die Bewertung der einzelnen auf die Objektstruktur bezogenen Gefahren, um die Schwachstellen im System zu erkennen.

Erfaßte und den Schutzobjekten zugeordnete relevante Gefahren sind letztlich Aufzählungen ohne substantiellen Aussagewert.

Wichtig für den Praktiker ist, daß schon mit sehr einfachen Verfahren ein systematischer Überblick über die Risikosituation eines Systems gewonnen werden kann. Quantitative Verfahren setzen die Abschätzung der Schadenshöhe bei Eintritt eines Schadensereignisses (Gefahr) sowie die Abschätzung der Eintrittswahrscheinlichkeit des Ereignisses voraus.

Setzt man diese Gefahren in Beziehung zu der Wahrscheinlichkeit des Eintritts und zur Höhe des möglichen Schadens und/oder Auswirkung auf das Unternehmen, dann erfolgt eine quantitative und/oder qualitative Bewertung der Gefahren in Form einer Risikobewertung.

Mögliche einfache Formeln für eine Risikobewertung können sein:

Objektives Risiko Ro = E (Eintrittswahrscheinlichkeit)
x A (Auswirkungen)
= Schadenserwartungswert

Risiko = Höhe des möglichen Schadens
– Eintrittswahrscheinlichkeit

Bewertete Risiken können dann zu einem Bedrohungsbild zusammengefaßt werden. Generell gilt: Je höher der Schadenerwartungswert oder Risikowert, um so höher der Handlungsbedarf, Sicherungsmaßnahmen zur Risikominimierung zu treffen.

In diesem Zusammenhang erscheint es sinnvoll, als Äquivalent für das noch tragbar erscheinende Restrisiko einen Akzeptanz-

Bild 2: Ablauf der Sicherheitsanalyse

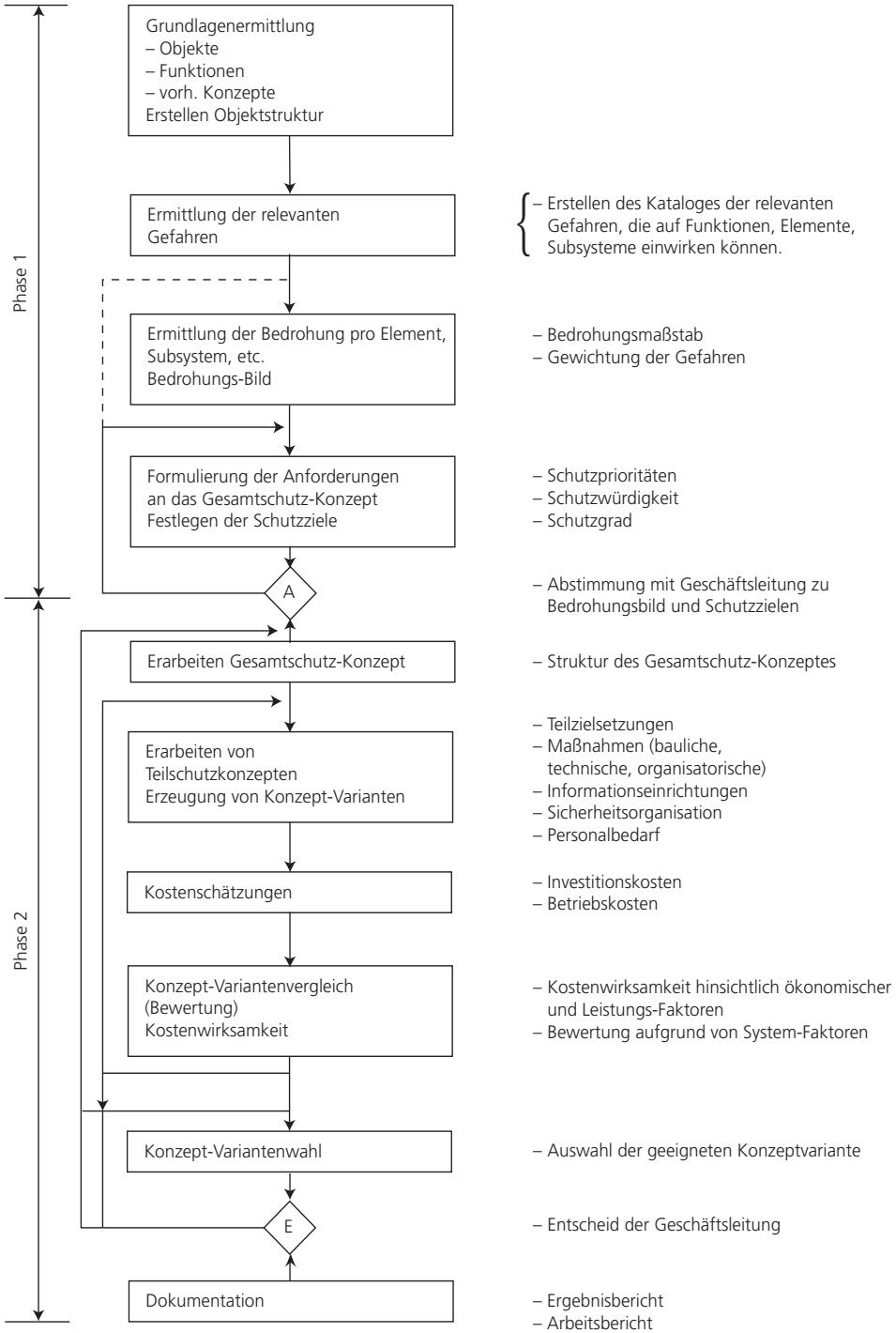


Bild 3: Gefahrenmatrix (Quelle: Wenk, Objektschutzplanung, 1992)

	Eingriffe Dritter (Außen-/Innentäter)	**Werk-spio-nage**	**Vanda-lismus**	**Dieb-stahl allge-mein**	**Brand-stiftung**	**Zerst. techn. Einr. (Sabo-tage)**	**Ge-heim-nis-verrat**	**Ab-sicht-liche Fehl-hand-lungen**
1	**Objekte**							
1.1	Gelände und Umfriedung							
1.1.1	Flächen innerh. juristischer Grenzen				×			
1.1.2	Flächen innerhalb				×			
1.1.3	Außenzaun (juristische Grenze)		×					
1.1.4	Bauhof, Betriebshof							
1.1.5	Zufahrtsstraßen und -wege							
1.1.6	Sicherheitszaun		×			×		
1.1.7	Brücken							
1.2	Gebäude							
1.2.1	Allgemeine Verwaltung	(×)	×	×	×	×	×	
1.2.2	Werkstätten	×	(×)	×	×	×	×	
1.2.3	Tankstelle				×			
1.2.4	Wache und Sicherheitsdienste		(×)		×	×		
1.2.5	Pforte							
1.2.6	Sozialgebäude			×	×	×		
1.3	Versuchseinrichtungen							
1.4	Mobile Objekte							
1.4.1	Testfahrzeug							
1.4.2	Wartungs- und Streifenfahrzeuge							
1.4.3	Baufahrzeuge, Fremdfahrzeuge		×	×	×	×		×
1.4.4	Bewegliche Unterkünfte und Läger		×	×	×			
1.4.5	Personen und Personengruppen							
1.5	Technische Einrichtungen							
1.5.1	Verkehrsleitsystem		×			×		×
1.5.2	Schranken, Tore etc.		×					
1.5.3	Beleuchtungseinrichtung		×			×		
1.5.4	Be- und Entwässerungsanlagen							
1.5.5	Feuerbekämpfungseinrichtungen		×			×		
1.5.6	Meßstellen		×			×		
1.5.7	Sicherheitseinrichtungen		×			×		×
1.5.8	Kommunikationssystem					×		×
2	**Funktionen**							
2.1	Verwaltung, Organisation, Betrieb							
2.2.	Betriebsabwickl./Leitung Verkehr					×		×
2.3	Werkstattbetr., Umbau/Wartung			×	×	×		
2.4	Versuchsbetrieb	×				(×)		
2.5	Wartung/Service							
2.6	Treibstoffversorgung				×	(×)		
2.7	Überwachung/Sicherheitsdienste					×		×

wert zu definieren. Unterhalb dieses Wertes können Sicherheitsmaßnahmen getroffen werden, sie sind jedoch nicht zwingend.

Die Parameter für die Eintrittswahrscheinlichkeit und Auswirkung kann der Durchführende einer Risikobewertung grundsätzlich an die Gegebenheiten einer Unternehmung anpassen. In der Praxis haben sich Modelle wie folgt bewährt:

Die Eintrittswahrscheinlichkeit von Schadensereignissen (Tabelle 1 und 2) kann u. a. abgeschätzt werden

- durch Bewertung von Ereignisszenarien
- durch Analyse vergleichbarer und komplementärer Ereignisse
- durch Auswertung von Statistiken (z. B. Schadensversicherer, Berufsgenossenschaften) und statistischen Daten aus dem Betriebsbereich (Abfrage bei kompetenten Stellen)
- durch Auswertung von Ausfalldaten und Zuverlässigkeitsdaten technischer Systeme
- mittels Analysen von Ereignisketten bei bekannten Basisereignissen (Ereignisbaumanalyse; nur bedingt einsetzbar)
- mit gesundem Menschenverstand und Erfahrungswissen.

Tabelle 1: Auswirkung (A)

Kategorie	Abkürzung	Erläuterung	Punkte
Existenzgefährdend	E	Die Weiterexistenz des Unternehmens ist in Gefahr.	10
Kritisch	KR	Hohe materielle und inmaterielle Schäden. Ausfall wichtiger Funktionen/Betriebsabläufe für einen bestimmten Zeitraum.	7
Beeinträchtigend	B	Materielle Schäden. Von außen nicht wahrnehmbare Funktionsbeeinträchtigungen.	4
Unkritisch	U	Geringe Sachschäden, jedoch keine Funktionsbeeinträchtigungen im Unternehmen.	0

Tabelle 2: Eintrittswahrscheinlichkeit (E)

Bewertung	Abkürzung	Erläuterung	Punkte
Sehr hoch	SH	Ist im Unternehmen schon mehrfach vorgekommen.	10
Hoch	H	Ist im Unternehmen schon einmal vorgekommen. Externe Beispiele aus vergleichbaren Betrieben/Branchen sind bekannt.	8
Mittel	M	Ist im Unternehmen noch nicht vorgekommen. Externe Beispiele aus vergleichbaren Betrieben/Branchen sind bekannt.	6
Klein	K	Ist im Unternehmen noch nicht vorgekommen. Vereinzelte Beispiele aus vergleichbaren Betrieben/Branchen sind bekannt. Möglichkeit kann nicht gänzlich ausgeschlossen werden.	3
Nicht relevant	NR	Ereignis ist nicht denkbar und auszuschließen.	0

Bei der Bewertung der Risiken sollte auch die Bewertung von Anhängigkeiten und immateriellen Schäden wie

- Auswirkungen auf abhängige Bereiche
- Einfluß auf Image
- Kundenabwanderung
- Verlust von Marktanteilen
- Einfluß auf die Wettbewerbsfähigkeit
- Einfluß auf die Handlungsfreiheit

Beachtung finden.

Trägt man die bei der Risikobewertung gewonnene Klassifizierung für die einzelnen Objekte und Gefahren matrixartig auf, so ergibt sich eine Bedrohungsmatrix, wie in Bild 4 dargestellt. Daraus lassen sich die Schwachstellen im betrachteten Betrieb herauslesen, an denen primär mit angepaßten Sicherheitsmaßnahmen anzusetzen ist.

Eine andere, sehr einfache Möglichkeit einer ersten Risikoabschätzung zeigt Bild 5. Hier wird die Höhe des Risikos durch eine bestimmte Gefahr auf eine bestimmte Funktionseinheit durch die Bewertungszahlen 0 bis 3 abgeschätzt. Eine Summierung der Zahlen nach Gefahren bzw. Funktionseinheiten ergibt die relevantesten Gefahren für die Gesamtanlage bzw. die am meisten gefährdeten Funktionseinheiten. Damit hat man eine systematisch erarbeitete Basis für die Maßnahmenplanung (Bild 6).

Tabelle 3: Höhe des möglichen Schadens (S)

Kategorie	Abkürzung	Erläuterung	Punkte
Existenzgefährdend	E	Schäden, die wesentliche Funktionen des Unternehmens in Frage stellen (Totalschäden, irreversible Zerstörungen). > 3 Mio/a und/oder mehrere Schwerverletzte und/oder Tote.	10
Kritisch	KR	Beeinträchtigung/Beeinflussung von Leistungsfähigkeit und Substanz (Geld, Zeitaufwand, Verlust von Inventar, Know-how, Vertrauenswürdigkeit und Image). > 500 TDM/a und/oder Verletzungen von mehreren Personen und/oder 1 Schwerverletzter/a.	7
Beeinträchtigend	B	Schäden zu Lasten der Leistungsfähigkeit des Unternehmens (Geld, Zeitaufwand, Produktionsmittel). > 100 TDM/a	4
Unkritisch	U	Rein finanzielle Schäden, die zu einer Beeinträchtigung des BE führen. < 20 TDM/a.	0

Beispiel Errechnung Schadenserwartungswert (Tabelle 3):

Objektives Risiko (Ro) (Schadenerwartungswert)

= Eintrittswahrscheinlichkeit (E) × Auswirkung (A)

E (M(Mittel/6 Punkte) x A (KR(Kritisch/ 7 Punkte) = 42 Punkte

Als vertretbares Restrisiko (Akzeptanzwert) könnte man E (Klein/3 Punkte) x B (Beeinträchtigung/4 Punkte) = 12 Punkte, annehmen.

Beispiel eines Risikowertes

Risiko (Risikowert)
= Höhe des möglichen Schadens (S)
× Eintrittswahrscheinlichkeit (E)

Risiko = S (E(Existenzgefährdend/10 Punkte) × E (M(Mittel/6 Punkte) = 60 Punkte

Mögliches Restrisiko (Akzeptanzwert) = B (Beeinträchtigend/4 Punkte) × K (Klein/ 3 Punkte) = 12 Punkte. Damit besteht auch hier Handlungsbedarf, das Risiko zu senken.

Bild 4: Bedrohungsmatrix (Verwaltungsbau) (Quelle: Wenk, Objektschutzplanung, 1992)

4.1	Direktionsbereiche			Brand	Technische Ausfälle	Unfälle	Diebstahl/Raub	Spionage	Sabotage	
Gefährdete Elemente	Gefahren									
4.1.4	Direktions-bereich Produktions-güter (PG)	HB	FB	1.1	1.2	1.3	2.1	2.2	2.3	Bemerkungen
4.1.4.1	Direktionsräume									
–	Direktion	2. OG		M/G	IR	IR	KL	G*	M	* Aktenkonzentration
–	Sekretariat	2. OG		M	IR	IR	KL/IR	M/G	KL/M	
–	Sitzungszimmer	2. OG		KL	IR	IR	KL/IR	G	KL/M	
4.1.4.2	Produktions-güter Marketing (PM)									
–	Büros	2. OG		KL	IR	IR	KL	M*	KL	* Marktdaten
–	Archiv	2. OG		M	IR	IR	IR	G/M	M	
4.1.4.3	Telecommuni-cation (Telec)									
–	Büros	3. OG		M	IR	IR	KL	G*	M	*Geheime Dokumente
–	Laborräume	3. OG		M	M	M	M	G*	G*	* Versuchsreihen
–	Abstellraum	3. OG		M/G	IR	IR	M	M	M	
–	Sitzungszimmer	3. OG		M	IR	IR	IR	G*	KL	* Vertraul. Gespräche
–	Ausstellungs-raum	3. OG		M/G	KL	KL	M	KL	M	

Ka Katastrophe
G groß
M mittel
KL klein
IR Irrelevant

Bild 5: Risikoverteilung

Gefahr				Klassifizierung	Funktionseinheiten Hauptgebäude und Werk II											
					Hauptgebäude	– Zentr. Versorgungseinheiten	– Lager	– Dienstleistung	– Zentralverwaltung	– Zentralarchiv	– Mech. Werkstätten	– System-/Integrationsräume	– Prüffelder	– Konstruktion	– Dokumentation, Logist.	Lager und Büros Werk II
Einwirkung Dritter	innere	1.1.1	Diebstahl aller Art	2			×	×			×	×	×			×
		1.1.2	Informationsdiebstahl, Abhören etc.	2					×	×		×	×	×	×	
		1.1.3	Vandalismus	2												×
		1.1.4	Überfälle, Streit, Angriffe (Pers.)	2				×								
		1.1.5	Sabotage/Anschläge (Brand, Explosion)	2		×			×			×	×			×
	äußere	1.2.1	Autobomben	3		(×)			(×)			(×)	(×)			×
		1.2.2	Brandanschläge/Bombenanschläge	3		×			×							×
		1.2.3	Anlagenzerstörung (z. B. EDV)	3		×						(×)				
		1.2.4	Entführung, Erpressung	3					×							
		1.2.5	Bombendrohung	3					×							
betriebliche		2.1	Brand/Löschmittel	2		×	×	×	×	×		×	×			×
		2.2	Explosion	3		×	×	×								
		2.3	Vergiftung	3				×								
		2.4	Stromschlag	3		×		×			×	×	×			
		2.5	Arbeitsunfälle (Transport etc.)	3		×	×	×			×	×	×			×
		2.6	Lösungsmittel	2			×	×								
		2.7	Verkehrsunfälle	1												
		2.8	Umweltbeeinflussung (HF)	2								×	×			
technische		3.1	Stromausfälle	1		×		×	(×)		×	×	×			
		3.2	Gaslecks	1	(×)	×										
		3.3	Ölschäden, Lecks	1		×										
		3.4	Wassereinbruch	1		×	×	×		×						
		3.5	Säuren, Laugen	1				×								
		3.6	Unterbr. Komm.-leitungen	1					×			(×)	×			
umgebungsbedingt		4.1	Witterungseinflüsse	1							(×)	(×)				
		4.2	EMP/EMV	1		×			(×)			×	×			
		4.3	Schadstoffemission (Luft)	1				×								
		4.4	Ölemission (Wasser, Boden)	1												
		4.5	Flugzeugabstürze, -unfälle	1												

Klassifizierung:
1: geringer möglicher Maximalschaden pro Ereignis, bzw. seltenes Ereignis/Naturereignis (acts of god)
2: Maximalschäden beträchtlich, Personenschäden unwahrscheinlich
3: Maximalschäden erheblich, umfangreich, Personenschäden wahrscheinlich

× = relevant
(×) = bedingt relevant (mittelbare Schadenswirkung)

Bild 6: Risikomaß (Quelle: Wenk, Objektschutzplanung, 1992)

Funktionseinheiten			Einwirkung Dritter											betriebliche Gefahren							
			innere					äußere													
			Diebstahl aller Art	Informationsdiebstahl, Abhören etc.	Vandalismus	Überfälle, Streit, Angriffe (Pers.)	Sabotage/Anschläge (Brand, Explosion)	Autobomben	Brandanschläge/Bombenanschläge	Anlagenzerstörung (z. B. EDV)	Entführung, Erpressung	Bombendrohung	Brand/Löschmittel	Explosion	Vergiftung	Stromschlag	Arbeitsunfälle (Transport etc.)	Lösungsmittel	Verkehrsunfälle	Umweltbeeinflussung
Bereiche, Funktionen, Objekte	Freigelände	– Umzäunung			○			●													
		– Umgebung (angrenzend)				•							•						•		
		Bereich I	•	•	•			⊗	○	●	•	○					○				
		Bereich II	•	•	•			⊗	○		•	○					○				
		Bereich III	•		•	•		⊗			●						○		•		
		– Hauptgebäudefront						⊗		●											
		– Nebengebäude Werk II			•			●													
	Funktionseinheiten Hauptgebäude und Werk II	Hauptgebäude																			
		– Zentr. Versorg.einheiten							•				•	○		•					•
		– Lager	○						•				•				•				
		– Dienstleistung			•	•			•				○	○	○		•	○			•
		– Zentralverwaltung		●			•		●		●	○	•								
		– Zentralarchiv		•									○								
		– Mech. Werkstätten				•										•	○				
		– System-/Integr.räume	•	○			•		○				○			•	•				
		– Prüffelder, Labors	○	○			•						○			•					•
		– Konstruktion		●																	
		– Dokumentation, Logistik		●																	
		– Güteprüfstelle		•																	
		– Ausbildung/Training				•															
		– Lager und Büros Werk II			•				○				•								
	Sonderobjekte	– Wache				•			○		○	○									
		– Archiv		•									○								
		– Kasse	•			○					○										
		– EDV		○					○	●			○								
		– Sonderlager	○				•						●	○	•			•			•
		– VS-Registratur		•																	

⊗ katastrophal
● groß
○ mittel
• klein

Will man nur eine einzige Gefahr (hier die Entwertung von Material) in die Betrachtung einbeziehen, so läßt sich ein Bewertungsverfahren nach Bild 7 heranziehen. Hier werden lediglich für jedes Element des betrachteten Betriebs die relevanten Kriterien, die die Entwendung von Material erleichtern, angekreuzt. Die Summe der Kreuze pro Element ist ein Maß für die Höhe des Entwendungsrisikos an dieser Stelle. Auch so bekommt man einen schnellen Überblick darüber, wo primär mit Maßnahmen anzusetzen ist.

Als letztes Beispiel einer Risikobetrachtung sei eine rein verbale Beschreibung der Risiken, die auf die Elemente eines Betriebes wirken, angegeben (Bild 8). Die Abschätzung der Risiken ist hier rein qualitativ.

Welche der hier kurz skizzierten Verfahren der Risikobewertung anzuwenden sind, hängt vom jeweiligen Einzelfall ab. Wichtig ist, daß das benutzte Verfahren soweit systematisiert ist, daß kein wesentliches Element und keine relevante Gefahr in der Bewertung übersehen wird.

Diese vorangestellte kurze Übersicht kann nur grob skizziert die Gefahrenanalyse und Risikobewertung darstellen. Deshalb sind nachfolgend wesentliche Analysestufen nochmals detaillierter dargestellt.

1.3 Gefahren-/Bedrohungsanalyse

Aufgrund der sich stets ergebenden individuellen Gefahrenlage sind allgemeingültige Konzepte zur Unternehmenssicherung selbst bei Unternehmen gleicher Aufgabenstellung nicht anwendbar, vielmehr muß im Rahmen einer Sicherungsanalyse ein Gefahrenbild entwickelt und hieraus sinnvolle Maßnahmen zur Gefahrenabwehr abgeleitet werden.

Quantitative Verfahren zum Ermitteln der Gefahrensituation und zum Ableiten geeigneter Abwehrmechanismen sind sehr problematisch, weil sich zum einen die Handlungsweise eines Täters als denkendes Individuum

Bild 7: Risikobewertung in einem Betrieb

	Großmenge	Leichte Zugänglichkeit	Handliche Form	Hohe EM-Konzentration	Absetzbarkeit	Gold	Entwendung ohne Risiko	Fehlmenge schwer erkennbar	Bewertung	Risikostufe
Tresor	X		X	X	X	X			5	3
Zentrallager	X	X	X	X	X			X	6	2
Mechanische Fertigung										
Halbzeugfertigung	X	X	X	X	X		X	X	7	1
Nietherstellung		X	X	X	X		X[1)]		5	3
Sinterei	X	X	X	X	X		X	X	7	1
Löterei		X	X	X	X		X		5	3
Schmelze	X	X	X	X	X			X	6	2
Chemische Fertigung										
Galvanik				X	X	X	X	X	5	3
Selektiv-Galvanik	X			X		X	X	X	5	3
Scheiderei	X		X	X	X		X	X	6	2
Gold- und Salzherstellung	X	X	X	X		X	X[1)]		6	2
Edelmetallpräparate		X	X	X		X		X	5	3

[1)] Kleinstmenge