HANSER

Leseprobe

Handbuch Produktentwicklung

Herausgegeben von Udo Lindemann

ISBN (Buch): 978-3-446-44518-5

ISBN (E-Book): 978-3-446-44581-9

Weitere Informationen oder Bestellungen unter

http://www.hanser-fachbuch.de/978-3-446-44518-5

sowie im Buchhandel.

Anbieter	Recherchemöglichkeiten	Adresse
DEPATISnet	Nationale deutsche Datenbank Patente/Marken/Muster, 60 Millionen Patente, Suche auf Deutsch und Englisch nach Nr., IPC-Klasse, Schlagworten	www.dpma.de
espacenet	80 Millionen Patentdokumente weltweit, Suche nur mit englischen Begriffen möglich, Zugriff auf europäische Patentdatenbanken	www.espacenet.com
uspto UNITED STATES PATENT AND TRADEMARK OFFICE	US Datenbank für Marken und Patente, Suche nach Schlagwort, Bildern, Nr.	www.uspto.gov/patents
PATENTSCOPE Search International Patent Applications	Internationale Datenbank der WIPO, 30 Millionen Patente, Suche nach Schlagwort, Nr., IPC-Klasse, Begriffe in 12 Sprachen, enthält rare Patentdokumente (z.B. japanische oder russische)	https://patentscope.wipo.int
HABM	Gemeinschaftsmarkensuche des HABM	www.oami.europa.eu
FPO IP RESEARCH & COMMUNITIES	Hauptsächlich amerikanische Patente, japanische Abstracts, Fachartikel	www.freepatentsonline.com
Lens	Amerikanische, europäische und australische Patente	www.lens.org
Google Patents	Suche in Patenten (EPA ,USPTO) und anderer wissenschaftlicher Literatur, hohe Anzahl Treffer, direkte Übersetzung möglich, Funktion „Stand der Technik“ findet automatisch ähnliche Patente	https://patents.google.com
Intellogist	Linksammlung und Infos rund um die Patentsuche	http://www.intellogist.com

Bild 5.19 Auswahl von freien Patentddatenbanken

II

Patentdatenbanken

Verwendung finden kommerzielle wie auch kostenfreie Datenbanken. Während der Inhalt beider Datenbankenformen annähernd deckungsgleich ist, bieten kommerzielle Datenbanken meist komfortablere Suchmasken. Dadurch, dass die meisten freien Datenbanken an den jeweiligen Patentämtern geführt werden, sind diese meist aktueller. Als Beispiele für kommerzielle Datenbanken seien hier „PatentWeb“ von Thomson Innovation und „PatBase“ von Minesoft genannt.

5.7 Know-how-Schutz

Norbert Gronau, Gergana Vladova

5.7.1 Notwendigkeit des ganzheitlichen und präventiven Know-how-Schutzes

Aufgrund des innovativen Potenzials des Produktentwicklungsprozesses wird häufig – und in manchen Unternehmen zum ersten Mal – in diesem Zusammenhang das Thema Know-how-Schutz diskutiert. Tatsächlich ist dieses Thema jedoch allgegenwärtig und tangiert beinahe jede unternehmerische Tätigkeit. Wissen ist eine strategische Ressource von Unternehmen und wird im Wettbewerb als erfolgskritischer Faktor gesehen. Somit erweist sich die Notwendigkeit, Wissen zu schützen, als existenziell notwendig für Unternehmen. Je proaktiver und präventiver sie sich damit auseinandersetzen, desto erfolgreicher können potenzielle materielle und immaterielle Schäden vermieden werden. Hierzu bieten sich unterschiedliche Schutzkonzepte

an, die die jeweiligen unternehmensspezifischen Gegebenheiten und Risiken adressieren. Insbesondere im Hinblick auf die gegenwärtigen und künftigen technologischen Entwicklungen, die damit einhergehenden Möglichkeiten der Datenverbreitung und -übertragung sowie die rasant steigende Bedeutung der Information und des Zugriffs auf unterschiedliche Informations- und Wissensquellen, steigt die Bedeutung eines angemessenen, angepassten und proaktiven Know-how-Schutzes.

Ein wesentlicher Aspekt in diesem Kontext ist die notwendige Unterscheidung zwischen Wissen und Informationen: Informationen sind leicht explizierbar, können gespeichert, vervielfältigt und problemlos weitergegeben werden. Wissen dagegen ist immer personengebunden und kann nicht ohne Verluste übertragen werden. Der Transfer von Wissen und Information findet folglich auf unterschiedliche Weise statt und erfordert unterschiedlichen Umgang. Bei der Auswahl der Betrachtungs- und Gestaltungsschwerpunkte ihrer Schutzkonzepte sollen Unternehmen eine möglichst ganzheitliche Perspektive anstreben – der alleinige Schutz digitaler Informationen und die Absicherung der Informationstechnik sind bei weitem nicht ausreichend und nur als ein (wichtiger) Teilaspekt zu betrachten. Genauso relevant und notwendig wie die Absicherung der technischen Infrastruktur ist vor diesem Hintergrund auch die Berücksichtigung von Maßnahmen, die Personen (Mitarbeiter, Geschäftspartner) oder Prozessverläufe adressieren.

Generell streben Unternehmen mit der Wissensweitergabe einen Nutzen an. Dieser entsteht beim reibungslosen Austausch der für den Ablauf der Unternehmensprozesse erforderlichen Informationen und Wissen. Die Transferprozesse verlaufen z. B. im Rahmen von abteilungsinterner und -übergreifender Zusammenarbeit und werden von der gemeinsamen Struktur, Kultur und Organisation geprägt. Neben den positiven Aspekten der Wissensteilung sind jedoch auch mögliche negative Nebeneffekte zu berücksichtigen. Ein Beispiel dafür ist die unkontrollierte, unbedachte und unnötige Übertragung von Informationen, wie das Versenden von Emails an mehrere Empfänger, die eventuell nicht direkt von den Inhalten betroffen sind. Solche Vorkommnisse können Prozessabläufe durch unnötige Verzögerungen beeinträchtigen (s. „Information Overload“). Weiterhin entstehen als Folge von Unzulänglichkeiten im Umgang mit Informationen und Wissen echte Gefahren für das unternehmerische Know-how. Wissensabflüsse können gefährlich für ein Unternehmen sein, da zum Beispiel der Wettbewerbsvorteil aus Wissens- und Informationsvorsprung verloren geht (Risiken der Wissens- und Informationsteilung). Wesentlicher Grund für die Entstehung von unterschiedlichen negativen Wissenstransferergebnissen sind in den meisten Fällen die fehlende Risikowahrnehmung, fehlende Regeln und fehlende Sensibilisierung der Mitarbeiter (Bahrs, Vladova 2011).

Adressiert werden können diese Herausforderungen durch den gezielten und bedachten Umgang mit Wissen im Unternehmen als Managementaufgabe, wobei die auf dieser Ebene getroffenen Entscheidungen von den Mitarbeitern verstanden und gelebt werden sollten. Die strategischen und operativen Bemühungen, Wissen zu verteilen, haben, wie aufgezeigt, gleichermaßen zu berücksichtigen, dass dies nicht immer von Interesse für das Unternehmen ist. Der Know-how-Schutz ist vor diesem Hintergrund ein Teil des betrieblichen Wissensmanagements, die Motivation dahinter ist jedoch mit umgekehrten Vorzeichen zu verstehen: Anstelle von Maßnahmen zur Ermöglichung des Wissenstransfers und der Wissensteilung sollen Vorkehrungen getroffen werden, die die Wissensweitergabe eher hemmen oder zumindest in Frage stellen. Auf Grundlage des Analyse- und Konzeptionsinstrumentariums des prozessorientierten Wissensmanagements können existierende Geschäftsprozesse auf Schwächen und Stärken beim Umgang mit Wissen und Information analysiert und neue Lösungen konzipiert werden. Bei der Konzeption von unternehmensspezifischen Wissensmanagementlösungen bezüglich der strategischen Ausrichtungen sind alle relevanten Akteure aktiv in die Entscheidungen über anstehende organisatorische, prozess- und personenbezogene sowie technische Maßnahmen einzubeziehen, denn ein Wissensmanagementkonzept, das pauschal oder top-down implementiert wird, führt häufig zu Akzeptanzproblemen. Ein Erfolgsfaktor für die Konzepteinführung, der eine höhere Akzeptanz gewährleistet, ist die explizite Berücksichtigung existierender Prozesse bei der Gestaltung der Veränderungen.

Im Anschluss an die oben beschriebenen Herausforderungen erweist sich in Bezug auf den Know-how-Schutz eine Unterscheidung zwischen gewollten und ungewollten Informations- und Wissensweitergaben als notwendig. Die Unterscheidung wird auf strategischer Ebene getroffen und in die operative Ebene kommuniziert und umgesetzt. Zusätzlich finden im Unterneh-

men unbewusste (unreflektierte oder unerkannte) Informations- und Wissenstransfers statt. Im Vorfeld der Analyse sind diese transparent zu machen und bei der Konzeptentwicklung einzubeziehen.

Zusammenfassung präventiver und ganzheitlicher Know-how-Schutz

Zusammenfassend lassen sich folgende Ausgangsgrößen für den bewussten Umgang mit schützenswertem Know-how im Unternehmen ableiten: Der Know-how-Schutz soll ganzheitlich und präventiv als Teil des Wissensmanagements im Unternehmen gestaltet und an bestehende Prozesse orientiert werden. Dabei sind alle bewussten und unbewussten (formellen und informellen) Wissens- und Informationsweitergaben relevant. Die Know-how-Schutz-Strategie ist eine Managementaufgabe, die operative Durchführung betrifft jedoch alle Mitarbeiter.

Nachfolgend wird daher ein ganzheitliches prozessorientiertes Verfahren zur Konzeption von Wissenstransfermaßnahmen vorgestellt, das explizit auch Risiken der Wissensweitergabe in die Analyse und Konzeption einbezieht. Die Herausforderung ist, auf Basis der aktuell stattfindenden Wissensweitergaben, gewollte und ungewollte zu bestimmen, um fehlende hinzuzufügen und störende zu entfernen, mit dem Ziel, proaktiv die Verteilung von Wissen und Informationen zu beeinflussen. Diese in der Praxis erprobte Methode befähigt Unternehmen dazu, selbstständig ein Konzept zum Know-how-Schutz zu entwickeln und anzuwenden.

5.7.2 Mögliche Anwendungskontexte der Methode

Bevor die Methode ausführlich erklärt wird, werden nachfolgend zwei mögliche Anwendungskontexte kurz vorgestellt. Das Ziel dabei ist es, einen gedanklichen Rahmen aufzuspannen und beispielhaft aufzuzeigen, welche Situationen in der unternehmerischen Praxis eine Gefahr darstellen können und vor diesem Hintergrund eine intensive Auseinandersetzung mit der Thematik des Know-how-Schutzes erfordern.

5.7.2.1 Anwendungskontext Produktpiraterierisiko

Ein Beispiel für ein Risiko durch Wissensabfluss ist die Produktpiraterie. Das Problem der Produktpiraterie besteht weltweit und hat gravierende wirtschaftliche Auswirkungen für Unternehmen, wie direkt entgangene Umsätze, Schädigung des Images oder Haftungsklagen gegen die Originalhersteller. Auch Käufer profitieren nur scheinbar von den Plagiaten. Diese können zwar in der Regel günstiger erworben werden, dafür sind jedoch Abstriche bei den Garantien und Haftungen des Herstellers hinzunehmen. Ferner entstehen Qualitäts- und damit einhergehend Sicherheitsprobleme bis hin zu lebensbedrohlichem Ausmaß, wie Berichte von gefälschten Bremsscheiben für Autos oder Flugzeugersatzteilen zeigen. Im Mittelpunkt des Interesses der Produktpiraten stehen die fertigen Produkte des Originalherstellers, welche häufig mittels Reverse Engineering analysiert werden, deren Herstellverfahren und Märkte sowie die verfügbaren Informationen, das Know-how und die relevanten Wissensträger (z. B. Mitarbeiter) Ansatzpunkte für eine Nachahmung. Zur Erlangung des fehlenden Wissens werden frei zugängliche Informationen sowie solche, die mit Tricks und Vorwänden erlangt werden, bis hin zur Abwerbung von Mitarbeitern und Industriespionage eingesetzt (Gronau, Meier, Bahrs 2011; Gronau, Bahrs, Vladova 2012).

Es existiert bereits eine Vielzahl von präventiven und reaktiven Maßnahmen als Antwort auf die Bedrohungen und Schäden durch Produktpiraten. Präventive Schutzmaßnahmen setzen vor Eintritt eines Schadenfalls ein. Reaktive Maßnahmen finden Anwendung, wenn Imitationen bereits auf dem Markt aufgetreten sind und damit einhergehende Verluste minimiert werden sollen.

Die in der Industrie etablierten Schutzmaßnahmen werden zumeist den reaktiven Maßnahmen zugeordnet. Im Falle von fälschlich zugewiesenen Produkthaftungen sowie bei Auftreten von Patentverletzungen sind juristische Maßnahmen einzuleiten, um den resultierenden möglichen monetären Verlust sowie Imageschaden zu reduzieren.

Um bei Rechtsstreitigkeiten Originalprodukte von Fälschungen zu unterscheiden und Produkte eindeutig zu identifizieren, bieten sich technische Schutzmöglichkeiten wie Produktkennzeichnungen und Herstellernachweise an. Hierzu gehören die Identifizierung, die durch die Ausstattung von Produkten mit äußeren Merkmalen ermöglicht wird, sowie die zum besseren Schutz geeigneten Markierungstechniken wie Hologramme, Mikroschriften, Farbpigmente, 1-D und 2-D Barcodes, Farbpigmentcodes, Sicherheitsfäden und Ähnliches. Technische Schutzmöglichkeiten helfen insgesamt zwar bei der Klärung der Originalität, verhindern

jedoch die Erzeugung eines Plagiats nicht zwangsweise. Sie dienen lediglich zur Erkennung von Fälschungen, ohne die eigentliche Ursache zu bekämpfen.
Gerade im Produktentstehungsprozess ist es besonders wichtig, die Gefahr des Wissensabflusses durch menschliche oder organisationelle Schwachstellen möglichst gering zu halten, da zum Einen sie zu diesem Zeitpunkt die einzige Möglichkeit bietet, das Produkt nachzuahmen und zum Anderen eine Nachahmung während der Produktentwicklung zu enormen Verlusten in Bezug auf die eigene Wettbewerbsstellung bei gleichbleibenden Investitionen in den eigenen Innovationsprozess. Mit anderen Worten – das Unternehmen trägt die Kosten für den eigentlichen Entwicklungsprozess und besitzt das innovative Potenzial dazu, verliert jedoch durch den Wissensabfluss seine angestrebte exklusive Position bei der Markteinführung des neuen Produktes.

5.7.2.2 Anwendungskontext Open Innovation Projekt

Unter dem Begriff Open Innovation wird in der Literatur die planvolle Öffnung der Innovationsprozesse und die strategische Einbindung des Unternehmensumfelds verstanden. Diese Bestrebungen gelten als zentrale Erfolgsfaktoren für eine verbesserte Innovationsfähigkeit. Vor allem kleine und mittelständische Unternehmen sind auf den Austausch mit Externen (z. B. Kunden, Lieferanten, Forschungseinrichtungen) angewiesen, um trotz ihres inhärenten Ressourcenmangels Wissen über Technologien und Märkte zu generieren und in Innovationen zu übertragen.
Bei gezielten Kooperationen mit externen Akteuren, insbesondere im Rahmen von Open Innovation-Projekten gilt es, die bereits thematisierten Risiken des Know-how-Abflusses und die Wichtigkeit relevanter Schutzmaßnahmen ebenso gestärkt in Betracht zu ziehen. Durch die Teilnahme an einem Open Innovation-Vorhaben sind Unternehmen in Bezug auf den ungewollten Wissensabfluss in der Regel angreifbar für feindliche Absichten. Gleichzeitig erwarten diese – im Unterschied zum Produktpiraterievorfall – positive Synergieeffekte bei dem Austausch mit Externen und sind dementsprechend unter Umständen geneigt, zu viel unternehmerisches Know-how im Rahmen der Zusammenarbeit preiszugeben.
Die Beteiligung an einem Open Innovation-Vorhaben gewährt Unternehmen in der Regel einen tieferen Blick in das schützenswerte Wissen der anderen Partner als eine normale Kooperation. Je intensiver der Open Innovation-Ansatz gelebt wird, desto mehr Wissen und Informationen tauschen Unternehmen innerhalb der unterschiedlichen Prozessphasen aus. Darüber hinaus wächst das Risiko einer Produktimitation mit der Anzahl der Projektpartner. Mit anderen Worten stehen die Breite und Tiefe des OI-Vorhabens in einer direkten positiven Korrelation zu dem Risiko der Produktimitation. Dieses Risiko des ungewollten Wissensabflusses steigt umso mehr, je ähnlicher die Produkt- oder Prozessportfolios sind. Die Gefahr, dass eigene Produkte nachgeahmt werden, besteht im Verlauf des gesamten Open Innovation-Prozesses. Besonders gefährdet sind Unternehmen bei Kooperationen mit industriellen Partnern, d. h. B2B-Kunden sowie Lieferanten, das Risiko besteht jedoch bei der OI-Zusammenarbeit mit Kunden und jeglichen Stakeholdern.

Zusammenfassung Anwendungskontexte
Beide Anwendungskontexte stellen jeweils ein Beispiel für Situationen in der unternehmerischen Praxis vor, bei denen gewollte und ungewollte Wissensabflüsse und -transferprozesse besonders kritisch angesehen werden müssen. Das Unternehmen sollte vor diesem Hintergrund in der Lage ist, seine eigenen Stärken und Schwächen einzuschätzen und generell oder auf das Projektvorhaben orientiert, eine Chance-Risiko-Analyse durchzuführen.

5.7.3 Methodisches Vorgehen zur Gewährleistung des Know-how-Schutzes

Bevor das ganzheitliche prozessorientierte Verfahren zur Konzeption von Wissenstransfermaßnahmen mit seinen einzelnen Phasen ausführlich vorgestellt wird, wird kurz auf das Ziel seiner Anwendung eingegangen – das Einrichten einer unternehmensspezifischen Knowledge Firewall.
Eine Knowledge Firewall ist ein Schutzkonzept, mit dem Unternehmen ihr Know-how gegen ungewollte Zugriffe, Verbreitung und Weiterleitung schützen können. Sie bietet einen umfassenden Schutz, der über Abteilungs- und Informationssystemgrenzen hinweg technische, organisatorische und räumliche Elemente integriert. Sie ist das Ergebnis einer Informations- und Wissensschnittstellenanalyse, bei welcher das schützenswerte Know-how einer Organisation, die Zugriffs-

punkte und die jeweils ergriffenen und fehlenden Schutzkonzepte ermittelt werden. Die Vorteile einer Knowledge Firewall können wie folgend zusammengefasst werden:

- Gewährleistung der Transparenz der Wissens- und Informationsflüsse
- Risikoklassifikation des Know-hows
- Einschätzung der Piraterieneigung der Akteure
- Einschätzung bestehender Schutzkonzepte im Unternehmen
- Entwicklung eines Maßnahmen- und Schutzkonzepts

5.7.3.1 Methode zur Identifizierung, Modellierung und Gestaltung von Informations- und Wissensschnittstellen (IWS-Analyse)

Die IWS-Analyse wurde am Lehrstuhl für Wirtschaftsinformatik und Electronic Government der Universität Potsdam entwickelt und hat als Ziel die Identifikation kritischer Informationen, kritischen Wissens sowie beteiligter Akteure in einem Wissenstransferprozess (vgl. zur Methodenbeschreibung Bahrs, Vladova 2011; Gronau, Meier, Bahrs 2011; Gronau, Bahrs, Vladova 2012). Dadurch wird die Menge der einseitigen Informations- und Wissensweitergaben zwischen zwei Gruppen mit unterschiedlichem Vertrauensgrad dargestellt. Informations- und Wissensflüsse werden direkt an den entsprechenden Schnittstellen analysiert und bewertet.

Die Anwendung der Methode ist durch das Vorgehensmodell in Bild 5.20 dargestellt. Die einzelnen Schritte der Anwendung werden nachfolgend vorgestellt und methodisch erläutert. Die Analyse erfolgt dabei ausgehend von einem Unternehmen, das sich gegen Produktpiraterie schützen möchte. Mitarbeiter dieses Unternehmens werden als interne Akteure bezeichnet. Externe Akteure werden durch das zu analysierende Unternehmen beurteilt und aufgrund der fehlenden Glaubwürdigkeit bei einer Piraterieabsicht nicht befragt.

Bei der Durchführung eines Projektes zur Schnittstellengestaltung im Unternehmen werden zuerst ein Intellectual Property Manager, welcher hauptverantwortlich für das Projekt ist, sowie jeweils der Leiter und Vertreter aller Fachabteilungen, welche an den verschiedenen Phasen beteiligt sind, bestimmt. Der Intellectual Property Manager ist an allen Schritten im Vorgehensmodell beteiligt und ihm obliegt die Projektkoordination. Die operativ tätigen Vertreter aus den Fachabteilungen sind für die Projektdurchführung vor allem in der Erhebungs- und Bewertungsphase wichtig. Ziel ist es, ein möglichst genaues und umfassendes Abbild der Realität zu erreichen. Die Leitungsebene der jeweiligen Fachabteilungen ist vor allem bei der Bewertung und Umsetzung der Maßnahmen relevant. Ihr obliegt in der Regel auch die Gestaltung der operativen Umsetzung nach Abschluss der Konzeption.

Schritt 1: Identifikation von Informations- und Wissensschnittstellen

Ziel vom Schritt 1 ist es, bei dem zu analysierenden Unternehmen die Schnittstellen zwischen Gruppen mit unterschiedlichem Know-how oder unterschiedlichem Vertrauensgrad, an denen Informationen oder Wissen ausgetauscht wird, zu identifizieren. Dazu werden zunächst interne Akteursgruppen durch eine Sekundäranalyse von Organigrammen und Prozessbeschreibung sowie einer ergänzenden Befragung (Primäranalyse) ermittelt. Die Erfassung erfolgt im Akteursmodell, welches sukzessiv in späteren Phasen erweitert werden

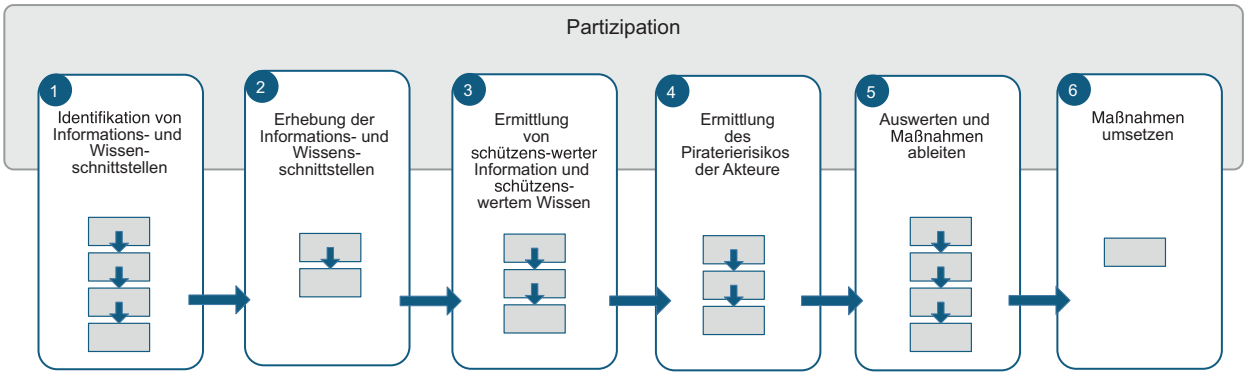

Bild 5.20 Vorgehensmodell zur Schnittstellengestaltung

kann. Ein weiteres Hilfsmittel zur Sicherstellung der Vollständigkeit ist die Nutzung einer integrierten Checkliste der Informations- und Wissensschnittstellenempfänger.

Schritt 2: Erhebung der Informations- und Wissensschnittstellen

Das Ziel dieses Schrittes ist die inhaltliche Erhebung und Dokumentation der Informations- und Wissensschnittstellen, die zuvor identifiziert wurden.

Die Erhebung erfolgt ausgehend von den Akteuren des zu analysierenden Unternehmens. Dabei werden die zwei nachfolgenden Leitfragen für jeden Akteur durchlaufen, der Informationen und Wissen für andere interne oder externe Akteure zur Verfügung stellt. Nach und nach werden so die Modelle der Informations- und Wissensschnittstellen angelegt. Standardmäßig werden externe Akteure durch das zu analysierende Unternehmen beurteilt und nicht direkt befragt, da von einem potenziellen Piraten keine wahrheitsgemäßen Antworten zu erwarten sind.

Befragt werden sollten Personen, die der Akteursgruppe zugehören. Bei der Modellierung von Akteuren auf Abteilungsebene hat sich eine Befragungszeit von 60–90 Minuten als ausreichend erwiesen. Folgende Leitfragen führen durch das Interview je Akteur:

1. Welche Information/welches Wissen in Ihrem Bereich halten Sie für besonders schützenswert?
2. Welche Information/welches Wissen ist bei welcher Aktivität für andere zugänglich?

In der Praxis hat sich ein kombiniertes Durchlaufen von Aktivitäten des befragten Akteurs und Empfängern, mit denen der befragte Akteur eine Austauschbeziehung pflegt, als sinnvoll erwiesen.

Durch die zusätzliche Betrachtung der Schnittstellen im Lebenszyklus kann die Vollständigkeit der Erhebung verbessert werden, da die bisherigen Fragen vor allem auf die gewöhnliche Geschäftstätigkeit abzielen. Ggf. existieren jedoch bei der Initialisierung oder Terminierung einer solchen Informations- und Wissensaustauschbeziehung besondere Abläufe, die ebenfalls zu erfassen sind.

Zur Dokumentation wird die Aktivitätssicht der Modellierungssprache „Knowledge Modeling and Description Language“ (KMDL) genutzt. Im Selbstanalysewerkzeug „Knowledge Firewall Designer“ (s. Kap. II-5.7.4) ist eine entsprechende Modellierungsumgebung integriert. Die Modellierung erfolgt je Aktivität, wie beispielsweise „Anfordern eines Angebotes“. Diese wird um die Akteure auf der Senderseite (in der Regel der Interviewpartner) und der Empfängerseite sowie durch die weitergegebenen Informations- und Wissensobjekte erweitert.

Das Schema der Modellierung ist in Bild 5.21 dargestellt. Zu jeder existierenden IWS wird ein Modell erstellt, um dadurch eine genauere Spezifikation der Schnittstellen zwischen Unternehmensteilen sowie innerhalb von Wertschöpfungsnetzwerken zu erreichen. Die Schnittstellen können den Aufgaben eines Prozesses zugeordnet werden.

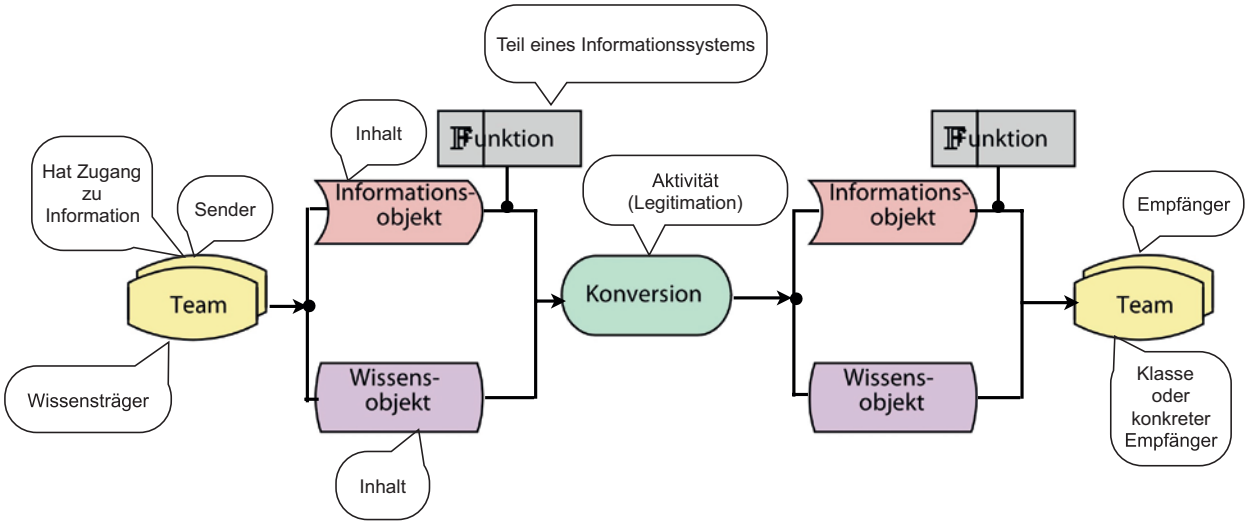

Bild 5.21 Grundmodell einer Aktivität im Wissensnetz

II

Schritt 3: Ermittlung vom Schutzbedarf und Risiken

Ziel dieses Schrittes ist die systematische Bewertung von Informationen und Wissen in Bezug auf das Risikopotenzial durch Produktpiraterie. Dieses Risiko wird als Kritizität bezeichnet. Die Bewertung erfolgt durch das Beantworten von geschlossenen und objektbezogenen Bewertungsfragen. Mittels Likert-Skala wird dabei die Zustimmung bzw. Ablehnung in fünf Stufen abgefragt. Dies erfolgt im Selbstanalysewerkzeug „Knowledge Firewall Designer“ (s. Kap. II-5.7.4) für jedes zuvor modellierte Informations- und Wissensobjekt. Im Funktionsbereich Bewertung ist der Bewertungsstatus jedes Objektes durch eine Ampel gekennzeichnet (rot = noch nicht bewertet, gelb = Bewertung begonnen aber unvollständig, grün = Bewertung vollständig).

Die Kritizität setzt sich aus den Risikofaktoren Kern-Know-how, Einmaligkeit und Nachahmungsrelevanz zusammen. Der Faktor „Kern-Know-how“ erfasst, ob es sich um wesentliches, für die betriebliche Leistungserstellung erforderliches Wissen handelt. Der Faktor „Einmaligkeit“ beschreibt, ob das Wissen auch aus anderen Quellen verfügbar ist und gibt damit Auskunft über die Notwendigkeit des Schutzes. Der Faktor „Nachahmungsrelevanz“ deckt mögliche Angriffspunkte von Piraten durch das jeweilige Know-how auf. Zu jedem Risikofaktor bestehen eine Reihe spezifischer Bewertungsfragen.

Bild 5.22 zeigt den schematischen Aufbau der Bewertung für die Zielgröße Kritizität. Im Selbstanalysewerkzeug werden direkt die Fragebogen-Items beantwortet. Ein weiterer methodischer Schritt ist die systematische Ermittlung der Piraterieneigung der Akteure. Die Bewertung erfolgt durch das Beantworten von strukturierten und objektbezogenen Bewertungsfragen im Selbstanalysetool. Auch hier erfolgt die Bewertung fünfstufig für jeden zuvor modellierten Akteur. Betrachtet werden die Voraussetzungen und Möglichkeiten der Akteure, von Produktpiraterie zu profitieren, die Vorgeschichte der Beziehung zu diesem Akteur sowie die Vernetzung zu typischen Produktionsstätten von Plagiaten sowie andere Faktoren. Zusätzliche Einflussfaktoren gelten für eigene Mitarbeiter (interne Akteure). Insbesondere Experten und Personen mit Schlüssel-Know-how müssen identifiziert und langfristig an das Unternehmen gebunden werden.

Bild 5.23 zeigt den schematischen Aufbau der Bewertung für die Zielgröße Piraterieneigung. Die Fragebogen-Items werden direkt im Selbstanalysewerkzeug beantwortet.

Der dritte Schwerpunkt der Analyse und Bewertung ist die systematische Überprüfung der vorhandenen

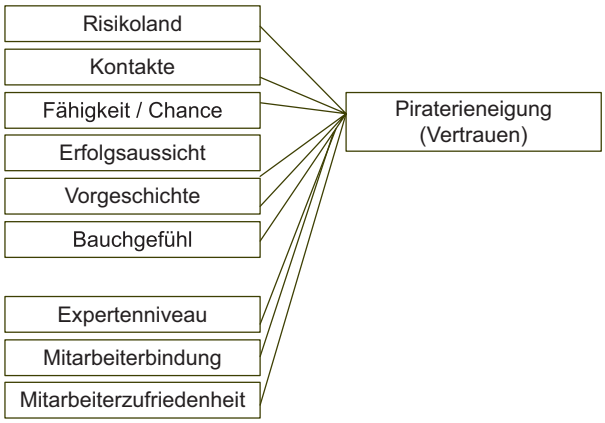

Bild 5.23 Schematischer Aufbau der Bewertung der Piraterieneigung

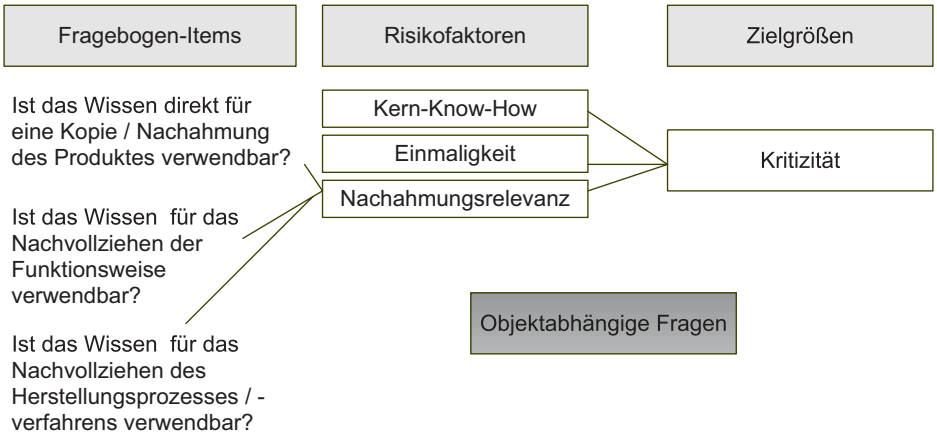

Bild 5.22
Schema der Kritizitätsbewertung

Schutzmaßnahmen gegen Produktpiraterie. Dies erfolgt entlang der modellierten Informations- und Wissensweitergaben und erreicht dadurch gegenüber pauschalen Checklisten einen hohen Detaillierungsgrad. Die Bewertung erfolgt durch die Beantwortung von objektbezogenen Bewertungsfragen. Auf der Likert-Skala wird dabei die Zustimmung/Ablehnung in fünf Stufen für jedes Informations- und Wissensobjekt sowie für Empfänger von Information und Wissen angegeben. Die bestehenden Schutzkonzepte werden überprüft durch Fragen: zum Zugriffsschutz gegenüber Dritten, zur Kopierbarkeit der Information bzw. des Wissens, zur Nachvollziehbarkeit des Wissenstransfers und zu vorhandenen Instrumenten wie Background Checks, Geheimhaltungsvereinbarungen, bereits erkannte Ereignisse der Vergangenheit, Sensibilisierung der Akteure und Nutzung öffentlicher Netzwerke.
Bild 5.24 zeigt den schematischen Aufbau der Bewertung für die Zielgröße Schutzkonzepte.

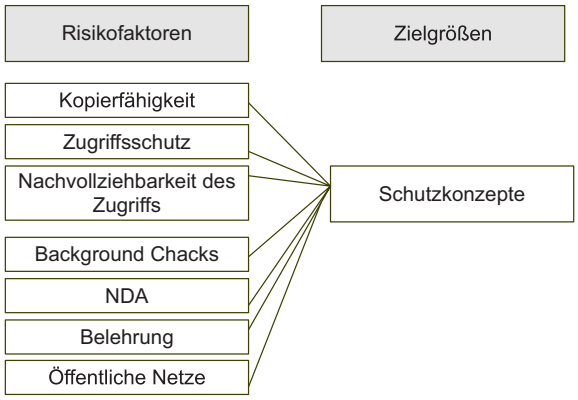

Bild 5.24 Schematischer Aufbau der Überprüfung der Schutzmaßnahmen

Schritt 4: Auswertung und Maßnahmen ableiten

Das Ziel dieses Schrittes ist es, risikoreiche Informations- und Wissensschnittstellen zu identifizieren. Dazu werden die vorherigen Einzelbewertungen zu einem Gesamtbild verdichtet und besonders risikoreiche Schnittstellen ermittelt.
Das Selbstanalysewerkzeug „Knowledge Firewall Designer“ bietet dazu verschiedene Auswertungsformen an: Reports, Risikoportfolio und die Proximitätsanalyse.

- Durch die Proximitätsanalyse werden die Inhalte in Kritizitätsgruppen geordnet und dargestellt, welche Akteure bzw. Akteursgruppen Zugang haben. Die Darstellung kann durch Anklicken von Akteuren verfeinert werden (Drill Down). Die Darstellung dient als Grundlage zur Planung des Zugangs sowie der notwendigen Schutzkonzepte für die Inhaltsarten. Dabei können den einzelnen Akteuren Risikoklassen zugewiesen werden.

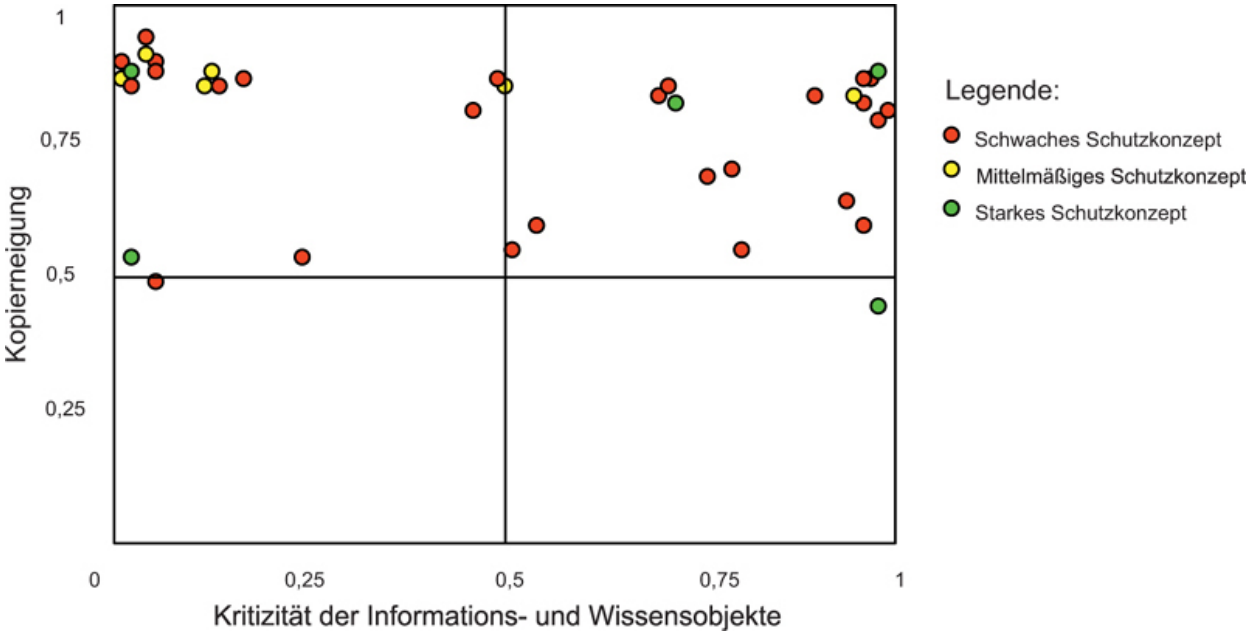

Bild 5.25 Risikoportfolio der Informations- und Wissensschnittstellen

- Reports zeigen besonders schützenswertes Know-how oder Akteure mit hoher Piraterieneigung auf.
- Das Risikoportfolio fasst die Perspektiven Kritizität, Kopierneigung und existierende Schutzkonzepte in einer Auswertung zusammen. Es ordnet die Informations- und Wissensobjekte auf der X-Achse nach Kritizität. Der Y-Wert bestimmt sich aus dem Akteur mit der höchsten Piraterieneigung, der Zugang zu dem jeweiligen Informations- oder Wissensobjekt hat. Die dritte Dimension wird durch die Farbe der Datenpunkte bestimmt. Rot steht für die Notwendigkeit eines schwachen, gelb eines mittelmäßigen und grün eines starken Schutzkonzepts. Ein beispielhaftes Piraterierisikoportfolio ist in Bild 5.25 dargestellt.

II

Das Risiko der Schnittstellen nimmt mit der Entfernung zum Ursprung zu. Entsprechend sind vor allem im Bereich rechts oben die Schnittstellen risikobehaftet.
Im Selbstanalysewerkzeug werden Beschriftungen der Datenpunkte durch Mausklick eingeblendet. Durch Reports kann eine Listdarstellung abgerufen werden.
Die Ursachenanalyse erfolgt durch eine Verfeinerung der Darstellung (Drill Down,) der im Diagramm oder in den Report aggregierten Daten. Dabei können sowohl Ergebnisse von Zwischenberechnungen bis hin zu Bewertungen einzelner Fragen abgerufen werden. So kann beispielsweise ermittelt werden, ob die Einmaligkeit eines Wissensobjektes maßgeblich für dessen Schutzwürdigkeit, oder die hohe Piraterieneigung eines Akteurs maßgeblich für das dargestellte hohe Risiko im Piraterierisikoportfolio verantwortlich ist.
Des Weiteren können Objekte aus Reports und aus Verfeinerungsansichten über die Drill Down Funktion aufgerufen werden. Die Risikoanalyse zeigt Handlungsbedarf für Schutzmaßnahmen gegen Produktpiraterie. Die Ursachenanalyse grenzt das Handlungsfeld ein.

Schritt 5: Maßnahmen umsetzen

Als Ergebnis der Analyse liegt ein Maßnahmenplan (ToDo-Liste) für jede Abteilung vor. Dieser enthält Änderungen der Schnittstellen und stellt so ein Regelwerk, das bestimmt, welche Inhalte wem gegenüber preisgegeben werden, bereit. Zusätzlich sind die zu ergreifenden Schutzmaßnahmen aufgeführt.

5.7.4 Knowledge Firewall Designer

Zur Unterstützung eines solchen Analyse- und Gestaltungsprojektes wurde parallel zur Methode der Knowledge Firewall Designer entwickelt. Dieses Werkzeug ermöglicht und erleichtert das Anlegen und Editieren des Akteurmodells, der Schnittstellenmodelle sowie die Verwaltung von Informations- und Wissensobjekten im Repository.
Darüber hinaus verfügt das Werkzeug über eine Interviewkomponente, die für die jeweiligen Bewertungssessions Bewertungsfragen dynamisch nach hinterlegten Regeln auswählt. Das Werkzeug verwaltet die Fragen, speichert die Antworten und hilft bei der Verfolgung des Interviewfortschritts.
Schließlich ist auch eine Auswertung der gesammelten Daten im Werkzeug möglich. Dabei können aus einem Katalog Maßnahmen für neue oder geänderte Schnittstellen ausgewählt werden. Das Werkzeug erstellt für jeden Akteur dementsprechend eine ToDo-Liste für die Umsetzung der Maßnahmen.
Das Tool kann kostenlos im Bereich „Tools“ auf der Homepage des Lehrstuhls für Wirtschaftsinformatik und Electronic Government der Universität Potsdam heruntergeladen werden (http://www.knowledge-firewall.de). Eine Online Anleitung steht dem Nutzer ebenso dort zur Verfügung (Gronau et al. 2012).

5.7.5 Fazit

Wenn ein Unternehmen seine Informations- und Wissensflüsse so gestalten möchte, dass sie kein Risiko mit sich bringen, dafür aber zum reibungslosen Ablauf der Prozesse beitragen, stellt sich schnell die Frage nach der Rolle jedes einzelnen internen und externen Beteiligten in Wissenstransferprozessen. Es ist nicht ausreichend, Regeln zu bestimmen oder technische Lösungen zur Verfügung zu stellen, wenn diese nicht gekannt und gelebt werden.
Für die Risikobewertung des Know-hows und der Schnittstellen wurde ein Analyseverfahren entwickelt, welches auf Basis der modellierten Objekte durch dynamisch gesteuerte Bewertungsfragen Risikofaktoren systematisch überprüft. Es werden zum Einen die Kritizität von Information und Wissen sowie zum Anderen die unternehmensspezifischen Handlungsschwerpunkte ermittelt. Zusätzlich werden im Unternehmen vorhandene Schutzmaßnahmen überprüft.
Für Unternehmen wird die Weitergabe und Verbreitung ihrer Informationen und Wissen transparent. Auf Basis der Analyse werden gezielt Maßnahmen unter Wirtschaftlichkeitsaspekten entwickelt und Umsetzungspläne für einzelne Abteilungen erstellt. Die bereit-

gestellten Maßnahmen erschweren die Informationsgewinnung für Piraten, Spione und Wettbewerber.
Die Analyse erfolgt mit einem Selbstanalysetool, das Anwender im Unternehmen durch den Analyseprozess führt und auch bei der Konzeption von Maßnahmen assistiert.
Die vorgestellte Methode dient dem präventiven Know-how-Schutz, da potenzieller Wissensabfluss bereits im Vorfeld erkannt und verhindert werden kann. Die Methode schließt eine Lücke, die in anderen Schutzkonzepten ungestaltet bleibt, und ist komplementär zum Schutz des Produktes vor Reverse Engineering. Begleitend können auch Maßnahmen ergriffen werden, die erst nach dem Auftritt des Pirateriefalls wirken, wie beispielsweise Kennzeichnung von Bauteilen und Nutzung juristischer Optionen.
Der Einsatz der Methode hat Potenziale durch den hohen Grad der Partizipation von Mitarbeitern verschiedener Fachabteilungen, ohne diese übermäßig zu belasten. Durch die Fokussierung auf die Wissens- und Informationsschnittstellen wird die Erhebung und Modellierung im Gegensatz zur klassischen Geschäftsprozessanalyse, wie sie sonst in Projekten des Prozessorientierten Wissensmanagements durchgeführt wird, schneller und einfacher. Das entwickelte Selbstanalyse-Werkzeug trägt zu dieser reduzierten Komplexität und verkürzten Durchführungszeit bei. Die Methode zeigt einen praktikablen Weg zur Erhebung und Konzeption von Wissenstransfers im Unternehmen und liefert eine notwendige Entscheidungsgrundlage. Sie beinhaltet darüber hinaus weitere Potenziale, die bisher noch nicht adressiert sind. So können zum Beispiel durch Analyse der existierenden, mit der Methode transparent gewordenen Schnittstellen und den jeweiligen Abläufen, Optimierungspotentiale ermittelt werden. Hierbei kann z. B. durch die Berücksichtigung von Szenarien, mit dem Ziel ein Gesamtoptimum zu erreichen, analysiert werden.
Als Stärke und Schwäche der Methode zugleich sind die relativen Bewertungen anzusehen. Insbesondere bei der Risikobetrachtung sowie bei der Nutzenabschätzung sind konkrete Zahlen ohnehin mit hoher Unsicherheit belegt. Die relativen Werte lassen sich leichter ermitteln, sie erschweren jedoch die Abwägung der Nutzen und Risiken. Ein Beispiel dafür ist die Entscheidung, wie die positiven Aspekte eine Verbesserung der Mitarbeiterzufriedenheit gegen die negativen Aspekte eines Piraterierisikos zu bewerten wären. In strittigen Fällen ist daher stets eine Einzelfallbetrachtung erforderlich. Zur Vergleichbarkeit der Werte trägt auch der Know-how-Schutz-Beauftragte bei. Die Methode liefert dann jedoch die notwendigen Informationen, um sowohl negative, als auch positive Aspekte einer möglichen Schnittstelle zu betrachten.

5.8 Literatur

Literatur bis Kapitel 5.6

BMBF: Patente als Informationsquelle für Innovationen. MIKUM-Bericht, Bonn 1996.

Cohausz, H., Wupper, H.: Gewerblicher Rechtsschutz und angrenzende Gebiete. 2. Auflage, Carl Heymanns Verlag, Köln 2014.

Deutsches Patent- und Markenamt: Jahresbericht 2014. Henrich Druck + Medien GmbH (Druck), Frankfurt am Main 2014.

Eisenmann, H., Jautz, U.: Grundriss Gewerblicher Rechtsschutz und Urheberrecht. 10. Auflage, C. F. Müller Verlag, Heidelberg 2015.

Götting, H.-P., Schwipps, K.: Grundlagen des Patentrechts. Teubner Verlag, Wiesbaden 2004.

Ilzhöfer, V.: Patent-, Marken- und Urheberrecht. 9. Auflage, Vahlen Verlag, München 2015.

Küffner, G.: Sicherer Stand für jeden Baum. In: Frankfurter Allgemeine Zeitung, Nr. 299, 24. Dezember 2007.

Offenburger, O.: Patent und Patentrecherche – Praxisbuch für KMU, Start-ups und Erfinder. Springer Gabler Verlag, Wiesbaden 2014.

Literatur ab Kapitel 5.7

Bahrs, J., Vladova, G.: Risiko und Nutzen von Wissensschnittstellen – Ein Gestaltungsansatz. Proceeding of the 6th Conference on Professional Knowledge Management – From Knowledge to Action. 23.2.2011, Bonn: GI.

Chesbrough, H. W.: Open Innovation: The New Imperative for Creating and Profiting from Technology, Boston 2003.

Enkel, E.; Gassmann, O.; Chesbrough, H. W.: Open R & D and open innovation: exploring the phenomenon. In: R & D Management, 39. Jg., 2009, H. 4, S. 311–316.

Fuchs, H. J.: Piraten, Fälscher und Kopierer: Strategien und Instrumente zum Schutz geistigen Eigentums in der Volksrepublik China. Gabler (Wiesbaden), 2006, S. 51.

Gronau, N., Vladova, G., Bahrs, J.: Produktpiraterie durch gezielten Umgang mit Wissen vorbeugend bekämpfen. In: WIRTSCHAFTSINFORMATIK & MANAGEMENT Ausgabe Nr. 2012-01.

Gronau, N., Meier, H., Bahrs, J. (Hrsg.): Handbuch gegen Produktpiraterie: Prävention von Produktpiraterie durch Technologie, Organisation und Wissensflussmanagement, GITO-verlag, Berlin, 2011.

Gronau, N.: Wissen prozessorientiert managen. Methoden und Werkzeuge für die Nutzung des Wettbewerbsfaktors Wissen in Unternehmen.Auflage. Oldenbourg (München), 2009.