

[2] Risikoidentifizierung als Basis für die Entwicklung einer Abwehrstrategie

Einführung

Um den Herausforderungen des Know-how-Schutzes wirksam begegnen zu können, ist eine fundierte Analyse der unternehmensspezifischen Risikosituation notwendig. Die Schaffung einer Wissensbasis zur Produktpiraterie hilft bei der Risikoanalyse. Dabei ist die Wertschöpfungskette in den Mittelpunkt der Betrachtungen zu stellen. Das folgende Kapitel zeigt auf:

- | wie ein Risikoprozessmodell zur Bewertung der Risikosituation beitragen kann
- | welche Perspektiven der Risikobewertung einzunehmen sind
- | welche Wissensquellen im Unternehmen auf welche Weise gefährdet sind
- | wie Auslöser und Ursachen des Wissensabflusses bestimmt werden können
- | auf welche Weise das vorgestellte Modell im Unternehmen angewendet werden kann.

Als Aufgabenbeschreibung für eine Abwehrstrategie gegen Produktpiraterie bietet sich die Definition einer erfolgreichen Strategie von Ulrich und Fluri an. Diese verstehen unter Strategie die „[...] Erfolgsvorsteuerung durch den frühzeitigen und systematischen Aufbau von strategischen Erfolgspotenzialen. Es geht dabei um Steuerungsgrößen qualitativer Art, nämlich um die erforderlichen Fähigkeiten der Unternehmung, auf den ‚Innovationsdruck‘ und auf ‚strategische Überraschungen‘ [...] wie ein guter Schachspieler aus einer Position der Stärke heraus flexibel, wirksam und erfolgreich reagieren zu können. [...] die Schaffung von Voraussetzungen zur ‚Beherrschung‘ der strategischen Ungewissheit und Komplexität, kann [...] nur erfolgreich gelöst werden, indem alle unternehmerischen Kräfte und Ressourcen von Anfang an konsequent in den Dienst einer klaren Unternehmensstrategie gestellt werden“ (Ulrich und Fluri 1995).

Ergänzend zu dieser Definition, bei der die Aufgabe der Strategie mit der eines erfolgreichen Schachspiels gleichgesetzt wird, sollte die Einschätzung eines der besten Schach-Großmeister aller Zeiten, Gary Kasparow, zu den Erfolgsfaktoren von Strategien nicht fehlen. Dieser machte deutlich, dass es im Schach wie im realen Leben bei Entscheidungsfindungen „[...] generell viel wichtiger [ist], eine kleine Menge von Zügen korrekt zu bewerten als wie ein Computer systematisch tiefer und tiefer nach besseren Zügen zu graben beziehungsweise immer mehr Züge ‚vorauszusehen‘“ (Kasparow 2010).

Es kommt bei der Entwicklung der Strategie nicht darauf an, detaillierte und quantifizierte Risikomaße festzusetzen und eine Vielzahl von „Zügen“ vorauszusehen, sondern darauf, die Situation richtig einzuschätzen und aus wenigen, bereits vorgefilterten Alternativen die für das jeweilige Unternehmen richtige auszuwählen. Übersetzt für die Herausforderung der Entwicklung und Umsetzung einer Strategie gegen Produktpiraterie bedeutet dies im Wesentlichen die Verfolgung von vier Zielen:

- Schaffung einer Informationsbasis und Einschätzung der Risiken
- Auswahl und Umsetzung von geeigneten Maßnahmen
- Überführung der Maßnahmen in standardisierte Prozesse
- Kontinuierliche Verbesserung des Schutzes.

Dabei sollte die Verantwortung der Leitung bezüglich Zieldefinition, Selbstverpflichtung, Risikoanalyse, Managementbewertung, Sensibilisierung bzw. Bewusstseins-schaffung im Unternehmen und Lenkung des Schutzes klar angesprochen werden. Weiterhin sind die Voraussetzungen für ein professionelles Management der Ressourcen zu schaffen, indem die Höhe der bereitgestellten Ressourcen sowie die notwendigen Kompetenzen festgelegt werden, das Personal geschult und eine geeignete Infrastruktur geschaffen wird. Ebenso sind die unternehmensspezifischen Anforderungen an eine Umsetzung zu definieren und zwar aus Produkt-, Prozess- und Kundensicht sowie aus normativer Sicht. Die Messung, Analyse und kontinuierliche Verbesserung des Schutzes erfordert die Definition von Anforderungen an eine Überwachung und Messung der Schutzqualität, die Durchführung von Audits und Prozessanalysen, eine Überwachung

im Markt, eine Datenanalyse, die Definition und Vermittlung des Verhaltens bei Entdeckung von Plagiaten, eine Analyse des Kundenverhaltens und, falls notwendig, die Korrektur fehlerhafter Maßnahmen sowie eine konsequente Aktualisierung der Wissensbasis im Unternehmen.

Zur Umsetzung dieser definierten Ziele sollte die Entwicklung einer Abwehrstrategie fünf Prozessschritten folgen, wie in Abbildung 2.1 dargestellt.

Dieser Prozess ist nicht als statisches Befolgen der Schritte, sondern als dynamischer Prozess anzusehen. Die Schritte werden sich hier im Zeitablauf überlagern und es wird Rückkopplungen geben. Wie genau ein Unternehmen auf diese Weise eine passende Abwehrstrategie entwickeln kann, wird in den folgenden Kapiteln dargelegt.

Abb. 2.1: Das Darmstädter Modell zur Entwicklung einer Piraterie-Abwehrstrategie

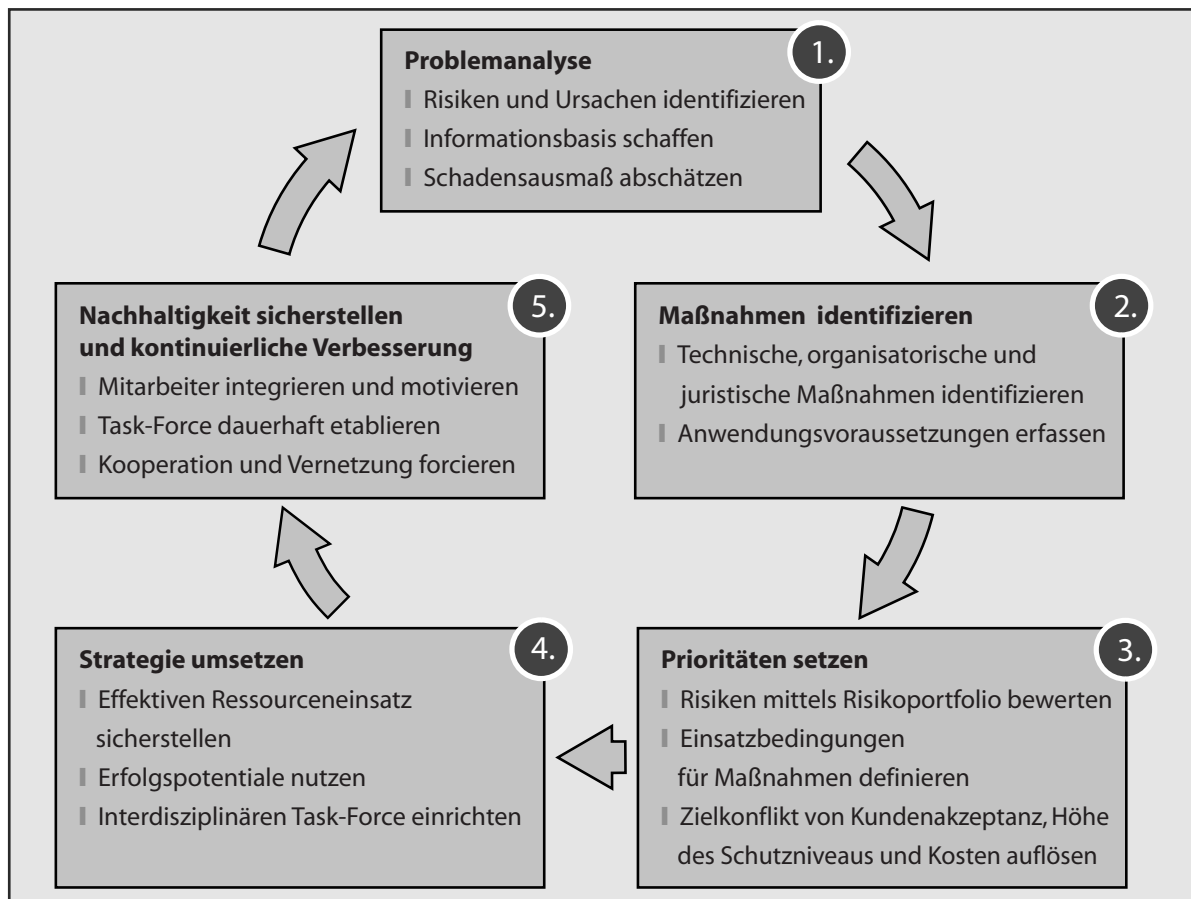
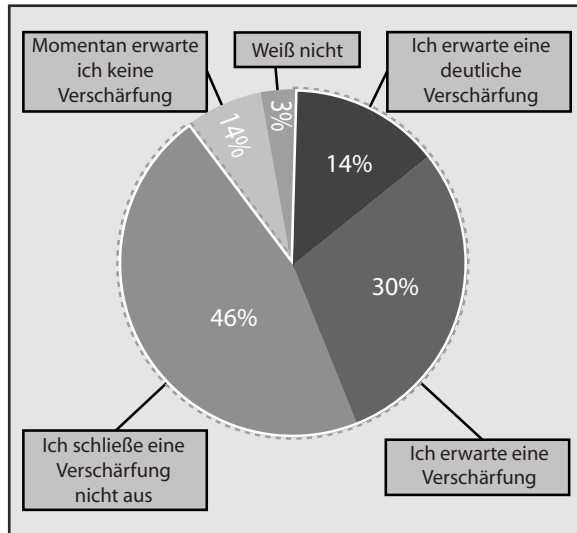
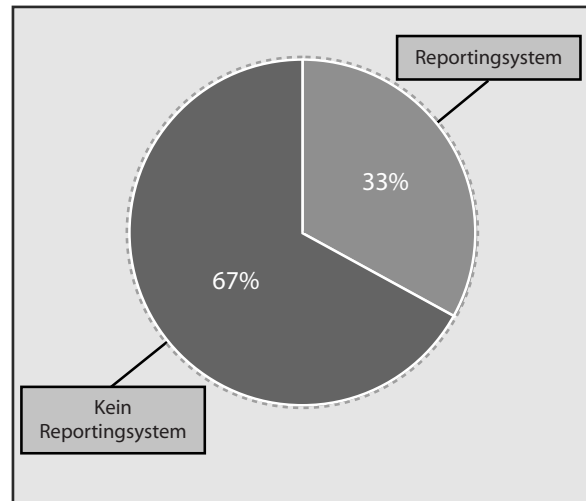


Abb. 2.2: Piraterie verschärft sich (Karg und Petersen 2010)**Abb. 2.3: Einsatz von Reportingsystemen zur Steuerung der Know-how-Schutzstrategie (Karg und Petersen 2010)**

2.1 Schaffung einer Wissensbasis zur Produktpiraterie

Obwohl Produktpiraterie nach einer aktuellen Studie fast drei Viertel aller Unternehmen in Deutschland betrifft bzw. nur zwölf Prozent der 230 befragten Unternehmen ausschließen, von Produktpiraterie betroffen zu sein, dagegen etwa 90 Prozent der Unternehmen eine Verschärfung des Problems entweder erwarten oder nicht ausschließen (Karg und Petersen 2010, siehe Abb. 2.2), ist bei fast allen Unternehmen die Wissensbasis zum Thema erstaunlich gering ausgeprägt (Staake und Fleisch 2008).

Dabei sind Informationen zur geschätzten Größe des Marktes für Plagiate, zum finanziellen Schaden, den ein Unternehmen erleidet, zur Rolle des Kunden sowie zu den Strategien und zum Kompetenzniveau der Piraten – immer bezogen auf das Umfeld, in dem sich das jeweilige Unternehmen bewegt – entscheidend für eine fundierte Risikobewertung und Auswahl geeigneter Maßnahmen. Eines der wichtigsten und zugleich häufig eines der am meisten vernachlässigten Ziele eines Unternehmens muss also das konsequente und strukturierte Sammeln sowie die fundierte Analyse aller Informationen sein. Dennoch hat die überwiegende Mehrheit der Unternehmen keine Reportingsysteme installiert (Abb. 2.3, Karg und Petersen 2010).

Eine detaillierte Informationssammlung ist notwendig, da selbst Unternehmen gleicher Branchenzugehörigkeit und mit ähnlichen Produktkategorien ganz unterschiedlichen Herausforderungen ausgesetzt sein können. Gleichzeitig haben Unternehmen sehr unterschiedliche Voraussetzungen zur Bekämpfung von Produktpiraterie hinsichtlich der verfügbaren Ressourcen, der bereits installierten Schutzmaßnahmen, sei es in den Prozessen oder in den Produkten, sowie der Produkteigenschaften, wie z. B. Komplexität, Sichtbarkeit am Markt oder verkaufter Stückzahlen. Die Risiken sind nicht nur von Unternehmen zu Unternehmen verschieden, sondern liegen zusätzlich noch auf unterschiedlichen Ebenen. So gibt es Unternehmensrisiken, die in der Charakteristik des Unternehmens zu suchen sind, und Prozessrisiken, wie z. B. unsichere Lieferwege bei der Supply Chain.

Abbildung 2.4 zeigt beispielhaft einen Meldebogen für die Entdeckung eines Plagiates. Hier werden die wesentlichen Eckdaten zum Imitat und dem entsprechenden Originalprodukt strukturiert erfasst, sodass diese Informationen ausgewertet und entsprechende Schlüsse zur Bedrohungslage gezogen werden können. Dieses Meldeblatt sollte Teil eines standardisierten Reportingsystems werden, wie es im Detail noch in Kapitel 4 beschrieben wird.

Abb. 2.4: Beispiel eines Meldeblattes für aufgegriffene Plagiate

Plagiatsvorfall

Meldebogen

Mitarbeiterkürzel:
E-Mail-Adresse:

Abteilung:
Telefon:

Datum:
Eingang:

Informationen zum Plagiat:

Was wurde imitiert?	Wo wurde das Plagiat vertrieben?	Wie wurde das Plagiat beworben?
Zu welchem Preis wurde das Plagiat angeboten?	Vermutete Qualität des Plagiats:	Wer hat das Imitat angeboten?
Wie wurden Sie auf das Plagiat aufmerksam?	Produktbezeichnung des Imitats:	Vermutete Herkunft der Fälscher:
Konnte ein Muster erworben werden und wurde dieses analysiert?	Wenn ja: Was sind die Ergebnisse der Analyse?	

Ableich mit Daten zum Originalprodukt:

In welcher Lebenszyklusphase befindet sich das imitierte Produkt?	Welchen Anteil am Gesamtumsatz erwirtschaftet das betroffene Produkt?	Mit welchem Fertigungsprinzip wird das imitierte Produkt hergestellt?
Welchen Individualitätsgrad besitzt das betroffene Produkt?	Wo wird das imitierte Produkt hergestellt?	Wie schätzen Sie die technologische Komplexität des Produktes ein?

Verteiler: Mitarbeiter => Beauftragter Plagiatschutz => Unternehmensleitung => Betroffener Produktmanager und Bereichsleitung => Rückmeldung an Mitarbeiter

2.2 Die Wertschöpfungskette als Mittelpunkt des Risikomanagementprozesses

Zusätzlich ins Kalkül gezogen werden sollten die Angriffszeitpunkte und -orte der Produktpiraten, bezogen auf die Lebenszyklusphase des Produktes bzw. auf die Wertschöpfungskette. Betroffen sind grundsätzlich alle Teile der Wertschöpfungskette, besonders schwer allerdings Forschung und Entwicklung sowie Vertrieb und Produktverkauf. Aber auch Produktion, Service,

Vorentwicklung und Ressourcenbeschaffung stehen im Fokus der Produktpiraten (Karg und Petersen 2010).

Eine Methodik zur Analyse der spezifischen Risikosituation muss einem ganzheitlichen Ansatz folgen und den gesamten Produktlebenszyklus abdecken, von der Ressourcenbeschaffung bis hin zur Entsorgung. Die Vorgehensweise und Ergebnisse müssen dabei einfach zu verstehen sein und einen allgemeingültigen Charakter haben. Gleichzeitig muss diese Methodik so modular aufgebaut sein, dass unternehmensspezi-

fische Risikosituationen bewertet werden können und diese praxisgerecht und einfach handhabbar ist. Als Ergebnisse werden die Evaluierung des gesamten Gefährdungspotenziales des Unternehmens im Kontext Produktpiraterie, die Identifikation von Schutzlücken im Unternehmen, die Ausgabe der relevanten Risiken mit Ursachen und möglichen Konsequenzen sowie geeignete Gegenmaßnahmen erwartet.

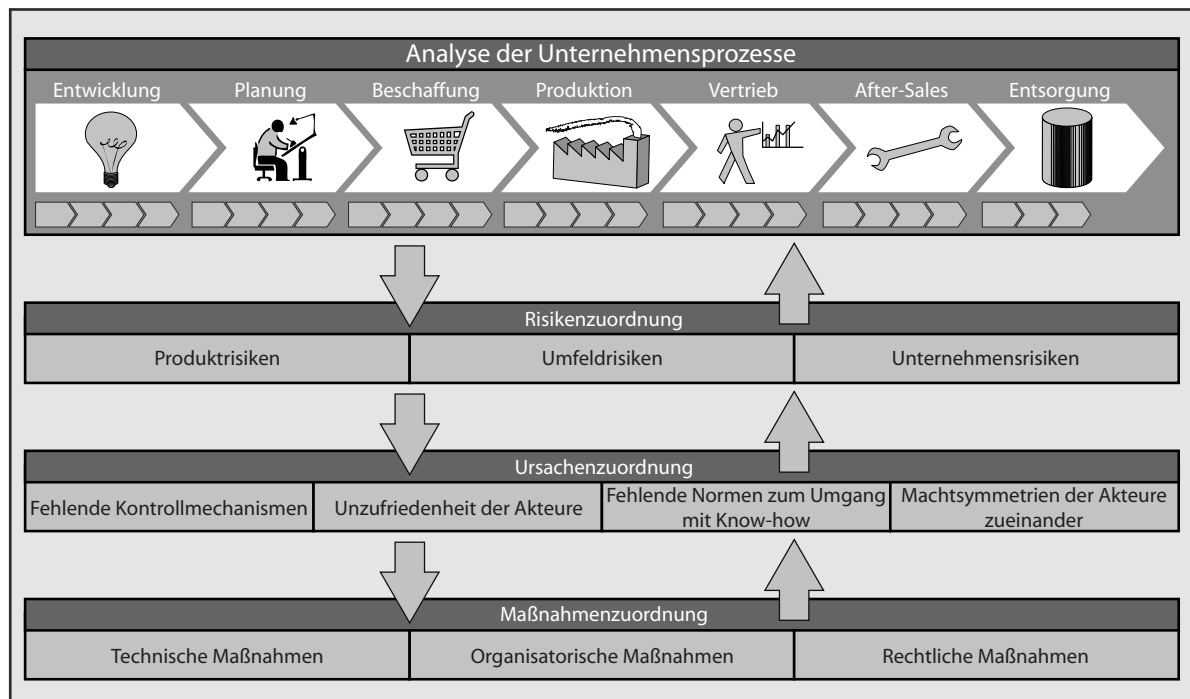
Das im Unternehmen bereits verfügbare Wissen und durch beständige Risikoanalysen neu gesammelte Informationen sollten systematisch dokumentiert werden, um für zukünftige Analysen zur Verfügung zu stehen. Die Risikobewertung kann dabei grundsätzlich mit Blick auf das Gesamtunternehmen oder aber mit Blick auf ein einzelnes Produkt erfolgen.

Bei der unternehmensbezogenen Analyse sollten die Prozesse mit ihren beteiligten Akteuren sowie die Wissensträger berücksichtigt werden. Auch die produktbezogene Analyse sollte mit Blick auf die Unternehmensprozesse erfolgen. Zusätzlich sind hierbei aber direkt bereits bekannte Plagiatsfälle mit den vorhandenen Produkten zu verknüpfen.

2.3 Entwicklung eines Risikoprozessmodells zur Identifizierung der Risikosituation

Zur Lösung dieser Aufgabe ist also ein Prozessmodell geeignet, wie es am Institut für Produktionsmanagement, Technologie und Werkzeugmaschinen (PTW) der TU Darmstadt entwickelt wurde. Dieses basiert auf einem typischen produzierenden Unternehmen in seinen Funktionsstrukturen Entwicklung, Produktionsplanung, Beschaffung, Produktion, Vertrieb, After-Sales und Entsorgung. Die einzelnen Funktionen werden in der entwickelten Methodik durch die Abbildung ihrer typischen Prozesse konkretisiert. Ein Prozess wird dabei mithilfe seiner Schritte, der handelnden Akteure und der mit ihm verbundenen Wissensträger beschrieben. Im Modell sind den Unternehmensprozessen Risiken mit ihren jeweiligen Ursachen zugeordnet, die spezifisch für Produktpiraterie in der Investitionsgüterindustrie sind. Gleichzeitig sind Gegenmaßnahmen, die zur Reduzierung der Risiken geeignet sind, im Modell integriert. Der grundlegende Aufbau des Modells ist in Abbildung 2.5 dargestellt.

Abb. 2.5: Struktur des Risikoprozessmodells



Mit in einer Software hinterlegten Merkmalen und Indikatoren kann jedes Unternehmen auf einfache Weise die für die eigene Situation relevanten Risiken und Schutzlücken ableiten und somit die wesentlichen Handlungsfelder für die Implementierung einer Abwehrstrategie identifizieren. Die verwendete Software ermöglicht es dabei, nicht nur den Prozess effizient zu steuern, sondern das Wissen auch zu sammeln, um so über die Zeit eine immer präzisere Datenbasis verfügbar zu machen. Damit die Risiken minimiert oder sogar eliminiert werden können, ist die Auswahl geeigneter Gegenmaßnahmen vonnöten. Dazu müssen die Ursachen der Risiken bekannt sein. Infolge einer Analyse der Risiken konnten vier Hauptursachenkategorien, nämlich „fehlende Kontrollmechanismen“, „Unzufriedenheit der Akteure“, „fehlende Normen zum Umgang mit Know-how“ und „Machtasymmetrien der Akteure zueinander“ identifiziert werden, die unterschiedliche Ausprägungen besitzen. Dadurch können wirksame Gegenmaßnahmen den Risikoursachen und somit den Risiken selbst gegenübergestellt werden. Die Strukturierung der Risiken bildet die Basis, auf der ein Unternehmen zum richtigen Zeitpunkt sowohl produkt- als auch prozessorientiert effektive Gegenmaßnahmen auswählen und realisieren kann.

Die Methodik muss hinsichtlich des Know-how-Verlustes die Fragen nach dem „Wie“, dem „Womit“, dem „Wer“ und dem „Warum“ beantworten können. Aufgrund der wachsenden Komplexität der Logistikketten mit einer zunehmenden Internationalisierung von Beschaffung, Produktion und Distribution so-

wie Reduzierung der Fertigungstiefe (vgl. u. a. Graf 2005) erfolgt eine intensive Verlagerung von Teilen des Know-hows zu den Wertschöpfungspartnern (Pfohl 2004). Gleichzeitig entstehen komplexe Unternehmensverbünde, deren Logistikketten ineinander verzahnt sind, was die Gefahr eines unerwünschten Wissensabflusses erhöht. Dies erklärt, weshalb die vorgeschlagene Methodik zur Einschätzung der Risikosituation auf die Wertschöpfungskette fokussiert. Charakter, Zielsetzung und Zielgruppe der Methodik sind in Abbildung 2.6 dargestellt.

2.4 Perspektiven der Risikobewertung

Die Risikosituation eines Unternehmens wird aus zwei Perspektiven betrachtet: unternehmensbezogen und produktbezogen (Abb. 2.7).

In der unternehmensbezogenen Perspektive lässt sich das Gefährdungspotenzial des Unternehmens hinsichtlich Produktpiraterie unter Berücksichtigung der Unternehmensprozesse, der hier vorhandenen Wissensträger sowie der beteiligten Akteure einschätzen. Unternehmensprozesse, Wissensträger und Akteure werden hier als Bestandteile eines Unternehmens definiert. In dieser Analyse wird versucht, alle Bestandteile des Unternehmens zu umfassen, d. h., es werden alle Prozesse, alle beteiligten Akteure und alle Wissensträger analysiert.

In der produktbezogenen Perspektive steht die Gefährdung der Produkte eines Unternehmens im Vordergrund. Daher setzt diese Perspektive das Vorhandensein eines Plagiats bzw. eines Plagiatverdachts voraus. Die Dimension Produkt wird mit den Faktoren Plagiateigenschaften, Eigenschaften des betroffenen Produktes und produktbezogenen Faktoren beschrieben.

Um die Risikosituation hinsichtlich der Produktpiraterie aus unternehmens- und produktbezogener Sicht systematisch zu analysieren, wird der Risikomanagementprozess zugrunde gelegt. Mithilfe der Phasen Risikoidentifizierung, Risikobewertung, Risikobehandlung und Risikomonitoring kann die Risikosituation nach den beiden oben genannten Perspektiven in strukturierter Weise untersucht werden. Bei der Anpassung des Risikomanagementprozesses an die Erfordernisse des Modells wird für die Phasen des

Abb. 2.6: Eigenschaften der Risikobewertungsmethodik

Art der Bewertung	Qualitative Bewertung
Ziel	Abbildung der Risikosituation
Ergebnis	Gefährdungspotenzial, Risiken, betroffene Prozesse, Ursachen und Maßnahmen
Zielgruppe	Entscheidungssträger des Unternehmens

Abb. 2.7: Perspektiven der Risikobewertung

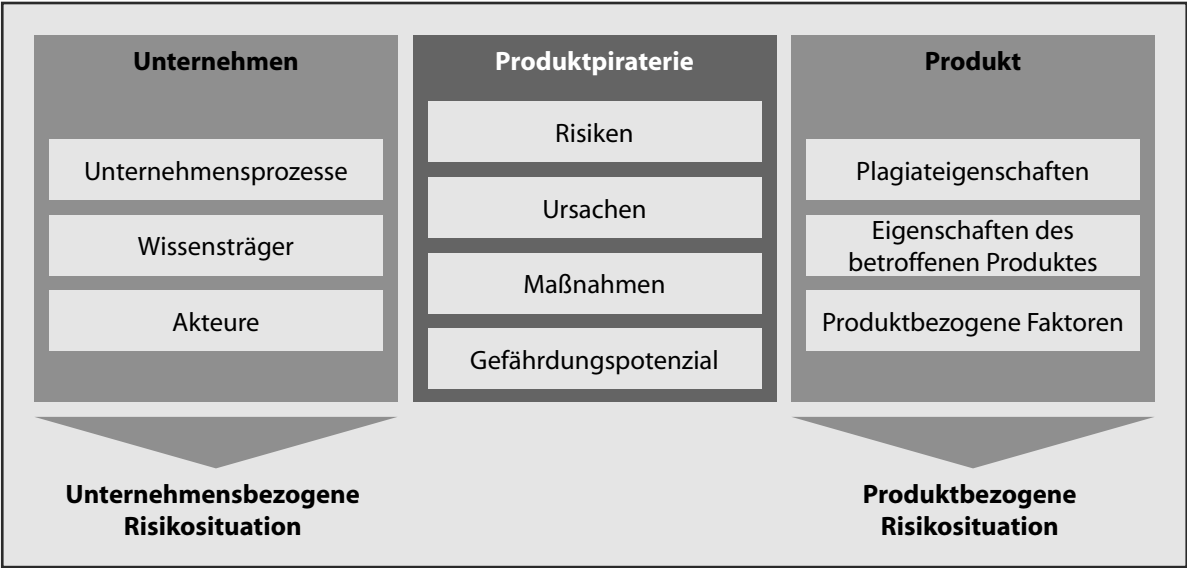


Abb. 2.8: Risikomanagementmodell

	Perspektive der Risikosituation	
	Unternehmensbezogene	Produktbezogene
Risikoidentifizierung	Wissensträger in Unternehmensprozessen	Produktbezogene Einflussfaktoren
Risikobewertung	Unternehmensindividuelle Risikobewertung Gefährdungspotenzial	Gefährdungsgrad Eintrittswahrscheinlichkeit
Risikobehandlung	Betroffene Prozesse Ermittlung von Ursachen Ableitung von Maßnahmen	Einbringen von Isolationsmechanismen
Risikomonitoring	Risiken Betroffene Prozesse Ursachen und Maßnahmen	Bedrohungslage des Produktes

Risikomanagementprozesses auch zwischen unternehmens- und produktbezogener Perspektive differenziert. Dies ist notwendig, da das IT-gestützte Instrument für jede dieser Perspektiven unterschiedliche Ergebnisse liefert. Der Schwerpunkt liegt aber auf der unternehmensbezogenen Risikosituation. Abbildung 2.8 stellt einen Überblick des präsentierten Risikomanagementmodells dar.

2.5 Wissensträger im Unternehmen

Wesentlich für die Bewertung einer Risikosituation ist die Identifizierung und Betrachtung der Wissensträger. Dabei stellt sich die Frage, womit bzw. wodurch der Wissensabfluss erfolgt (materieller Wissensträger) und wer den Know-how-Abfluss auslösen kann (personeller Wissensträger).

Grundsätzlich kommen als Wissensträger alle Medien und Personen in Betracht, die Daten und Informationen über das Produkt transportieren können.

Im Bereich der materiellen Wissensträger sind hier zu nennen:

- Produktdaten
- Das Produkt selbst mit seinen Bestandteilen
- Anlagen und Infrastrukturen
- Schutzrechte.

2

Produktdaten sind in gedruckten und digitalen Unterlagen, Dokumenten oder Präsentationen vorhanden. Da Produktdaten in nahezu jedem Prozess involviert sind, werden sie in Produktentstehungsdaten, Produktionsdaten, kaufmännischen Daten, Vertriebsdaten sowie Reparatur- und Wartungsdaten untergliedert.

Das Produkt und seine Bestandteile, wie Komponenten, Materialien, Prototypen und Produktmuster, tragen ebenso Know-how und können eine Quelle des ungewollten Know-how-Abflusses sein. Sie tragen vor allem Informationen über den Herstellungsprozess des Produktes.

Die Anlagen und Infrastrukturen im Unternehmen stellen ebenso einen Wissensträger im Unternehmen dar, denn durch Maschinenspezifikationen, Besichtigungen und das Ausspähen fremder Produktionsstätten bei Betriebsrundgängen kann viel Know-how abfließen.

Schließlich enthalten Schutzrechte, wie z.B. Patente, sehr sensible Informationen über das Produkt. Daraus können wichtige Informationen über das Produkt selbst und seinen Herstellungsprozess gewonnen werden.

Abb. 2.9: Wissensquellen im Unternehmen

Produktdaten		Akteure	Sonstiges	
Produktentstehungsdaten <ul style="list-style-type: none"> ■ Produktidee ■ Skizzen & Entwürfe ■ Berechnungen ■ Simulationsergebnisse ■ Zeichnungen ■ Versuchsunterlagen ■ Nullserieninformationen ■ Forschungsergebnisse 	Vertriebsdaten <ul style="list-style-type: none"> ■ Prospekte ■ Datenblätter ■ Kataloge in allen Formen ■ Angebotsunterlagen ■ Unternehmenspräsentationen ■ Artikel in Fachzeitschriften ■ Produktankündigung ■ Internetpräsenz ■ Geschäftsberichte ■ Pressemeldungen ■ Kundenrabattstruktur ■ Produktpräsentation ■ Preislisten 	Mitarbeiter Externe Partner <ul style="list-style-type: none"> ■ Entwicklungspartner ■ Serviceanbieter ■ Zwischenhändler ■ Lieferant ■ Endkunde Lieferant <ul style="list-style-type: none"> ■ Maschinenhersteller ■ Anlagenhersteller ■ Betriebsmittellieferant ■ Rohstofflieferant ■ Komponentenlieferant ■ Halbzeuglieferant Serviceanbieter <ul style="list-style-type: none"> ■ Logistikdienstleister ■ Reparaturdienstleister ■ Inbetriebnahmedienstleister ■ Lohnhersteller ■ Externer Auditor ■ Reinigungsdienstleister 	IK-Systemen <ul style="list-style-type: none"> ■ Internet ■ E-Mails ■ Intranet ■ Wissenstransferportale ■ Konstruktionsdatenbanken ■ Produktionsdatenbanken ■ Vertriebsdatenbanken ■ Laufwerke Anlagen und Infrastrukturen <ul style="list-style-type: none"> ■ Zugangseinschränkungen ■ Abgangseinschränkungen ■ Maschinensteuerungsprogramme ■ Spannkonzepete ■ Vorrichtungskonzepete ■ Werkzeugkonzepete 	Produkt <ul style="list-style-type: none"> ■ Prototyp & Vorprodukte ■ Produktmuster ■ Ausschussware ■ Komponenten / Bauteile ■ Materialien ■ Ersatzteile ■ Produkttechnologie ■ Herstellungsprozess Rechtliche Absicherung <ul style="list-style-type: none"> ■ Verträge ■ Zertifikate ■ Schutzrecht Produktbezogene Aktivitäten <ul style="list-style-type: none"> ■ Externe Tests / Feldversuche ■ Schulungen ■ Schutzmaßnahmen ■ Produktsonderapplikationen ■ Externe Instandhaltung ■ Messen
Produktionsdaten <ul style="list-style-type: none"> ■ Montageplan ■ Fertigungsplan ■ Normen & Toleranzen ■ Verpackungsdaten 				
Qualitätsprüfungsdaten <ul style="list-style-type: none"> ■ Qualitätsvorschriften ■ Prüfprotokolle ■ Prüftechnologie 	Reparatur- und Wartungsdaten <ul style="list-style-type: none"> ■ Reparaturanleitungen ■ Wartungsanleitungen ■ Inbetriebnahmeanleitungen ■ Ausfallfelddaten 			
Kaufmännischen Daten <ul style="list-style-type: none"> ■ Herstellungskosten ■ Beschaffungskosten ■ Lieferantenbewertungen ■ Bestelldaten ■ Deckungsbeitrag 				

Personelle Wissensträger sind zunächst alle an der Produktion beteiligten Akteure. Sie werden in zwei große Gruppen untergliedert: Mitarbeiter und externe Partner. Zu den externen Partnern gehören Lieferanten und Serviceanbieter (wie z. B. externe Auditoren, Lohnfertiger, Entwicklungspartner, Logistikdienstleister, Reinigungsdienstleister). Abbildung 2.9 gibt einen Überblick über die verschiedenen Wissensträger.

2.6 Auslöser des Wissensabflusses

Um mit den Maßnahmen nicht die Symptome zu bekämpfen, sondern die Ursachen, sind die Auslöser für Know-how-Abfluss zu identifizieren. Im Allgemeinen ist ein Know-how-Abfluss im Unternehmen auf vier Faktoren zurückzuführen:

- Fehlende oder unzureichende Kontrollmechanismen
- Fehlende oder unzureichende Normen zum Umgang mit Know-how
- Unzufriedenheit der Akteure
- Starke Verhandlungsmacht der Akteure.

Diese vier Faktoren sind später für eine exaktere Ursachenermittlung noch mit dem Umfeld des Wissensabflusses und den Wissensträgern zu verknüpfen und sollen hier zunächst beschrieben werden.

2.6.1 Fehlende oder unzureichende Kontrollmechanismen

Als Kontrollmechanismen werden alle Maßnahmen zum Schutz von Unternehmens-Know-how bezeichnet. Ziele dieser Kontrollmechanismen sind die Senkung der Eintrittswahrscheinlichkeit von Schadensfällen, die Minimierung der Auswirkungen, die Kontrolle bestehender Restrisiken sowie die frühzeitige Erkennung und rechtzeitige Verhinderung neuer Risiken (Linkies und Karin 2010). Wenn in Unternehmen kein Bewusstsein über die Problematik der Produktpiraterie herrscht, fehlen Kontrollmechanismen, die einen ungewünschten Know-how-Abfluss vermindern und regulieren. Beispiele von fehlenden Kontrollmechanismen sind nicht vorhandene Identifizierungsmerkmale im oder am Produkt, sodass eine Unterscheidung von Plagiaten nicht möglich ist, oder fehlende Ein- und Ausgangskontrollen in sensiblen Unternehmensbereichen wie der Entwicklung.

2.6.2 Fehlende oder unzureichende Normen oder Richtlinien zum Umgang mit Know-how

Sicherheitsrichtlinien stellen Regeln dar, die jeder befolgen muss, und beschreiben Verfahren, wie diese Regeln anzuwenden und durchzusetzen sind (Cobb 2003). Richtlinien müssen so einfach wie möglich gehalten werden, damit sie von den Mitarbeitern verstanden werden. Sie müssen sowohl von Vorgesetzten als auch von Mitarbeitern akzeptiert werden. Das Nichtvorhandensein von Richtlinien und Normen im Unternehmen ermöglicht einen ungewollten Know-how-Abfluss. Deswegen ist es essenziell, im Unternehmen Richtlinien zu definieren, die Mitarbeiter bei Interaktionen mit anderen Akteuren beachten müssen. Damit wird die ungewollte Preisgabe sensibler Informationen, z. B. bei Verhandlungen verhindert.

2.6.3 Unzufriedenheit der Akteure

Unter Zufriedenheit (oder Unzufriedenheit) eines Akteurs wird die für eine Person kennzeichnende Einstellung gegenüber dem Arbeitsverhältnis verstanden (in Anlehnung an Scupin 2006). Insbesondere im Hinblick auf die Produktpiraterie ist die Mitarbeiterzufriedenheit von großer Bedeutung. Die Unzufriedenheit der Mitarbeiter gilt als eine der häufigsten Quellen der Produktpiraterie, gerade vor dem Hintergrund gesellschaftlicher und technischer Veränderungen. Eine zunehmende Zahl von Zeitarbeitern, die häufig auch im administrativen Bereich Zugriff auf sensible Informationen haben, oder der Einsatz von „ewigen Praktikanten“ bedeutet nicht selten auch eine gesunkene Mitarbeiterbindung. Die Entwicklung in der Informations- und Kommunikationstechnologie (große Datenspeicher, E-Mail etc.) erleichtert zusätzlich den Know-how-Diebstahl (Huber 2009). Je unzufriedener ein Mitarbeiter ist, desto wahrscheinlicher ist es, dass er ein unkorrektes Verhalten aufzeigt. Motive dafür können Not, Geldgier, Rache oder Profilierungswünsche sein. Aber nicht nur unzufriedene Mitarbeiter, sondern auch unzufriedene Kunden, Lieferanten oder Serviceanbieter sind ein Risiko für die Entstehung von Piraterie. Auch sie können Piraterietäter werden.

2.6.4 Starke Verhandlungsmacht der Akteure

Verhandlungen sind auf vielen Industriegütermärkten der zentrale Transaktionsmechanismus. In Verhandlungen legen Anbieter und Nachfrager in einem

Prozess des Informationsaustausches und der gegenseitigen Beeinflussung die technischen, ökonomischen und juristischen Details einer Transaktion fest. Je stärker die Verhandlungsposition eines Akteurs ist, desto wahrscheinlicher ist ein starker Lieferant, der sich bei Vertragsverhandlungen nicht an den Abschluss von Exklusivverträgen binden lässt und in der Folge Materialien oder Maschinen an andere Kunden weiterverkauft. Ein weiteres Beispiel ist die Nichteinhaltung von Vertraulichkeitsvereinbarungen durch einen Kunden. Dies kann z. B. gefährlich werden, wenn der Kunde Ersatzteile, Komponenten oder Serviceleistungen bei anderen Anbietern nachfragt und er diesen Anbietern spezifische Informationen über die Produkte oder Dienstleistungen zur Verfügung stellt. Diese Anbieter können auch Piraten sein. Der Kunde kann aber ebenso selbst Kopien in Auftrag geben.

wissentlich oder unwissentlich in ihrer Schutzfunktion, indem sie sensibles Wissen preisgeben.

Im zweiten Fall sind externe Partner des Unternehmens, wie z. B. Zulieferer oder Logistikdienstleister, für den Wissensabfluss verantwortlich. Sie sind Produktpiraterietäter oder haben keine besonderen Schutzmechanismen vor Piraterie. Im letzten Fall findet der Know-how-Abfluss abwärts in der Supply Chain statt, d. h., Kunden oder Zwischenhändler sind für die Entstehung des Pirateriefalls verantwortlich. Sie können auch selbst Fälscher sein. Abbildung 2.10 zeigt einen Überblick über Auslöser und Umfeld des Wissensabflusses sowie betroffene Wissensträger.

Die Ursachen von Know-how-Verlust können nun durch eine Kombination dieser drei Kategorien ermittelt werden, wie in Abbildung 2.11 dargestellt.

2.7 Umfeld des Wissensabflusses

Nach der Identifikation der möglichen Wissensträger im Unternehmen und den Gründen für einen Know-how-Abfluss ist als dritte Bewertungsgröße das Umfeld des Wissensabflusses von Interesse, um so eine eindeutige Kategorisierung der Ursache vornehmen zu können. Eine Möglichkeit ist die Unterscheidung des Umfeldes des Know-how-Abflusses nach Unternehmen, Branchen oder Märkten.

Im ersten Fall beschränkt sich der Wissensabfluss auf das Unternehmen, d. h., zuständige Mitarbeiter für den Wissenstransfer oder vielmehr -abfluss versagen un-

Abb. 2.11: Definition der Ursache des Wissensabflusses

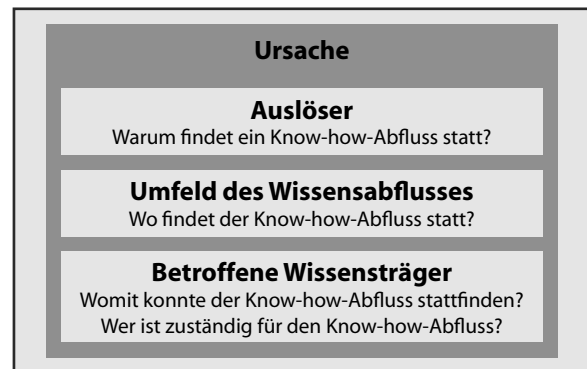
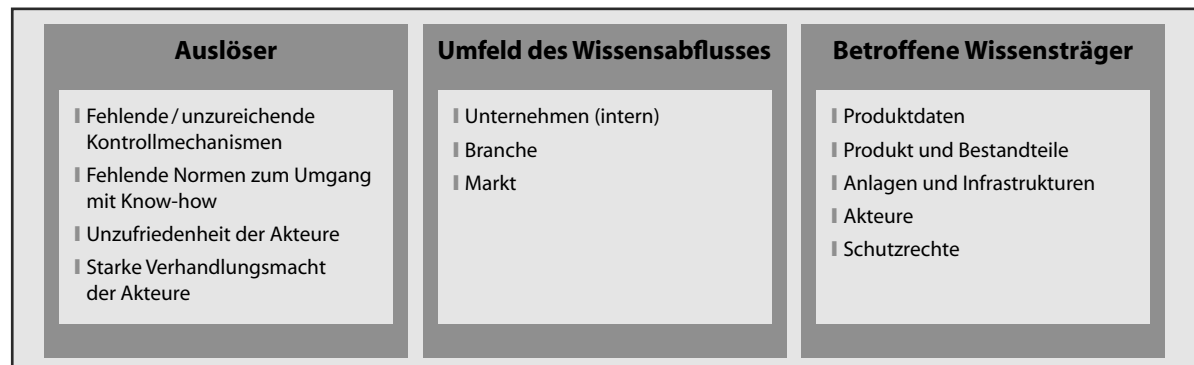


Abb. 2.10: Determinanten des Wissensabflusses



2.8 Überführung der Methodik in eine Software

Das Risikomanagement-Modell wurde in drei Schritten in ein IT-gestütztes Instrument umgesetzt. Dazu sind die Daten systematisch aufbereitet und in einer Software implementiert worden.

Die systematische Aufbereitung der Unternehmensdaten stellt die erste Phase des Risikomanagement-Modells dar. In dieser werden die Daten zur Beschreibung der Situation gesammelt, erfasst und aufbereitet. Ziel dieser Phase ist die systematische Erfassung der relevanten, unternehmensspezifischen Risikosituation, sodass eine IT-gestützte Repräsentation des Wissens möglich ist.

Die Risikosituation eines Unternehmens wird anhand der Faktoren Produktpiraterierisiken, Ursachen, Maßnahmen, Unternehmensprozesse, Wissensträger, Akteure und Produkt sowie deren Beziehungen zueinander abgebildet.

2.8.1 Einstieg in die Software über einen Fragebogen

Die Ermittlung der spezifischen Risikosituation erfolgt über einen Fragebogen. Der Fragebogen ermöglicht den Einstieg in die Methodik des IT-gestützten Instruments. Adressat des Fragebogens sind Entscheidungsträger im Unternehmen. Insbesondere sollten Experte aus der Unternehmensführung, aus Forschung & Entwicklung, aus Vertrieb und aus der Konstruktion befragt werden, da vor allem in diesen Unternehmensbereichen sensible Informationen vorliegen. Abbildung 2.12 zeigt einen Ausschnitt der Microsoft-Excel-basierten Benutzeroberfläche des IT-Instruments.

Die Inhalte des Fragebogens betreffen das Thema Know-how-Sicherheit im Unternehmen. Deshalb werden die Frageninhalte wie folgt gegliedert:

- Wissensträgerkategorien
- Produkt mit seinen Bestandteilen

Abb. 2.12: Screenshot der Benutzeroberfläche des IT-gestützten Risikomodells

Fragenkatalog Risikocheck

Ermöglicht die Identifizierung der Schutzlücken Ihres Unternehmens und die Ermittlung des Risikogefährdungspotenzials Ihres Unternehmens.

Thema 1: Betroffene Geschäftsprozesse

1 Welche **Geschäftsprozesse** gibt es in Ihrem Unternehmen (intern oder extern ausgelagert)?

<input checked="" type="checkbox"/>	Entwicklung
<input checked="" type="checkbox"/>	Produktionsplanung
<input checked="" type="checkbox"/>	Beschaffung
<input checked="" type="checkbox"/>	Produktion
<input checked="" type="checkbox"/>	Vertrieb
<input checked="" type="checkbox"/>	After Sales
<input checked="" type="checkbox"/>	Entsorgung

2 Welche von diesen Geschäftsprozesse sind **outsourced** (komplett oder teilweise)?

	Outsourced	Nicht outsourced	kann ich nicht bea
Entwicklung	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Produktionsplanung	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Beschaffung	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Produktion	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Vertrieb	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Produktpirateriebewertung 3.2.0 vom 02.09.2010

Herzlich willkommen zum Bewertung des Piraterierisikos

mit prooriginal.procom.de verbinden

mit localhost:8080 verbinden

Bewertungsfall

Risikocheck

Plagiatfall

Plagiatfallbewertung

Risikocheck Ergebnisse Plagiatverfolgung Konfiguration

- Produkt in seiner Wertschöpfungskette
- Produktionsanlagen
- Infrastruktur
- Akteure
- Rechtliche Absicherung

Im Fragebogen sind sowohl geschlossene als auch offene Fragen hinterlegt. Für geschlossene Fragen sind für den vorliegenden Anwendungsfall die Nominal-, die Ordinal- und die Likert-Skalierung sinnvoll (s. u., vgl. Homburg und Krohmer 2009). Zweck der Fragen ist, zu erkennen, welche Wissensträger im Unternehmen vorhanden sind und ob diese gegen Produktpiraterie im Unternehmen geschützt sind. Die erstellten Fragen verlangen bei der Beantwortung eine subjektive Bewertung. Daher wird die Likert-Skalierung angewendet. Die benutzte Skalierung hat als Auswahlmöglichkeiten „ja“, „komplett“, „überwiegend“, „eher weniger“, „nein“ und „kann ich nicht beantworten“. Offene Fragen spielen nur eine informative Rolle und werden zur Erfassung neuer Wissensträger verwendet. Ein Ausschnitt des Fragebogens ist in Abbildung 2.13 dargestellt, der vollständige Fragebogen steht auf der

Website des Centrums für Angewandte Methoden gegen Produktpiraterie (www.camp.tu-darmstadt.de) als Download zur Verfügung.

Die Umsetzung der Methodik setzt eine formale und maschinenlesbare Darstellung des Wissens über Produktpiraterie voraus, was mithilfe von Ontologien realisiert werden kann. Zur IT-gestützten Modellierung der Ontologie ist die Software Protégé geeignet. Dabei handelt es sich um ein kostenloses Open-Source-Java-Tool, das eine erweiterbare Architektur für die Erstellung von kundenspezifischen, wissensbasierten Anwendungen bietet.

2.8.2 Abbildung von Risikobeziehungen durch eine Ontologie

Die Produktpiraterie- und die Unternehmensfaktoren, sowie ihre Beziehungen miteinander werden in eine Ontologie modelliert, wie in Abbildung 2.14 dargestellt.

In dieser Ontologie sind Klassen für die Faktoren Produktpiraterierisiken, Globale Risiken, Prozesse und

Abb. 2.13: Strukturierung des Fragebogens

3.3 Sind die folgenden Qualitätsprüfungsdaten gegen unbefugten Zugriff in Ihrem Unternehmen geschützt ?						
	Ja, ... es existieren Kontrollmaßnahmen zum Schutz dieser Daten, wie z.B.: - Berechtigungsstufen für den Zugriff auf diese Informationen. - Verschlüsselung dieser Daten. - IT-Sicherheitsmaßnahmen, bspw. "Digital Rights Management". - regelmäßige Änderungen ihres Passworts für die computerunterstützten Daten. - es gibt eine Systematik, mit der Informationen im Unternehmen nach ihrer Sensibilität klassifiziert werden. - es werden keine Originaldokumente an Dritte herausgegeben.	Teilweise, ... die Daten sind z.B. nur in bestimmten Teilprozessen geschützt, nicht im gesamten Prozess.	Nein, ... es existieren keine Kontrollmaßnahmen zum Schutz dieser Daten.		Kann ich nicht beantworten, ... weil bspw. diese Daten nicht vorhanden sind.	
	komplett	überwiegend	eher weniger	gar nicht	diese Daten sind nicht vorhanden	keine Informationen vorhanden
Qualitätsvorschriften	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Prüfprotokolle	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Prüftechnologie	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
andere und zwar...	<input type="text"/>					

Prozessschritte, Ursache, Umfeld des Wissensabflusses und Gegenmaßnahmen erstellt. Die Beziehungen zwischen diesen Faktoren werden als Slots dargestellt. Zur Repräsentation der Ausprägungen der Faktoren werden Instanzen erstellt. Beispielweise kommen für die Klasse „Prozess“ die Instanzen „Entwicklung“, „Produktion“, usw. in Betracht. Auf diese Weise ist das Netzwerk von Informationen mit logischen Relationen maschinenlesbar.

Beim Ausfüllen des Fragebogens gibt der Anwender zunächst die vorhandenen Prozesse im Unternehmen ein. Aus diesen Angaben werden nur die mit diesen ausgewählten Prozessen verknüpften Informationen ausgewählt. Der Bewertungsablauf ist in Abbildung 2.15 dargestellt.

In einen nächsten Schritt wird abgefragt, welche Wissensträger in diesen Prozessen einen gewissen Schutz gegen Produktpiraterie haben. In Bezug auf

die ausgewählten Wissensträger wird ein spezifisches Risiko abgeleitet, welches sich auf ein globales Risiko bezieht. Der Anwender bewertet diese Risiken anhand der dreistufigen Skalierung „hoch“, „mittel“ und „niedrig“. Als Hilfe zur Bewertung können die dazugehörigen spezifischen Risiken abgefragt werden.

Nachdem die globalen Risiken bewertet wurden, ermittelt die Software das gesamte Gefährdungspotenzial. Als Ergebnis wird das Gefährdungspotenzial des Unternehmens mit den Ausprägungen „hoch“, „mittel“ oder „niedrig“ beschrieben. Zudem werden Listen über die ungeschützten Wissensträger, spezifische sowie globale Risiken des Unternehmens, betroffene Prozesse und Prozessschritte, mögliche Ursachen (mit dem betroffenen Umfeld) und geeignete Maßnahmen für jedes Risiko erstellt. Somit kann sich der Anwender ein Bild über die gesamthafte Risikosituation des Unternehmens bilden.

2

Abb. 2.14: Ontologie des Risikoprozessmodells

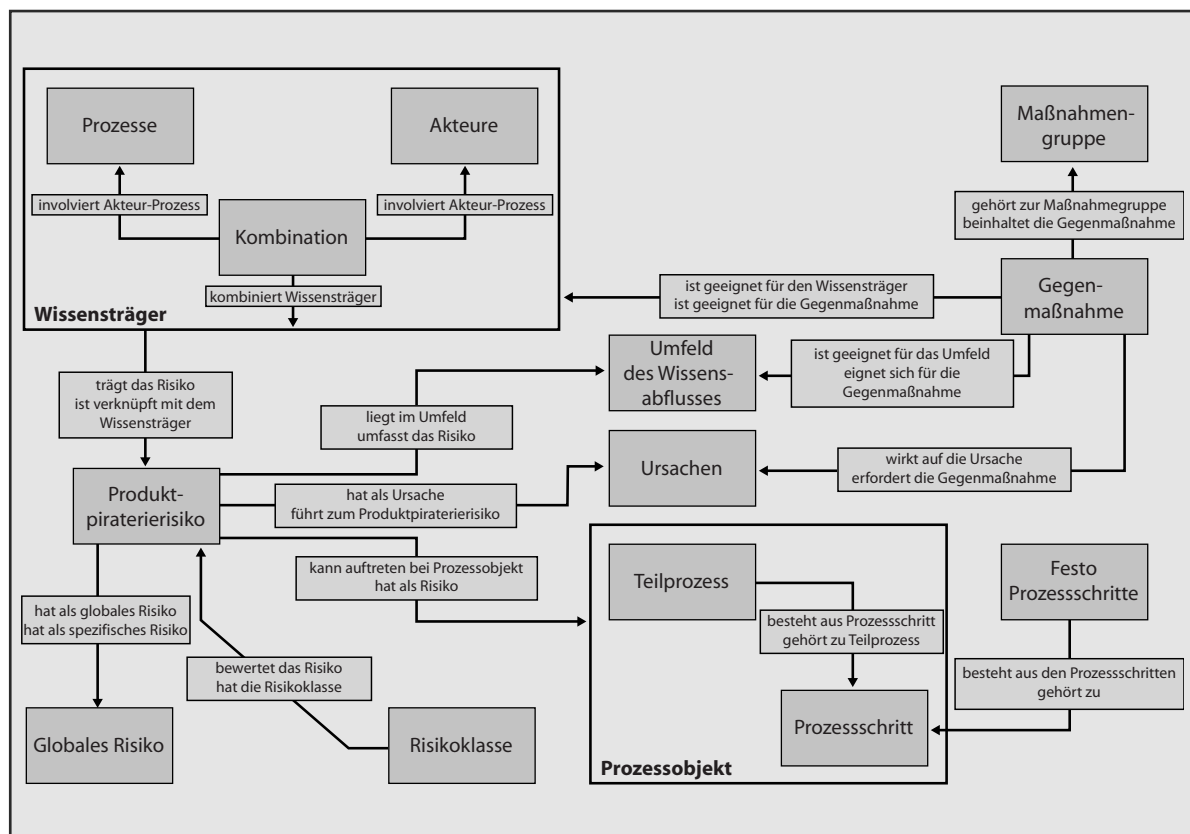
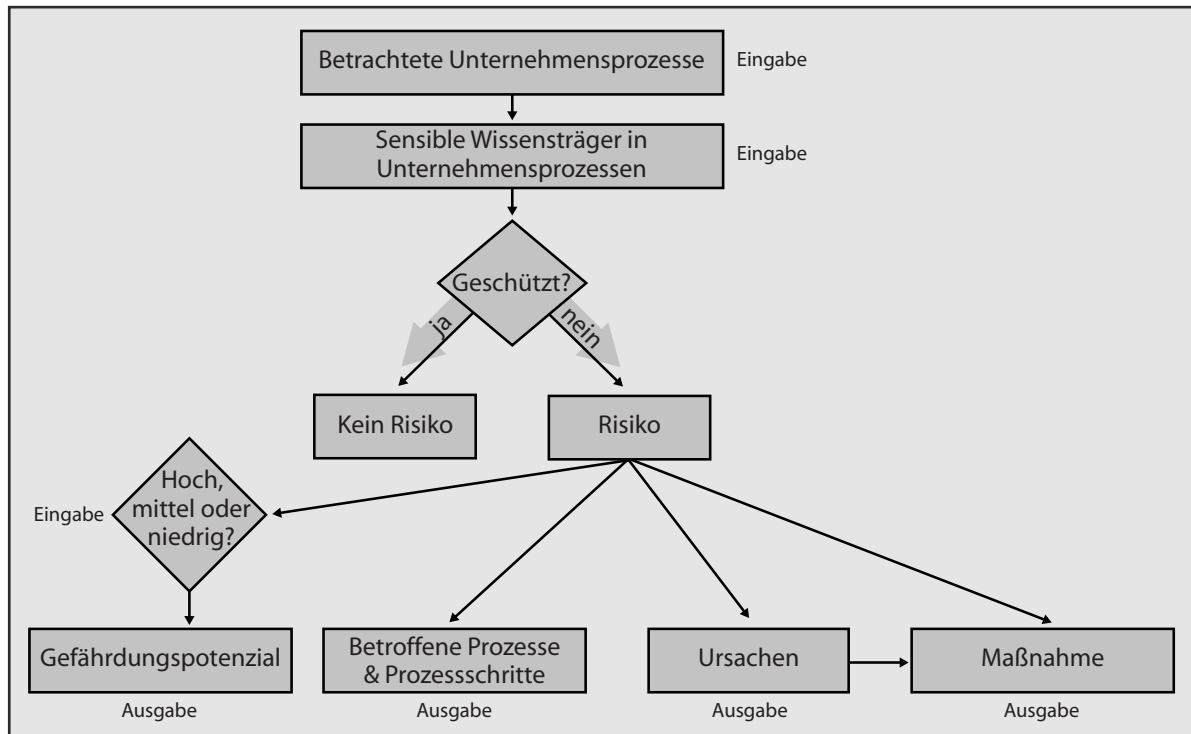


Abb. 2.15: Bewertungsablauf des Risikoprozessmodells

2.9 Anwendung des Modells im Unternehmen

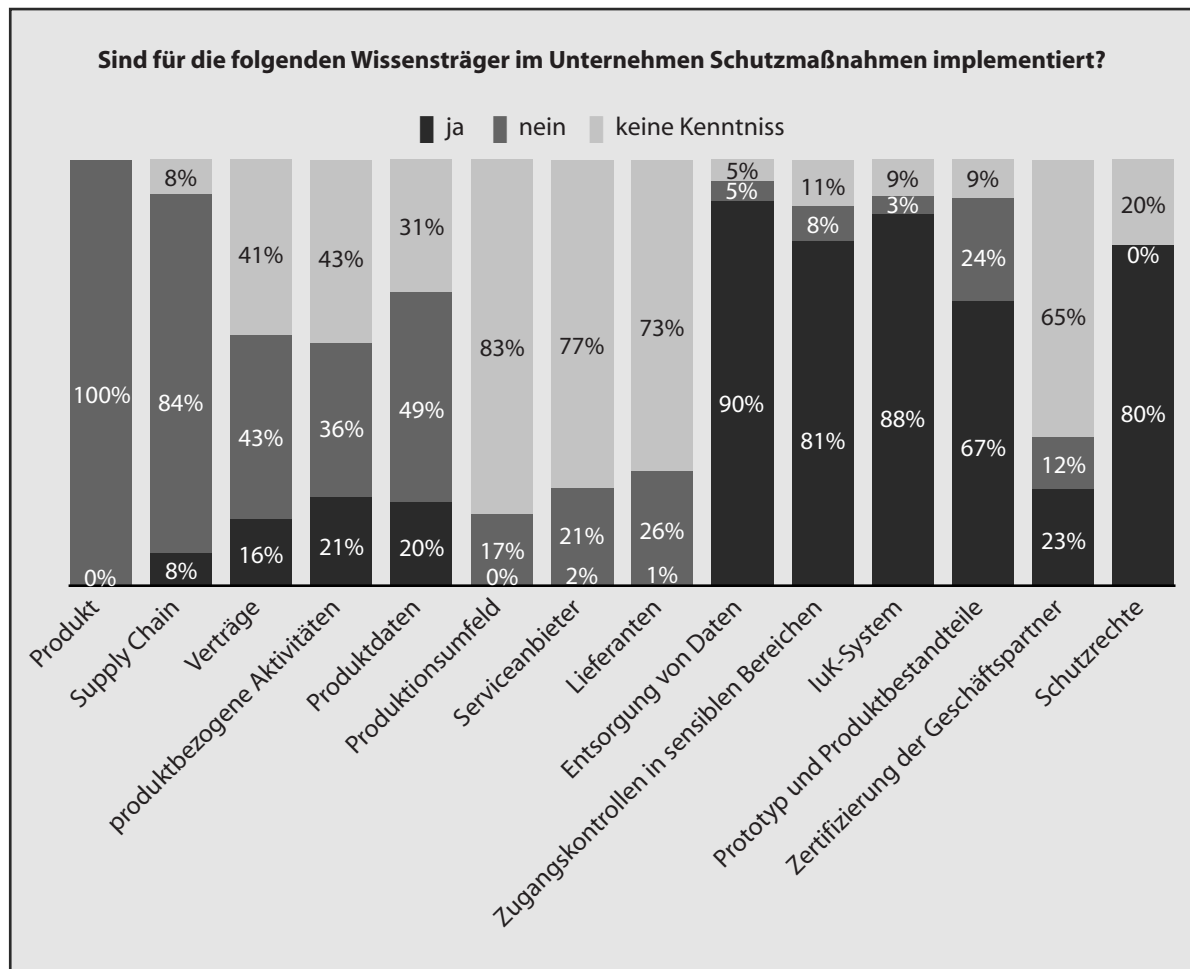
Die Anwendung der skizzierten Methodik sollte in fünf Schritten durchgeführt werden. Im ersten Schritt werden die Experten ausgewählt. Die Auswahl der Experten spielt eine wichtige Rolle, da von diesen maßgeblich die Qualität der Ergebnisse abhängt. Da Führungskräfte umfangreiches Wissen über die Prozesse im Unternehmen besitzen, sind sie gute Kandidaten für das Ausfüllen des Fragebogens. Praxisfälle haben gezeigt, dass es sinnvoll ist, jeweils einen Experten aus den Bereichen Entwicklung, Patentwesen (Intellectual Property), Marketing, Vertrieb und Produktmanagement auszuwählen. Mit diesen Experten sollten die Interviews anhand des

Fragebogens durchgeführt werden. Wichtig ist es, den befragten Experten die Ergebnisse der Risikoermittlung darzulegen und diese mit ihnen zu besprechen. Der Ablauf ist in Abbildung 2.16 dargestellt.

Die Befragten benötigen zwischen 30 und 45 Minuten zum Ausfüllen des Fragebogens. Innerhalb kürzester Zeit (je nach Anzahl der Experten in weniger als einem Manntag) ist das Unternehmen somit in der Lage, eine umfassende Bestandsaufnahme über das Schutzniveau und die Risikosituation des Unternehmens durchzuführen. Die wichtigsten Handlungsfelder werden dabei ermittelt und gleichzeitig die Ursachen der identifizierten Risiken sowie mögliche Gegenmaßnahmen ausgegeben.

Abb. 2.16: Prozessschritte der Risikobewertung im Unternehmen

Abb. 2.17: Ergebnisse der Bewertung der Wissensträger im Unternehmen (beispielhaft)



2.9.1 Modellergebnisse

Das Modell gibt entsprechend den Antworten Schutzlücken aus. Abbildung 2.17 zeigt exemplarisch die Ergebnisse einer Risikoanalyse, bei der nach der Existenz von Schutzmaßnahmen bei verschiedenen Wissensträgern und Prozessen gefragt wurde. Erkennbar ist, an welchen Stellen bereits Schutzmaßnahmen implementiert sind, welche Aspekte noch nicht geschützt sind und wo noch Ungewissheit herrscht.

Anhand der Abbildung wird deutlich, dass einige Wissensträger nicht geschützt sind, es fehlen also z. B. Kontrollmechanismen. Ebenfalls als kritisch anzusehen sind aber die Wissensträger, bei denen im Unternehmen keine Kenntnis darüber existiert, ob Schutzmaßnahmen vorhan-

den sind. Dies deutet entweder auf fehlende Normen zum Umgang mit Know-how hin oder es ist ebenfalls als fehlender Schutzmechanismus zu werten. In gleicher Weise, wie in obiger Abbildung dargestellt, werden die Ergebnisse für alle Wissensträger und Akteure ausgegeben und somit die wichtigsten Handlungsfelder ermittelt.

Zusätzlich werden aber auch konkrete Risiken durch das Modell ausgegeben, die entsprechend spezifiziert sind. Die Prozessschritte, in denen die identifizierten Risiken auftreten, sind ebenfalls dargestellt. Die Maßnahmen mit detaillierten Beschreibungen sind den identifizierten Ursachen zugeordnet und bekämpfen somit nicht die Symptome, sondern gehen das Problem an der Wurzel an. Abbildung 2.18 gibt einen Überblick über das Ergebnisfenster.

Abb. 2.18: Screenshot des Ergebnisfensters der Risikobewertungssoftware

2	Risikoliste	<ul style="list-style-type: none"> Rechtsdurchsetzung im betroffenen Land unsicher Externe Partner agiert in kritischen Ländern Know-How-Abfluss durch eigene Mitarbeiter Know-how-Aufbau Dritter Externe Partner nutzt selbst Wissen Externe Partner ist korrupt Externe Partner veräußert Wissen an Dritte Einbringen von Grauware in die Wertschöpfungskette Produkt ist in der Wertschöpfungskette nicht sich Produkt ist einfach nachzubauen Der Kunde ist korrupt Informationsabfluss aus Produktdaten Informationsabfluss über Detailwissen / Preiswissen Informationsabfluss aus Informations- und Kon 	<ul style="list-style-type: none"> Maßnahmenliste Vermeidung von Know-How-Abfluss durch eigene Reduzierte Information an externe Partner Informationsmanagement mit Blick auf Produktpir Zugriffsrechte Verbesserung der IT-Sicherheit Datenschutz Kundenbindung Marktab Sicherung Maßnahmen gegen Reverse Engineering Maßnahme der Prozesstechnologie Zeitlicher Vorsprung Produktauthentifizierung mit Information Verdeckte Produktauthentifizierung Offene Produktauthentifizierung 	Maßnahmenliste
	Prozessliste	<ul style="list-style-type: none"> Entsorgung After Sales Vertrieb Produktion Beschaffung Produktionsplanung Entwicklung 	<ul style="list-style-type: none"> Ursachenliste Fehlende Normen zum Umgang mit Know-how In Unzufriedenheit der Akteure Intern Fehlende Kontrollmechanismen Intern keine Hauptursache Branche Starke Verhandlungsposition der betroffenen Al Unzufriedenheit der Akteure Markt Fehlende Kontrollmechanismen Branche Fehlende Normen zum Umgang mit Know-how Bi 	Ursachenliste

2.9.2 Risikobewertung

Die anschließende Risikobewertung erfolgt in zwei Stufen. Zunächst wird eine unternehmensindividuelle Risikobewertung durchgeführt. Anschließend wird das Gefährdungspotenzial (GP_i) im Unternehmen ermittelt.

Abb. 2.19: Formel zur Ermittlung des Gefährdungspotenzials GP_i

$$GP_i = \frac{1}{n} \sum_{i=1}^n r_i = \frac{r_1 + r_2 + \dots + r_n}{n}$$

Die Bewertung der Risiken und des Gefährdungspotenzials wird wie folgt realisiert: Jedes ermittelte Risiko r_i (mit $i=1 \dots n$) wird qualitativ mit einer dreistufigen Skala (hoch=3, mittel=2 und niedrig=1) durch den Anwender bewertet.

Der Wert jedes ausgewählten Risikos wird addiert, um als Ergebnis das arithmetische Mittel nach der in Abbildung 2.19 gezeigten Formel zu berechnen. Dieses Ergebnis stellt das Gefährdungspotenzial GP_i dar. Der Wert des Gefährdungspotenzials wird gerundet, um eine Bewertung in der dreistufigen Skala (hoch=3, mittel=2, niedrig=1) zu erhalten. Auf diese Weise kann ein Wert über die Risikosituation des Unternehmens ermittelt werden.

Schutz vor Produktpiraterie

Ein Handbuch für den Maschinen- und Anlagenbau

Abele, E.; Kuske, P.; Lang, H.

2011, XII, 160 S. 138 Abb., 17 Abb. in Farbe., Hardcover

ISBN: 978-3-642-19279-1