



Elektronische Sicherheitssysteme

2.10 Schwachstellenanalyse

2.10.1 Gefahren identifizieren

2.10.2 Risiken beurteilen

2.10.3 Maßnahmen erstellen

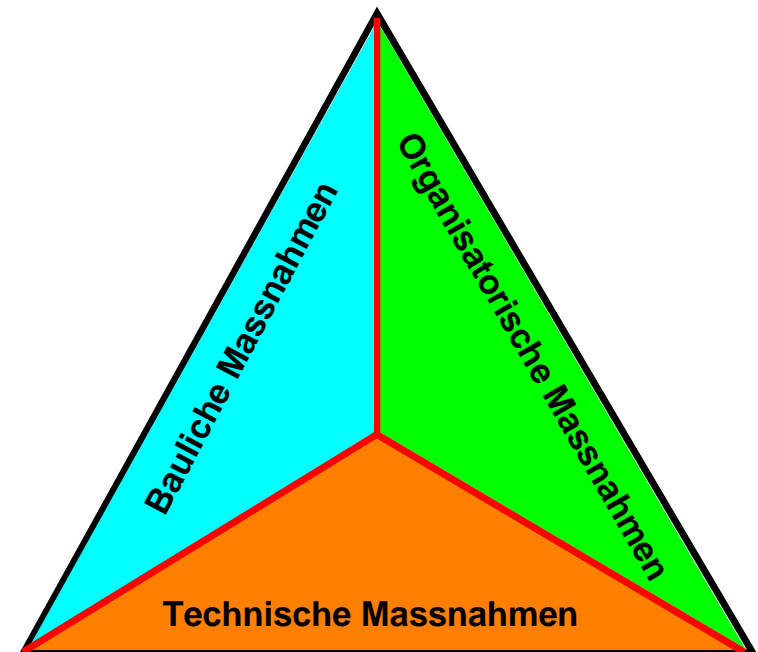
2.10.4 Sicherheitskonzepte



Warum beschäftigen wir uns mit diesem Thema?

Verschiedene Bedrohungen können die Sicherheit eines Unternehmens beeinträchtigen. In der Praxis werden nach einem Schadenfall oft nur punktuelle Massnahmen realisiert.

Ein übergeordnetes Konzept ist ein Arbeitsmittel, um die baulichen, technischen und organisatorischen Massnahmen ausgewogen zu planen und zu realisieren.





Das menschliche Leben ist eng verflochten mit der Abschätzung von Risiken für Leib, Leben und Besitz.

Jeder Mensch sieht sich vor die Aufgabe gestellt, seine persönlichen Risiken zu kennen, mit ihnen zu leben, sie eventuell zu vermeiden oder zu reduzieren. Schafft er das nicht, können unerwünschte Ereignisse dazu führen, dass der Mensch Schaden an seiner Gesundheit, seinem Besitz, seinem Ansehen oder an anderer Stelle nimmt.

Der Zusammenschluss von Menschen zu sozialen Gemeinschaften führte dazu, dass auch eine Gemeinschaft mit den Risiken klarkommen musste, die alle Mitglieder der Gruppe betrafen. Von Anfang an war und ist Risikomanagement ein wichtiger Teil des menschlichen Lebens.



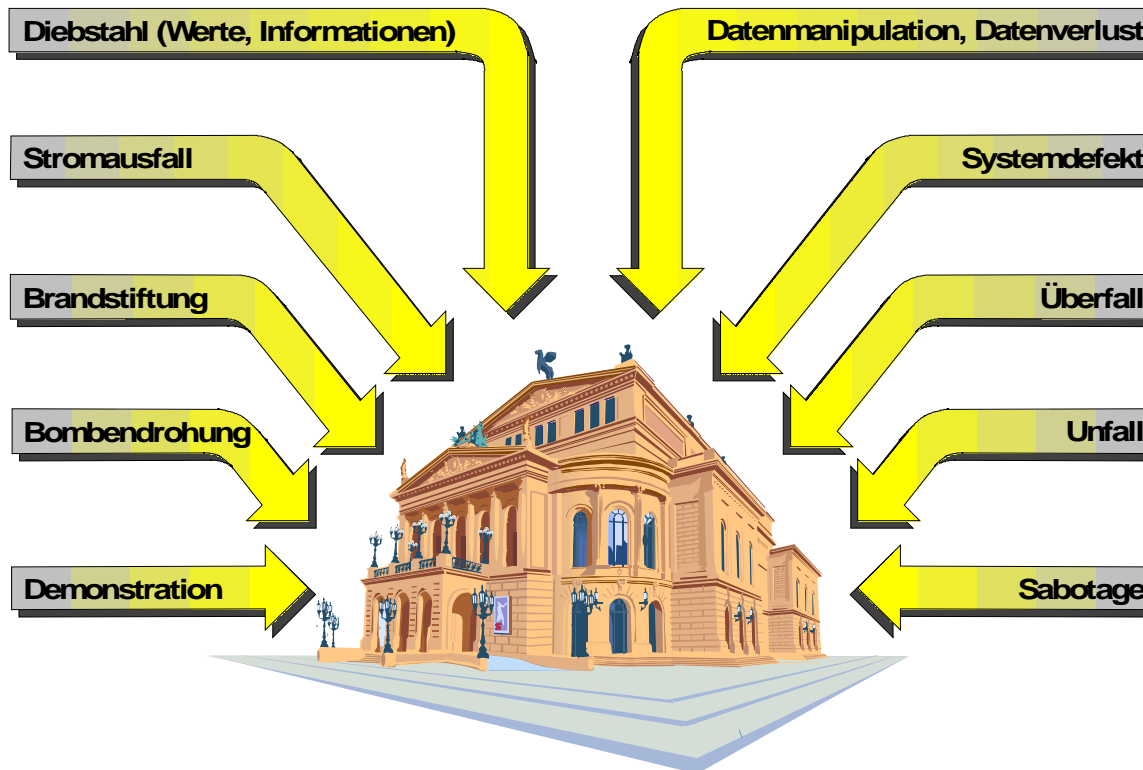
Zweck: Gefahren, die den kontinuierlichen Betriebsablauf bedrohen, erkennen und bekämpfen,

1. Gefahren identifizieren, Risiken beurteilen und Prioritäten setzen

2. Planung, Realisierung und Überwachung von Maßnahmen
 1. organisatorisch
 2. technisch



Bedrohungsbild



Zusatzinformationen: Methodik Sicherheitskonzept.pdf



Zusammenhang zwischen Schwachstelle, Wert, Bedrohung und Schaden

Beispiel:

Wenn die Tür zum Rechenzentrum **kein Schloss** hat (Schwachstelle)

und in diesem Rechenzentrum eine CD mit **wichtigen Betriebsdaten** (Wert)
unbewacht und frei zugänglich (Schwachstelle 2) auf einem Tisch liegt

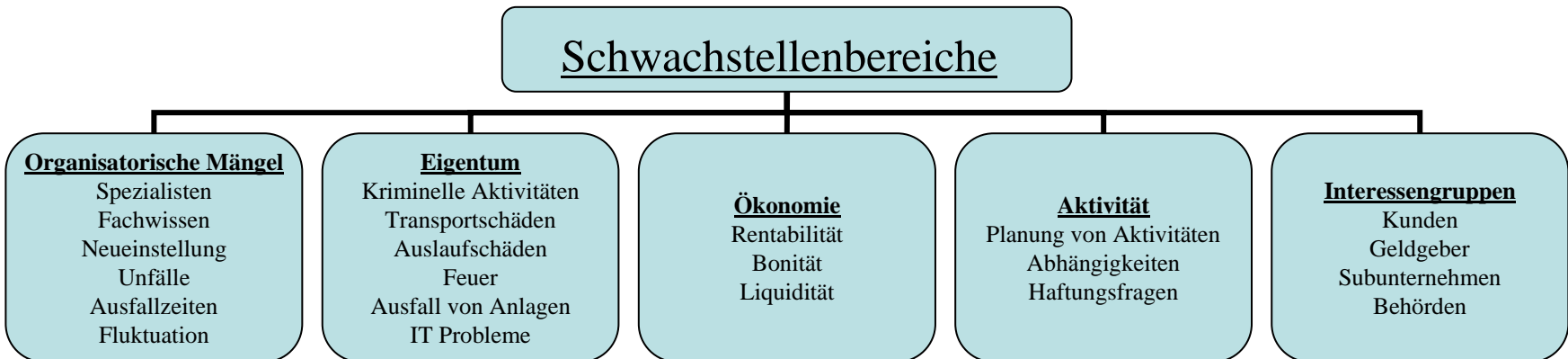
und ein **potentieller Dieb** draußen herumläuft (Bedrohung),

dann wird dieser Dieb mit einer gewissen **Wahrscheinlichkeit** (Wahrscheinlichkeit)
tatsächlich in das Rechenzentrum eindringen und die Betriebsdaten aus dem
Rechenzentrum **stehlen** (Schaden).



Beispiel (Schwachstellenkatalog)

Art der Schwachstelle	Erläuterung	Art der Bedrohung	Risiko-bewertung und Priorität	Verbesserungs-Vorschlag/Empfehlung (Maßnahmen)
Kein Schloss in der Tür zum Rechnerraum	Die Tür zum Rechnerraum ist nicht gesichert. Außerdem erfolgt keine Aufzeichnung, wann und wer diesen Raum betritt..	Einbruch - Potentiellen Dieben wird es leicht gemacht, diesen Raum unbemerkt zu betreten	3/B	<ul style="list-style-type: none"> •Installation einer Zutrittskontrolle •Erstellen von Zugangsberechtigungen •Optional Videoüberwachung und Videoaufzeichnung
Papierlager neben dem Kopierer	Erhöhte Brandlast, eventuell fahrlässiges Handeln,	Möglicher Brand, besonders, wenn der Kopierer nicht beaufsichtigt wird (Nachts)	4/A	<ul style="list-style-type: none"> •Installation eines Rauchmelders über dem Kopierer •Papierlager verlegen





Natürliche Ereignisse

Menschliches Fehlverhalten

Fehlfunktionen

Missbrauch

Diebstahl

Vandalismus

***Weitere Einteilungen
Von
Schwachstellenbereichen***

Quelle: R. Moses „Risk Analysis and Management“



Risiken personeller Art

Unfälle

Unfälle haben Fehl- und Ausfallzeiten, schwere Verletzungen oder Schlimmeres zur Folge.

Ausfallzeiten

Dies kann im Extremfall sogar zur Produktionsunterbrechung führen, wenn man für solche Fälle nicht vorgesorgt hat und andere geschulte Mitarbeiter nicht einspringen können.

Fluktuation

Ein schlechtes Betriebsklima, eine unzureichende Entlohnung, unzufriedenstellende Arbeitsbedingungen, Angst vor Arbeitsplatzverlust und eine unsichere Unternehmenszukunft sind Faktoren, die in Mitarbeitern Abwanderungsgedanken reifen lassen.



Risiken personeller Art

Neueinstellungen

Eine unglückliche Auswahl bei der Einstellung neuer Mitarbeiter oder das Delegieren von Aufgaben an ungeeignete Mitarbeiter kann zu Problemen führen:

Fachwissen

Es gilt, Fachwissen zu pflegen und dieses gleichzeitig ständig weiterzuentwickeln.

Einsatz von Spezialisten

Manchmal ist es sinnvoll, Aufgaben, die Spezialwissen erfordern, an Experten weiterzugeben. Expertenwissen macht sich bezahlt, auch wenn es teuer ist



Unfallrisiken

Unfälle ereignen sich meist ohne Vorwarnung.

Unfälle haben Fehl- und Ausfallzeiten, schwere Verletzungen oder Schlimmeres zur Folge. Auch wenn sich noch keine schweren Unfälle am Arbeitsplatz (oder auf dem Weg zum oder vom Arbeitsplatz) ereignet haben, sind „kleinere Unfälle“ erste Warnzeichen. Auch die sogenannten “Beinaheunfälle“ weisen auf mögliche Risiken hin. Eine schlechte Arbeitsvorbereitung, mangelhafte Ausrüstung oder eine fehlende Erste Hilfe Ausbildung sind mitentscheidend für besonders gravierende Unfallfolgen.

Tipp:

Unfallpotentiale können mit Hilfe von Unfallstatistiken analysiert werden. Sollen Risiken im voraus identifiziert und Gegenmaßnahmen abgeleitet werden, sind für risikobehaftete Maschinen und Arbeitstätigkeiten Sicherheitsanalysen durchzuführen.



Risiken durch Mitarbeiterausfall

Aufgrund der Erkrankungen von Mitarbeitern in Schlüsselpositionen können Engpässe in den betrieblichen Abläufen entstehen. Dies kann im Extremfall sogar zur Produktionsunterbrechung führen, wenn man für solche Fälle nicht vorgesorgt hat und andere geschulte Mitarbeiter nicht einspringen können.

Erkrankungen können auch durch das Unternehmen beziehungsweise die Arbeitstätigkeit selbst verursacht werden, z. B. durch unergonomische Arbeitsbedingungen. Außerdem lebt ein kleines Unternehmen durch das Engagement seiner Mitarbeiter.

Tipp:

Die durchschnittlichen Fehlzeiten in den einzelnen Abteilungen können als Kennzahlen für andere Abteilungen herangezogen werden (achten Sie jedoch auf korrekte Bezugsgrößen und vergleichen Sie nicht Äpfel mit Birnen). Sie können auch über Ihre Berufsgenossenschaft entsprechende Referenzzahlen einholen.



Risiken am Eigentum

Kriminelle Aktivitäten

Einbruch, Sabotage, Vandalismus

Transportschäden

Zu berücksichtigende Gefahren können auch durch eigenen Transportaktivitäten (z. B. Werksverkehr) ausgelöst werden. Bei einem Verkehrsunfall können z. B. transportierte Waren beschädigt oder Passagiere verletzt werden.

Auslaufschäden

Sie können durch Wasser oder andere flüssige Substanzen verursacht werden.



Risiken am Eigentum

Feuer

Sind Vorkehrungen getroffen und eine eventuelle Brandstiftung erschwert?

Ausfall von Anlagen/Betriebsmitteln

Jede Maschine und jedes Gerät kann an einem bestimmten Punkt, aufgrund von Abnutzung oder Materialermüdung, versagen. Meist passiert dies im ungünstigsten Moment.

Informationsrisiken

Ein Geräteausfall der Computer, Computerviren, ein kleines Feuer oder ein Wasserschaden können wichtige Informationen zerstören. Dateien können ungewollt oder mutwillig gelöscht werden.



Risiko durch kriminelle Aktivitäten

Zusätzlich zu den wertvollen Maschinen, Geräten und Rohstoffen, ziehen auch Fertigwaren Diebe an.

Ungenügende Beleuchtung und ein ferner Standort macht es den Einbrechern und Vandalen leichter zu handeln.

Besucher könnten vertrauliche Informationen von unvorsichtig aufbewahrten Papieren erwerben. Ein Missbrauch könnte dem Unternehmen viel Schaden zufügen.

In einigen Branchen stellen gewalttätige Kunden eine Gefahr dar.



Tipps

Risiko durch kriminelle Aktivitäten

- Regelmäßige Inspektionsrundgänge,
 - Kameraüberwachung,
 - Zugangskontrolle,
 - Alarmanlagen,
 - zuverlässige Sperrungssysteme und
 - geeignete Zäune verhindern unbefugten Zugang zum Grundstück.
-
- Die Sicherheit erhöht sich auch, wenn die Ware gekennzeichnet wird, denn so ist sie auf dem Schwarzmarkt schwierig zu verkaufen.



Risiko durch Feuer

Falls keine ausreichenden Vorkehrungen zur Brandeindämmung und –bekämpfung getroffen worden sind, erhöht sich die Wahrscheinlichkeit, dass sich ein Feuer ausbreiten kann.

Ein Brandstifter in Ihrer Umgebung kann Ihrem Unternehmen ebenfalls ernsthaft schaden. Die Gefahr und die Folgen von Brandstiftungen können durch erhöhte Beleuchtung und Überwachung im Außengelände verringert werden. Abfallbehälter und andere brennbare Materialien, die unmittelbar in der Nähe eines Gebäudes aufbewahrt werden, ziehen Brandstifter an.

Allgemeine Ordnung und Sauberkeit, regelmäßige Instandhaltung von Maschinen und Geräten sowie korrekte Lagerung von brennbaren Flüssigkeiten und Gasen verringern Feuergefährdungen. Ferner sollten Abfall, Altpapier und andere brennbare Materialien weit genug vom Gebäude entfernt gelagert werden.



Risiken in der Unternehmensökonomie

Rentabilität

Kosten können sich unkontrolliert in die Höhe schrauben, wenn die Kostenüberwachung unzureichend ist. Falsche oder fehlende Kostenzuweisungen führen zu unrealistischen Produkt- und Servicepreisen.

Bonität

Um auf einer gesunden Basis zu arbeiten, braucht ein Unternehmen ausreichend Eigenkapital. Ein Unternehmen sollte sich nicht allein durch Fremdkapital finanzieren.

Liquidität

Der Zahlungsrückstand von Großkunden kann sich nachhaltig auswirken. Vorübergehende Zahlungsunterbrechungen seitens der Kunden können die eigene Liquidität stark beeinträchtigen. Auch Kreditverweigerungen schwächen die Liquidität.



Risiken in der Unternehmensökonomie

Planung von Aktivitäten

Wenn Investitionen in die Entwicklung neuer Produkte und potentieller Dienstleistungen unzulänglich sind und auf sich verändernde Bedürfnisse und Nachfragen der Kunden nicht rechtzeitig eingegangen wird, übernehmen die Mitwettbewerber unter Umständen eine führende Rolle auf dem Markt..

Abhängigkeiten

Heutzutage bilden viele Unternehmen Netzwerke. Das bedeutet, dass der Erfolg des eigenen Unternehmens vom Handeln und vom Erfolg anderer Unternehmen beeinflusst wird.

Haftungsfragen

Unternehmer sind für ihre Produkte verantwortlich. Das bedeutet, sie haften auch für Schäden, die aus der Herstellung und dem Vertrieb ihrer Produkte entstehen. Für Umweltschäden können sie ebenfalls haftbar gemacht werden.



Risiken bei den Interessengruppen

Unabhängig von den unternehmerischen Betätigungsfeldern ist jedes Unternehmen immer eingebunden in ein Netzwerk von geschäftlichen Partnern (Zulieferer, Subunternehmer, Verbände, Kammern, Behörden, Kunden). Ohne diese Vernetzung ist unternehmerisches Handeln unmöglich. Der Aufbau von Netzwerken ist verknüpft mit zeitgemäßem Management und Unternehmenspraktiken.

Die genaue Kenntnis des Unternehmensumfelds bietet Chancen, die Risiken in Zusammenhang mit den Kooperationspartnern zu erkennen. Kunden, Geldgeber, Untervertragsnehmer und Behörden werden als Interessensgruppen im folgenden behandelt.

- Kunden
- Geldgeber
- Subunternehmer
- Behörden



Kein Risiko:

Das Risikopotential ist so niedrig, dass es für das Unternehmen als nicht signifikant eingestuft wird, oder das beschriebene Problem hängt nicht mit den Unternehmensaktivitäten und dem betrieblichen Umfeld zusammen.

Risiko unter Kontrolle:

Das Problem stellt ein signifikantes Risikopotential für das Unternehmen dar, ist aber unter Kontrolle. Dadurch ist die Auftretenswahrscheinlichkeit gesunken.

Handlungsbedarf:

Das Risikopotential ist hoch. Weitere Analysen sind notwendig oder es müssen sofort Maßnahmen ergriffen werden. Die identifizierten Risikofaktoren haben bereits zu erheblichen Verlusten geführt oder können noch dazu führen.



Die Dringlichkeit der Durchführung von Maßnahmen wird in erster Linie auf der Grundlage des Bedrohungspotentials von Risiken für das Unternehmen entschieden.

Das Ausmaß eines Risikos hängt von zwei Faktoren ab:

- **Wahrscheinlichkeit:** Je häufiger oder wahrscheinlicher eine Gefahr auftritt, desto größer ist das Risiko.
- **Folgen:** Je größer der Schaden ist den eine Gefahr verursacht, desto größer ist das Risiko.



Das Ausmaß eines Risikos kann beispielsweise entweder mit Worten

- vernachlässigbar, gering, mäßig bis unakzeptabel oder untertätlich oder
- numerisch z.B. 1 bis 5 beschrieben werden.

Wahrscheinlichkeit des Ereignisses	Folgen des Ereignisses		
	Gering	Schädlich	Ernst
Unwahrscheinlich	1. Bedeutungsloses Risiko	2. Geringes Risiko	3. Mäßiges Risiko
Möglich	2. Geringes Risiko	3. Mäßiges Risiko	4. Bedeutsames Risiko
Wahrscheinlich	3. Mäßiges Risiko	4. Bedeutsames Risiko	5. Unerträgliches Risiko

2.10.2. Risiken bewerten



Schadensauswirkung	Stufe	Beschrieb der Auswirkungen
Klein	1	Geringe Auswirkungen: <ul style="list-style-type: none"> - Dienstleistung nicht wesentlich gestört - keine Verletzte - kein Imageverlust
Mittel	2	Mittlere Auswirkungen: <ul style="list-style-type: none"> - Dienstleistungen wesentlich gestört - Sachschäden und Betriebsausfall- - wenige Verletzte - mittlerer Imageverlust
Gross	3	Grosse bis katastrophale Auswirkungen: <ul style="list-style-type: none"> - Weitere Dienstleistungen unmöglich - Große Sachschäden und Betriebsausfall - einige Schwerverletzte - grosser Imageverlust

2.10.2. Risiken bewerten



Eintrittswahrscheinlichkeit	Stufe	Kriterium
Klein	1	unwahrscheinlich z. B. 1 mal in 5 Jahren
Mittel	2	möglich z. B. 1 bis 2 mal pro Jahr
Gross	3	Wahrscheinlich z. B. 5 bis 10 mal pro Jahr



Risiko = Eintrittswahrscheinlichkeit x Grösse des potentiellen Schadens

Eintrittswahrscheinlichkeit	Schadensfolge		
	gering	Mittel	Groß
Unwahrscheinlich - klein	1x1=1	2x1=2	3x1=3
Möglich - mittel	1x2=2	2x2=4	3x2=6
Wahrscheinlich - groß	1x3=3	2x3=6	3x3=9



Festlegung der Priorität

Priorität	Risikowert	Massnahmen
A	6 oder 9	Es sind zwingend Risiko mindernde Massnahmen zu treffen
B	4	Es muss von Fall zu Fall über Massnahmen entschieden werden.
C	1, 2 oder 3	Es werden keine Massnahmen getroffen.



Sicherheitspolitik

Die Sicherheitspolitik legt fest, welche Risiken der Auftraggeber/Bauherr selber tragen resp. welche er auf ein erträgliches Mass verringern bzw. welche er gegebenenfalls versichern will.

Schutzziele und Auflagen

Schutz von Personen:

Mitarbeiter, Besucher, Handwerker, Servicetechniker etc.

Schutz der Werte:

Sachwerte, Materielle Werte und immaterielle Werte

Vorgaben von Versicherungen, der Geschäftsleitung, der internen Revision oder des Sicherheitsverantwortlichen, Feuerwehr, Brandschutznorm

2.10.3. Maßnahmen erarbeiten



1. Die Dringlichkeit der Maßnahmen hängt von dem Ausmaß der Risiken ab.
2. Beginnen Sie mit den Maßnahmen, deren Gefahrenpotential am höchsten eingeschätzt wurde und beseitigen Sie diese Gefahren umfassend und systematisch.
3. Aber vernachlässigen Sie nicht ganz die "akzeptablen oder moderaten Risiken". Diesen kann oft mit relativ geringfügigen Kosten entgegengewirkt werden.
4. Nicht alle Risiken können beseitigt werden.



Übertragung und Verteilung des Risikos:

Eine Gefahr kann auf einen anderen Akteur, beispielsweise mit Vereinbarungen, übertragen werden. Typische Vereinbarungen betreffen Transport und Subunternehmen. Eine andere Alternative ist z. B. die Folgen einer Gefahr durch Versicherungen zu reduzieren.

Beibehalten des Risikos:

Risiken sind ein Bestandteil von Unternehmensaktivitäten. Einige Risiken müssen toleriert werden, weil sie Bestandteil der unternehmerischen Verantwortung sind. Vorschläge zum Umgang mit identifizierten Gefahren und Problemen oder zu ihrer weiteren



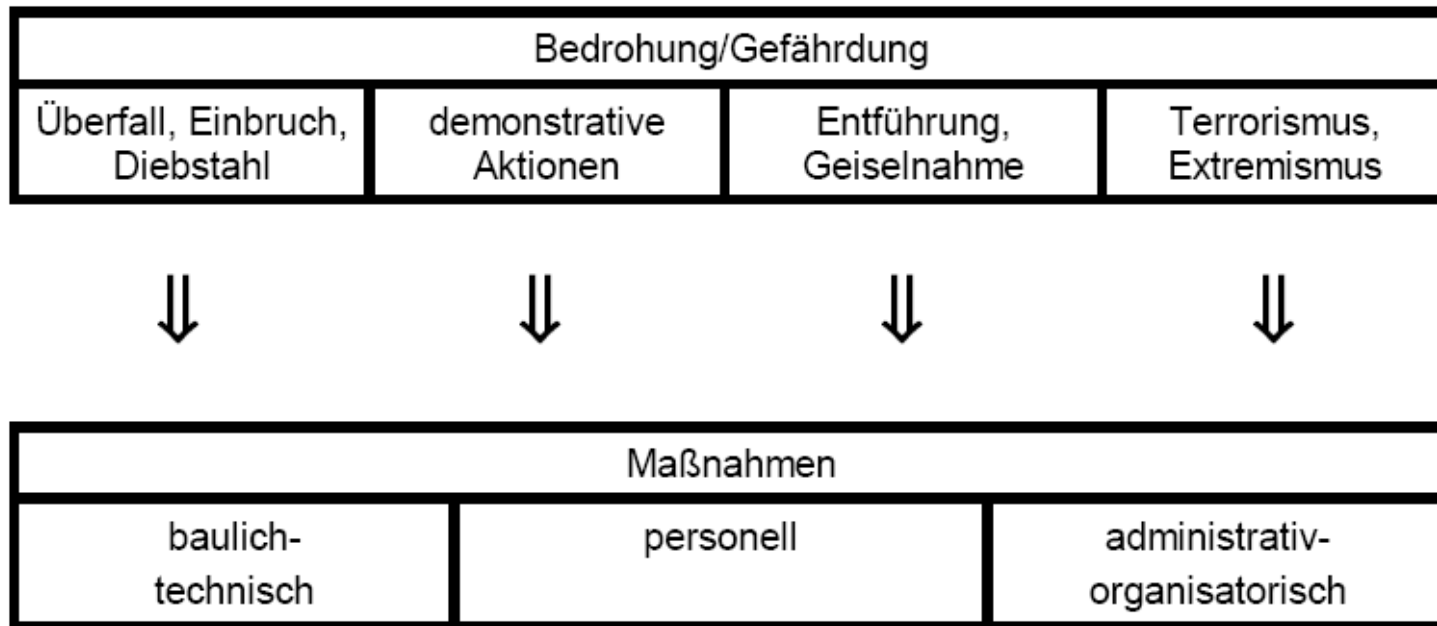
Vermeidung des Risikos:

Normalerweise ist es nicht möglich, ein Risiko vollständig auszuschließen. Dies ist meist nur dann zu erreichen, wenn diese Unternehmensaktivität eingestellt oder vermieden wird. Die mit der Handhabung einer gefährlichen Chemikalie verbundenen Risiken können z. B. durch das Wechseln zu einer unbedenklichen Substanz vermieden werden.

Reduzierung des Risikos:

Ein Risiko kann verringert werden, wenn es möglich ist, die Wahrscheinlichkeit oder die Folgen eines Falls zu beeinflussen. Das Bestreben geht dahin, die Umstände so anzupassen, dass die betreffende Gefahr so selten wie möglich auftritt und dass ihre Folgen, bei Auftreten, so gering wie möglich sind.

2.10.3. Maßnahmen erarbeiten





Beispiel: Entgegenwirken von kriminellen Aktivitäten und Personenschutz

Organisatorisch:

- Rundgänge durch Werkschutz
- Einbindung von Wachschutzunternehmen
- Sensibilisierung von Mitarbeitern

Technisch:

- Einbruchmeldeanlage
- Zutrittskontrollanlage
- Videoüberwachung
- Brandmeldeanlage

Baulich:

- Zäune
- Bessere Tore und Fenster



Weitere Möglichkeiten organisatorischer Maßnahmen

Erarbeiten sie Beispiele von organisatorischen Maßnahmen in der Gruppe. Einige Beispiellösungen werden im Anschluss zur Verfügung gestellt.



Weitere Möglichkeiten organisatorischer Maßnahmen

- Unterschiedliche Zutrittsregelungen
- Formalitäten bei Anlieferung von Werten und Waren
- Alarmierungs- und Interventionskonzept
- Alarmerfassung und -bearbeitung
- Lagerung, Klassifizierung und Handhabung vertraulicher Akten, Datenträger
- Pflichten und Aufgaben des Sicherheitspersonals
- Schlüssel- und Ausweisverwaltung



Weitere Möglichkeiten baulicher Maßnahmen

Erarbeiten sie Beispiele von baulichen Maßnahmen in der Gruppe. Einige Beispiellösungen werden im Anschluss zur Verfügung gestellt.



Weitere Möglichkeiten baulicher Maßnahmen

- Festlegen der Sicherheitszonen und Brandabschnitte
- Festlegen von Personenvereinzellungen
- Festlegen der Wandstärken für sicherheitsrelevante Räume
- Fluchtwege / Notausgänge
- Schleusen
- Sicherheitsverglasungen
- Sicherheitstüren und Brandschutztüren
- Treppenhäuser und Lifte
- etc.



Weitere Möglichkeiten technischer Maßnahmen

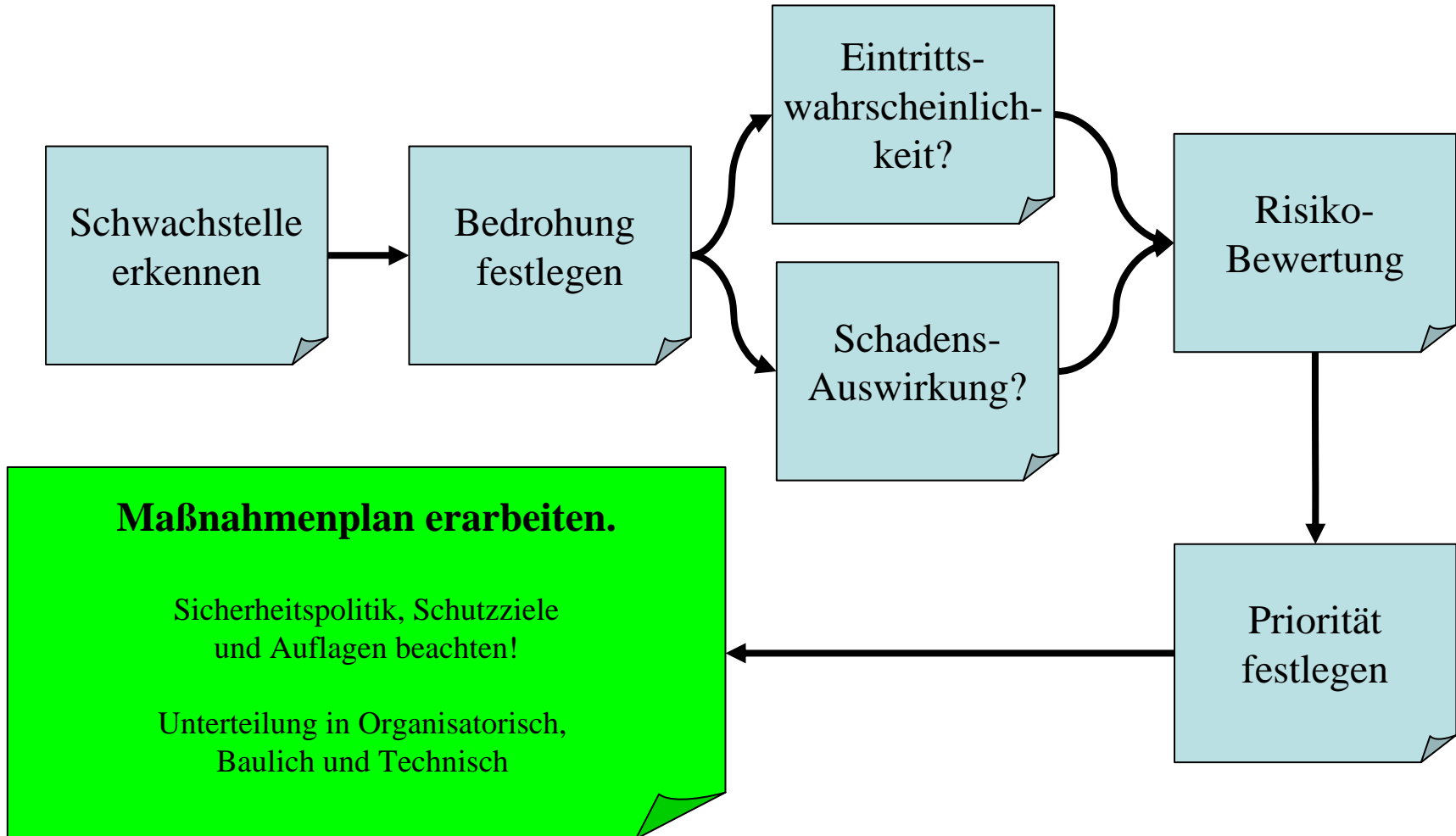
Erarbeiten sie Beispiele von technischer Maßnahmen in der Gruppe. Einige Beispiellösungen werden im Anschluss zur Verfügung gestellt.



Weitere Möglichkeiten technischer Maßnahmen

- Brandmeldeanlage
- Brandfallsteuerungen
- Automatische und manuelle Löschanlage
- Einbruchmeldeanlage
- Not- Energieversorgung
- Evakuationsanlage (Notruf)
- Fluchtweg- und Notbeleuchtung
- Gasmeldeanlage
- Kommunikationssysteme

2.10.4. Sicherheitskonzept





Durchführung einer Schwachstellenanalyse und Risikobewertung

- Erarbeitung in Gruppenarbeit
- Erfahrungen verschiedener Personengruppen kombinieren
- Nur die Risikopotentiale beschreiben, die für das jeweilige Unternehmen spezifisch sind
- auflisten der identifizierten Themenbereiche so präzise wie möglich.

Tipps:

- gemeinsam den Leiter des Teams festlegen
- am Anfang ebenfalls festlegen, wer mitschreibt
- Zeitplan festlegen
- Abschweifen vom Thema vermeiden.



Schwachstellenanalyse für einen Tankstellenbetrieb.

Ein Tankstellenpächter beauftragt sie mit der Schwachstellenanalyse seiner Tankstelle. Anhand dieser Schwachstellenanalyse sollen Sie ein Konzept erarbeiten, das das alltägliche Risiko beim Betrieb dieser Tankstelle minimiert.

Die Tankstelle liegt an einer Bundesstraße außerhalb einer kleinen Ortschaft. Vor allem Nachts ist wenig Betrieb. Trotzdem ist die Tankstelle sowie der dazu gehörende Shop 24h, 7 Tage in der Woche geöffnet. Der Pächter klagt nicht nur über gelegentlichen Benzindiebstahl, sondern auch über Diebstahl von Zigaretten im Shop. Sein Mitarbeiterstamm (8, davon 6 im Verkauf/Kasse) besteht derzeit zum größten Teil aus Studenten, die etwa halbjährlich wechseln. Es ist auch schon vorgekommen, dass einer dieser Mitarbeiter Diebstähle aktiv unterstützt hat. Sicherheitstechnische Anlagen existieren noch nicht.

2.10.4. Sicherheitskonzept – Übung



Art der Schwachstelle	Erläuterung	Art der Bedrohung	Risiko Priorität	Verbesserungs- Vorschlag/Empfehlung



Schäden werden bei Tankstellen durch unterschiedliche Risiken hervorgerufen.

Sie entstehen im wesentlichen durch

- Benzindiebstahl,
 - Ladendiebstahl im Shopbereich,
 - Freundschafts- bzw. Verwandtschaftskäufe und
 - Raubüberfälle.
-
- Weitere Ausführungen in gesonderten File
„Schwachstellenanalyse an Tankstellen.pdf“