Produktpiraterie durch gezielten Umgang mit Wissen vorbeugend bekämpfen

Vor dem Hintergrund gefährlicher Produktpiraterie stellt sich vermehrt die Frage nach dem Umgang mit Informationen und Wissen sowie nach Methoden zur Erfassung und zum Schutz aller möglichen Wissens- und Informationsquellen. In diesem Beitrag wird ein Verfahren zur Konzeption von Wissensmanagementmaßnahmen vorgestellt, das explizit Risiken und Nutzen konkreter Wissensweitergaben einbezieht.

Von Norbert Gronau, Julian Bahrs und Gergana Vladova

Das Problem der Produktpiraterie besteht weltweit und hat gravierende wirtschaftliche Auswirkungen für die Unternehmen, wie direkt entgangene Umsätze beziehungsweise Gewinne, Schädigung des Images und Haftungsklagen gegen die Originalhersteller [1]. 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 bis zu lebensbedrohliche Sicherheitsprobleme, wie Berichte über gefälschte Bremsscheiben für Autos oder Flugzeugersatzteile zeigen [2].

Der Verband des Deutschen Maschinen- und Anlagenbaus (VDMA) zeigt in seiner Untersuchung zu Produkt- und Markenpiraterie 2008, dass neben Komponenten und Ersatzteilen zunehmend ganze Maschinen nachgeahmt werden. Die Zahl der Produktimitationen ist alleine zwischen 2008 und 2010 um über acht Prozent gestiegen. Der aus Produktpiraterie resultierende Schaden beträgt für den deutschen Maschinen- und Anlagenbau 6,4 Milliarden Euro jährlich [3].

Neben der Evaluation der Erfolgsaussichten durch den Produktpiraten bieten die fertigen Produkte des Originalherstellers,

welche mittels Reverse Engineering analysiert werden, deren Herstellverfahren und Märkte sowie die verfügbaren Informationen, das Know-how und die 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 wurden, bis hin zur Abwerbung von Mitarbeitern und Industriespionage eingesetzt.

Existierende Maßnahmen gegen Produktpiraterie

Im Laufe der Zeit wurde eine Vielzahl von präventiven und reaktiven Maßnahmen als Antwort auf die Bedrohungen und Schäden durch Produktpiraten entwickelt. Präventive Maßnahmen setzen vor Eintritt eines Schadenfalls ein, wohingegen reaktive Maßnahmen Anwendung finden, wenn Imitationen bereits auf dem Markt aufgetreten sind und die damit einhergehenden Verluste minimiert werden sollen.

» Zum vollständigen Schutz vor Produktpiraterie ist ein passendes Gesamtkonzept aus Prävention und Reaktion notwendig. «

Die in der Industrie etablierten Maßnahmen werden zumeist den reaktiven Maßnahmen zugeordnet. Im Fall von fälschlich zugewiesenen Produkthaftungen sowie bei Auftreten von Patentverletzungen sind juristische Maßnahmen einzuleiten, um den daraus resultierenden möglichen monetären Verlust und Imageschaden zu reduzieren. Rechtliche Maßnahmen sind jedoch langwierig und erst nach Schadenerkennung möglich. Vor allem kleine und mittelständische Unternehmen sind darüber hinaus nicht immer in der Lage, juristische Abteilungen zu beschäftigen, um bei jedem rechtlichen Streit entsprechend gut vertreten zu sein.

Um bei Rechtsstreitigkeiten Originalprodukte von Fälschungen zu unterscheiden und um Produkte eindeutig zu identifizieren, bieten sich technische Schutzmöglichkeiten wie Produktkennzeichnungen und Herstellernachweise an. Neben der einfachen Identifizierung, die durch die Ausstattung des Produkts mit äußeren Merkmalen ermöglicht wird, eignen sich zum besseren Schutz insbesondere Markierungstechniken wie Hologramme, Mikroschriften, Farbpigmente, 1-D- und 2-D-Barcodes, Farbpigmentcodes, Sicherheitsfäden und Ähnliches. Vergleichsweise umfassenderen Schutz bietet die Radiofrequenz-Identifikation (RFID) – elektromagnetische Kennzeichen, die in der Lage sind, eine eindeutige Nummer zu speichern [4]. Durch RFID-Tags können versteckte Informationen in einem geschützten Bereich direkt am Produkt abgelegt werden. Maschinen und Anlagen können mithilfe von RFID durch kognitive Identifizierung beim Austausch von Verschleißteilen oder Hinzufügen zusätzlicher Komponenten diese selbstständig erkennen und auf ihre Echtheit überprüfen [4]. Bei Zerstörung des RFID-Tags oder bei Datendiebstahl entlang der Lieferkette wird allerdings auch dieser Schutz unwirksam. Technische Schutzmöglichkeiten helfen insgesamt zwar bei der Klärung der Originalität, verhindern die Erzeugung eines Plagiats jedoch nicht ganz. Sie dienen oft lediglich zur Erkennung von Fälschungen, ohne die eigentliche Ursache zu bekämpfen.

Zum vollständigen Schutz vor Produktpiraterie ist deswegen ein passendes Gesamtkonzept aus Prävention und Reaktion mit juristischen, technischen und organisatorischen Maßnahmen notwendig. Der bedachte Umgang mit Wissen und das Management zur Verhinderung von ungewolltem Wissensabfluss, womit sich die hier vorgestellte Methode beschäftigt, sind ein essenzieller Teil der Prävention.

Umgang mit Wissen und Informationen im Unternehmen – eine Risiko-Nutzen-Abwägung

Bisher ist vorrangiges Ziel in Forschung und Praxis gewesen, Wissen und Informationen zu verteilen und zugänglich zu machen. Diese Ausrichtung ist jedoch zu einseitig: Wissen ist ein Wettbewerbsvorteil, es kann also nicht immer das Ziel von Unternehmen sein, Wissen nur zu verteilen. Unternehmen streben mit der Wissensweitergabe einen Nutzen an. Dieser entsteht, wenn Informationen und Wissen reibungslos ausgetauscht werden, da diese für den Ablauf der Unternehmensprozesse förderlich sind oder aber zum Schaffen einer gemeinsamen Struktur, Kultur und Organisation beitragen. Wenn allerdings zu viele Informationen übertragen werden, kann dies für die Prozessabläufe als Belastung wirken (Information Overload). Wissensabflüsse können sogar gefährlich für ein Unternehmen sein, wenn der Wettbewerbsvorteil aus Wissens- und Informationsvorsprung verloren geht und die Erstellung von Produktplagiaten ermöglicht wird.

Folglich kann und muss eine Aufgabe des Wissensmanagements sein, zwischen gewollten und ungewollten Informations- und Wissensweitergaben zu unterscheiden. Zusätzlich finden unbewusste (unreflektierte oder unerkannte) Informations- und Wissenstransfers statt. Es gilt, diese transparent zu machen und in die Gestaltung von Wissensmanagementmaßnahmen einzubeziehen. Es ist dabei erforderlich, bestehende Strukturen mit den positiven und negativen Eigenschaften aufzudecken und anzupassen.

In diesem Beitrag wird ein Verfahren zur Konzeption von Wissensmanagementmaßnahmen vorgestellt, das explizit auch die Risiken der Wissensweitergabe in die Analyse und Konzeption einbezieht. Für die Analyse wird auf einen in der Praxis bereits erprobten Modellierungsansatz für wissensintensive Geschäftsprozesse zurückgegriffen. Durch Hinzufügen eines Bewertungssystems können die Chancen und Risiken einer Wissens- und

Informationsweitergabe bestimmt und gegeneinander abgewogen werden.

Die Knowledge Firewall

Die Maßnahmen zur Verhinderung des ungewollten Wissensabflusses müssen mehrere Stellen in virtuellen und realen sozialen Interaktionen berücksichtigen. Es stellt sich die Frage, wie alle Wissens- und Informationsflüsse – mit zugehörigen Akteuren, Wissen und Informationen – prozess- und informationssystemübergreifend gestaltet werden können. Hierzu bietet sich im Unternehmen die Einrichtung einer Knowledge Firewall als Instrument zur Analyse und Planung an.

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 Zugriffspunkte und die jeweils ergriffenen und fehlenden Schutzkonzepte ermittelt werden.

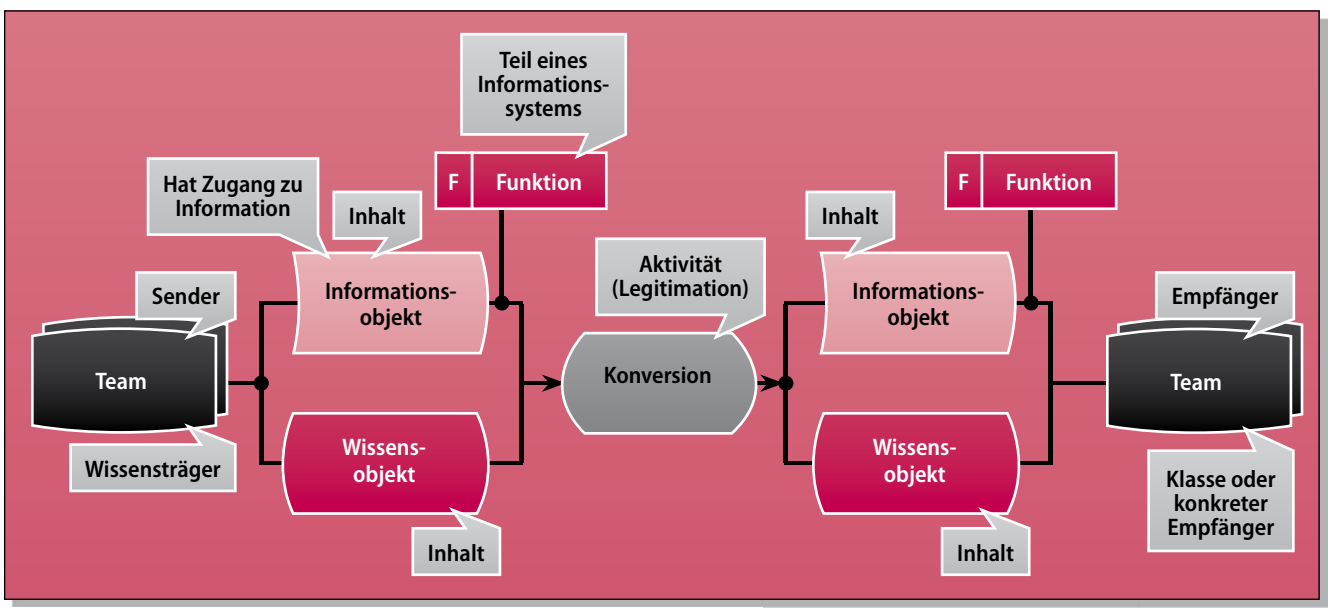
Die zahlreichen Möglichkeiten, die eine Knowledge Firewall bieten kann, zeigen wir am Beispiel der WikiLeaks-Debatte. Der Datenabfluss und die Veröffentlichung von diplomatischen US-Berichten über Regierungen und ihre Mitglieder hätten verhindert werden können durch:

1. **Transparenz über Verbreitung:** Die Informations- und Wissensschnittstellenanalyse stellt die Zugriffs- und Abflussmöglichkeiten der (Welt-)Akteure übersichtlich dar.
2. **Risikoklassifikation des Know-hows:** Anders als in vielen Unternehmen unterliegen die Depeschen bereits einer Geheimhaltungsklassifikation. Allerdings scheint hier der relative Bezug verrutscht, denn auch die niedrigste Geheimhaltungsstufe ist noch schützenswert. In vielen Unternehmen ist nicht bekannt, welche Inhalte überhaupt schützenswert sind.
3. **Überprüfung der Akteure:** Ein Großteil des Know-how-Missbrauchs erfolgt aus den eigenen Unternehmensreihen. Oft sind es frustrierte Mitarbeiter, die ihrem Arbeitgeber schaden wollen oder aus dem Know-how Profit schlagen. Mit der Einrichtung einer Knowledge Firewall werden interne und externe Akteure mit Zugriff auf schützenswerte Inhalte ermittelt sowie überprüft, inwieweit sie zu einem Missbrauch fähig sind oder davon profitieren können. Besonderes Augenmerk wird dabei auf die Bindung und Motivation der Mitarbeiter gelegt.
4. **Präventive Geheimhaltung:** Bei der Gestaltung der Knowledge Firewall wird jede Informations- und Wissensweitergabe hinterfragt und Know-how überall geheim gehalten, wo dies operativ möglich ist. Hierdurch wird die Anzahl der Missbrauchsmöglichkeiten stark reduziert.
5. **Schutzkonzept:** Die Informations- und Wissensschnittstellenanalyse untersucht die bestehenden Schutzkonzepte und zeigt Lücken auf. Zugriffsanomalien werden schnell erfasst und beseitigt.

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 ent-

Abb. 1 *Grundmodell einer Aktivität im Wissensnetz*



Nutzen einer Knowledge Firewall

- Sicherung der Transparenz
- Risikoklassifikation des Know-hows
- Einschätzung der Akteure
- Präventive Geheimhaltung
- Entwicklung eines Schutzkonzepts

wickelt und hat die Identifikation kritischer Informationen, kritischen Wissens sowie beteiligter Akteure in einem Wissenstransferprozess zum Ziel. 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.

Den Ausgangspunkt der IWS bildet der Sender, der über eine Aktivität Informations- und/oder Wissensobjekte an einen Empfänger transferiert. Es werden alle Einzelaktivitäten, die einem gemeinsamen Empfänger zugeordnet werden können, zu einer IWS zusammengefasst. Das Risiko des Wissenstransfers an einer IWS kann lediglich aus der Sicht des Senders objektiv erhoben werden, da ein potenzieller Produktpirat in seiner Rolle als Empfänger kaum vertrauenswürdig über seine Absichten berichten würde. Zu dem Nutzen kann zusätzlich auch der Empfänger befragt werden.

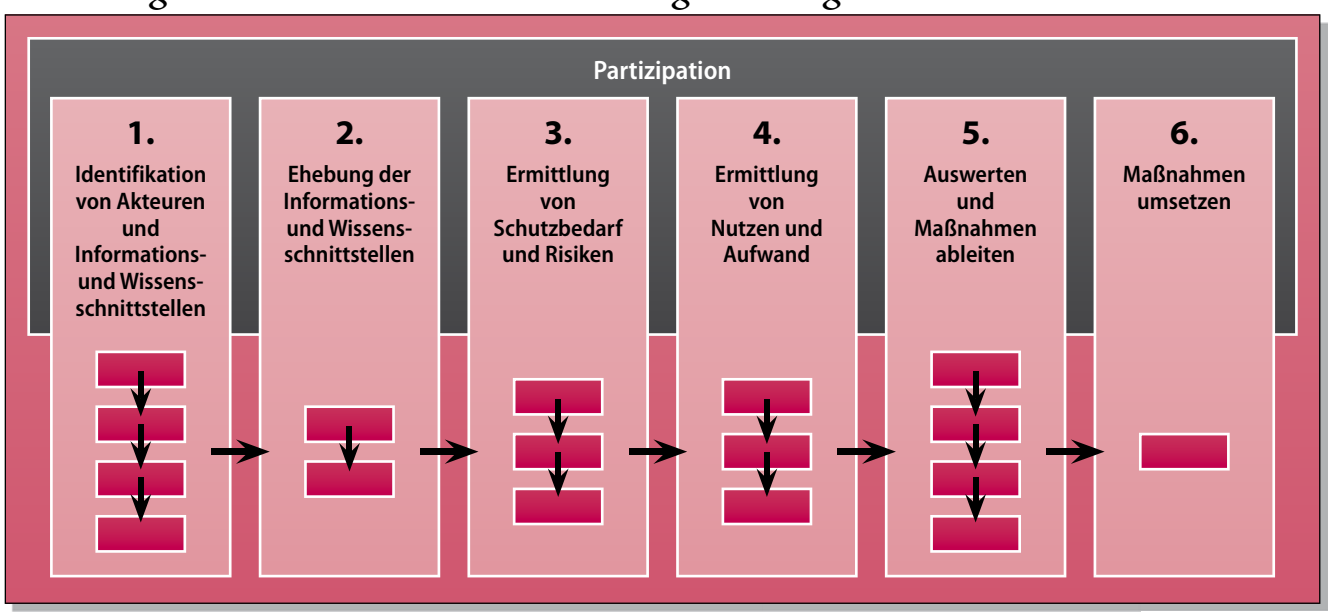
Zu jeder existierenden IWS wird ein Modell erstellt, um dadurch eine genauere Spezifikation der Schnittstellen zwischen Unternehmensteilen sowie innerhalb von Wertschöpfungsnetzwerken zu erreichen (vgl. Abbildung 1). Die Schnittstellen können den Aufgaben eines Prozesses zugeordnet werden. Dabei wird zwischen unternehmensinternen und -externen Schnittstellen unterschieden. Durch die zunehmende Arbeitsteilung und Konzentration auf Kernkompetenzen beginnt sich diese Teilung jedoch aufzulösen [5]. Umso wichtiger wird daher die Festlegung, welche Informationen und welches Wissen im Netzwerk preisgegeben werden. Zur Modellierung wird die Notation der Aktivitätssicht der Knowledge Modeling and Description Language (KMDL) genutzt, die jedoch den Zwecken dieser Methode angepasst wurde (vgl. dazu [6]).

Der Weg zur Knowledge Firewall im Unternehmen

Für die konkrete Anwendung im Unternehmen wurde ein Vorgehensmodell entwickelt, welches in Abbildung 2 mit seinen relevanten Schritten dargestellt wird.

Bei der Durchführung eines Projekts zur Schnittstellengestaltung im Unternehmen werden zuerst ein Intellectual-Property-

Abb. 2 *Vorgehensmodell zur Schnittstellengestaltung*



Schritte eines Projekts

- Was genau muss im Unternehmen analysiert und verändert werden (IWS-Identifikation und Akteurmodell)?
- Was passiert an jeder konkreten IWS und wer ist beteiligt?
- Wie kritisch sind das dort übermittelte Wissen und die Informationen, und kann den beteiligten Akteuren Vertrauen geschenkt werden?
- Was muss investiert werden und was gewinnt das Unternehmen durch die regelgerechte Gestaltung der IWS?
- Mit welchen Maßnahmen werden die gesetzten Ziele erreicht?

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.

Projektverlauf

Zu Beginn des Projekts wird – je nach der aktuellen Unternehmensstrategie – operativen Störungen und gewünschter Reichweite des Projektes, der genaue Untersuchungsbereich abgegrenzt. Der Projektverlauf umfasst folgende Schritte (vgl. Abbildung 2):

1. Im ersten Schritt werden die bestehenden IWS im Unternehmen identifiziert sowie ein Akteurmodell aufgebaut, welches in einer hierarchischen Struktur alle relevanten Akteure für die weitere Analyse verwaltet. Dabei wird angestrebt, vor allem solche Teams zu bilden, die über homogene Informations- und Wissensressourcen verfügen. Dies erfolgt oft analog zur Aufbaustruktur von Unternehmen, kann im Einzelfall jedoch eine zusätzliche, geringfügig feinere Unterteilung von Abteilungen bedeuten. Mit jedem erkannten Akteur (Person oder Team), zu dem eine Beziehung im Untersuchungsbereich identifiziert wird, ist ein Erhebungstermin zu vereinbaren.
2. In Schritt zwei werden die Schnittstellen erfasst und modelliert. Dieser sowie die beiden nachfolgenden Schritte werden in mehreren Sessions jeweils vom Intellectual-Property-Manager und mindestens einem Vertreter je Akteur, der jeweilige Fach- und Situationskenntnis mitbringt, durchgeführt. Die Sessions verlaufen in Form von Gesprächen, in welchen mit einem teilstrukturierten Interview die bestehenden Informations- und Wissensaustauschbeziehungen erhoben und im Modell erfasst werden. Die einfache Modellierung sowie ein hierfür entwickeltes Modellierungswerkzeug (vgl. Abschnitt Knowledge Firewall Designer) ermöglichen das direkte Erfassen im Gespräch. Dabei wird automatisch gleichzeitig ein Katalog von Informations- und Wissensobjekten angelegt, die im Repository verwaltet werden.

> *» Die Leitungsebene der jeweiligen Fachabteilungen ist vor allem bei der Bewertung und Umsetzung der Maßnahmen relevant. «*

3. In Schritt drei stehen die Bewertung der Schutzwürdigkeit (Kritizität) der erhobenen Informations- und Wissensobjekte, eine Einschätzung der Piraterieneigung der jeweiligen internen oder externen Akteure, die Beurteilung des bestehenden Schutzes sowie Aufwand und Nutzen der Wissensweitergabe im Mittelpunkt.
4. Im vierten Schritt erfolgen anschließend die Bewertung des Aufwands und Nutzens und die Ermittlung weiterer, gegebenenfalls noch fehlender Informations- und Wissensweitergaben aus der Empfängerperspektive. Die Empfänger können dabei auf den bereits erstellten Katalog der Informations- und Wissensobjekte und die Betreuung des Intellectual-Property-Managers zurückgreifen. Hierdurch kann eine Wissens- beziehungsweise Informationsnachfrage nach operativer Notwendigkeit (Pull-Prinzip) ausgelöst werden. Die Beurteilung der Sender bezüglich dieser zusätzlichen Wissensbedarfe ist je nach Nutzenperspektive von ihnen im Nachgang einzuholen.
5. Die Schritte fünf und sechs betreffen die konkrete Bestimmung von Maßnahmen zur Gestaltung der IWS sowie die Durchsetzung dieser Maßnahmen.

Besondere Aufmerksamkeit ist den Schritten drei und vier zu schenken, da hier unternehmensspezifische Besonderheiten zum

Ausdruck kommen. Dadurch erst wird die Erfassung der konkreten Situation ermöglicht und die Grundlage für maßgeschnittene Maßnahmen geschaffen.

Für die Bewertungen wird ein einheitliches Konzept mit relativen Zustimmungswerten zu konkreten Einzelfakten auf einer Likert-Skala entwickelt und genutzt. Dazu werden vollständig strukturierte Fragenkataloge zu Risiken und Chancen des Wissenstransfers verwendet. Sowohl Risiken als auch Chancen sind in Zielgrößen zerlegt, denen dann die konkreten Fragen zugeordnet sind (vgl. [6])

Gestaltung der Informations- und Wissensverteilung im Netzwerk der Akteure

Nach der Erhebung und Bewertung der Informations- und Wissensschnittstellen wird die Chance gegen das Risiko abgewogen. Die Auswertungen und Maßnahmenbestimmungen im Schritt fünf werden vom Intellectual-Property-Manager gemeinsam mit der Leitungsebene der jeweiligen Akteure durchgeführt. Chance und Risiko werden in einem Portfolio einander gegenüberstellt und die eingetragenen Schnittstellen in vier Zonen aufgeteilt. Für jede Zone kann jeweils eine Normstrategie abgeleitet werden.

- **Zone I:** Risiko und Chance bei der Wissensteilung sind hoch. Die Führungsebene soll für jeden einzelnen Fall über die Wissensteilung entscheiden.
- **Zone II:** Die Chance bei der Wissensteilung ist hoch, das Risiko gering. Eine Wissensteilung sollte in jedem Fall stattfinden.
- **Zone III:** Chance und Risiko der Wissensteilung sind gering. Die Entscheidung sollte gemeinsam im Team unter Einbezug von Führungskräften stattfinden.
- **Zone IV:** Das Risiko ist hoch, der Nutzen der Weitergabe gering. Es wird eine sofortige Unterbrechung oder gezielte Reduktion der Wissensteilung empfohlen

Schnittstellen mit geringem Nutzen oder zu hohem Risiko können tendenziell eliminiert und somit kann der Aufwand für ungewollte oder unnötige Weitergaben reduziert werden.

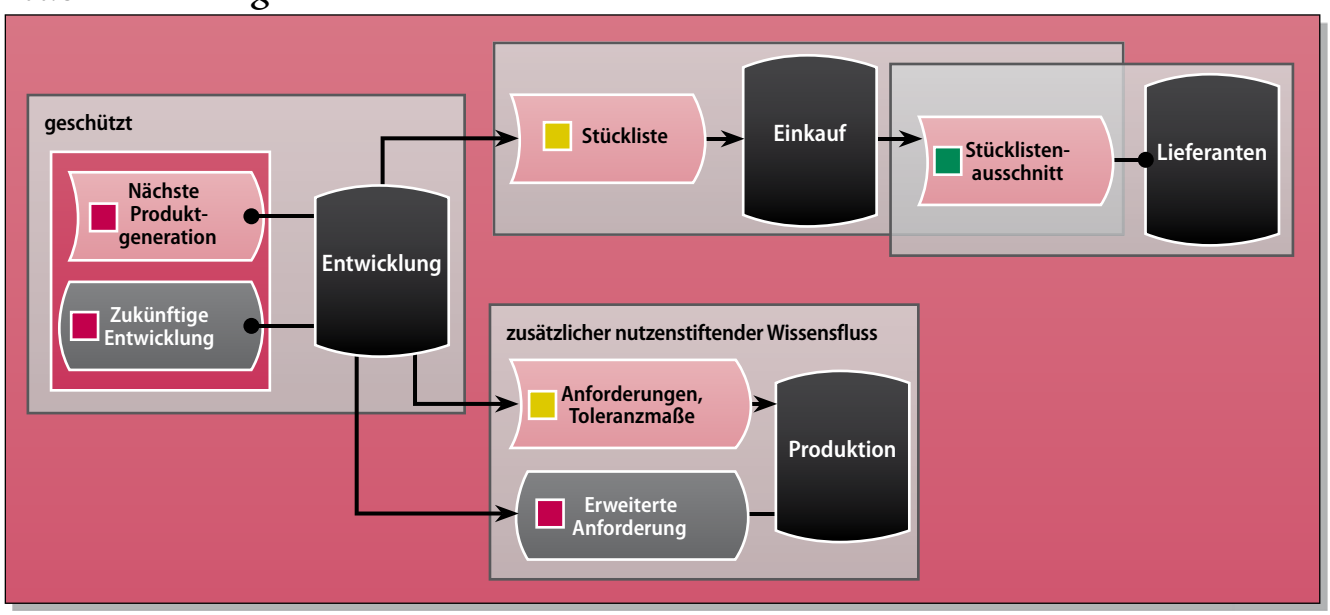
Die Betrachtung der vorhandenen Wissensweitergaben (Ist-Situation) ist jedoch für eine bessere Gestaltung nicht ausreichend: Es ist zu überprüfen, ob bestehende Informations- und Wissensangebote weitere Akteure erreichen sollten und zusätzliche, zurzeit nicht stattfindende Weitergaben veranlasst werden sollten. Dies erfolgt durch Potenzialaussagen über die entsprechenden Inhalte durch die Empfänger. Für so gewonnene zusätzliche Informations- und Wissensschnittstellen kann erneut die Bewertung durchlaufen und parallel bereits Nutzen gegen Risiko abgewogen werden.

Ziel ist die Verbesserung der Informations- und Wissensteilung in Unternehmen. Dabei werden vor allem wiederkehrende Bedarfe ermittelt und bedient. Einmaliger, unvorhersehbarer Ad-hoc-Bedarf kann jedoch „vermittelt“ werden, indem die Verzeichnisse des Informations- und Wissensangebotes verfügbar gemacht werden.

Knowledge Firewall Designer

Zur Unterstützung eines solchen Analyse- und Gestaltungsprojekts 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.

Abb. 3 *Gestaltung des Wissensnetzes*



Darüber hinaus verfügt das Werkzeug über eine Interviewkomponente, die für die jeweiligen Bewertungs-Sessions 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 To-do-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 [7]. Eine Online-Anleitung steht dem Nutzer ebenso dort zur Verfügung.

Ausblick

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. Der Einsatz der beschriebenen Methode hat unter anderem gerade durch den hohen Grad der Partizipation von Mitarbeitern verschiedener Fachabteilungen Potenziale, ohne sie übermäßig zu belasten. Durch die Fokussierung auf die Wissens- und Informationsschnittstellen werden die Erhebung und Modellierung im Gegensatz zur klassischen Geschäftsprozessanalyse schneller und einfacher. Das entwickelte Selbstanalysewerkzeug 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 über die Betrachtung von Nutzen und Risiken die notwendige Entscheidungsgrundlage.

» Durch die Fokussierung auf die Wissens- und Informationsschnittstellen werden Erhebung und Modellierung schneller. «

Die bisherige Erfahrung in sieben Unternehmen zeigt einen Aufwand für die Methodenanwendung von circa zwei Stunden pro Sender bei etwa sechs Sendern für ein mittleres Unternehmen. Es empfiehlt sich, die Analyse durch einen (unternehmensinternen) Intellectual-Property-Manager durchzuführen. Sie muss bei wesentlichen Änderungen in den Geschäftsprozessen oder für neue Kooperationspartner vervollständigt werden. Eine periodische Überprüfung, zum Beispiel jährlich, ist anzustreben. Der Aufwand für die Pflege ist jedoch geringer als der für die Einrichtung.

Letztendlich entwickelt jede Person im privaten realen und virtuellen Leben ihren eigenen Maßnahmenkatalog, um den Umgang mit sensiblen Informationen und Wissen zu managen. Für das Unternehmen sind gemeinsame, allgemeingültige und befürwortete Regeln und Maßnahmen wichtig. Die Knowledge Firewall und die dahinterstehende Methode haben das Ziel, die Gestaltung dieser gemeinsamen Werte zu ermöglichen.

Links und Literatur

[1] Neeman, C. W.: Methodik zum Schutz gegen Produktimitationen. Shaker (Aachen), 2007, S. 2 ff.

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

[3] Verband Deutscher Maschinen-und Anlagenbau e. V. VDMA: Studie über Produkt- und Markenpiraterie in der Investitionsgüterindustrie 2008 sowie 2010. http://www.conimit.de/fileadmin/files/Fakten_und_Statistiken/Statistiken/WM_Ergebnisse_VDMA-Umfrage_Produktpiraterie_2008.pdf sowie http://www.vdma.org/wps/wcm/connect/14c4a6804591ec13a677bf6eafad0bcd/VDMA+Umfrage+Produkt-+und+Markenpiraterie+2010.pdf?MOD=AJPERES&CACHEID=14c4a6804591ec13a677bf6eafad0bcd (Abruf am 27.7.2011).

[4] Günthner, W. A. et al.: Potenziale des Produktpirateriesschutzes durch kognitive Authentifizierung. In: Industriemanagement, 6, 2008, S. 23-27

[5] Picot, A.; Reichwald, R.; Wigand, R. T.: Die grenzenlose Unternehmung. Information, Organisation und Management. Lehrbuch zur Unternehmensführung im Informationszeitalter. 5. Auflage, Gabler (Wiesbaden), 2003, S. 2.

[6] Bahrs, J.; Gronau, N.; Vladova, G.: Mit Wissensflussmanagement Produktpiraterie unterbinden. In: ZFO, 6, 2010, S. 376-382.

[7] www.wi.uni-potsdam.de.

Autoren

Professor Dr. Norbert Gronau
ist Inhaber des Lehrstuhls für Wirtschaftsinformatik und Electronic Government der Universität Potsdam. Er ist Autor zahlreicher wissenschaftlicher Veröffentlichungen und Verfasser beziehungsweise Herausgeber mehrerer Bücher. Seine Forschungsinteressen liegen in den Bereichen Betriebliches Wissensmanagement und Wandlungsfähige ERP-Systeme.

Julian Bahrs
war wissenschaftlicher Mitarbeiter am Lehrstuhl für Wirtschaftsinformatik und Electronic Government der Universität Potsdam und ist Senior Consultant bei der IPI GmbH. Seine Forschungs- und Beratungsschwerpunkte liegen bei der Analyse und Gestaltung wissensintensiver Geschäftsprozesse und Wissensmanagementsystemen.

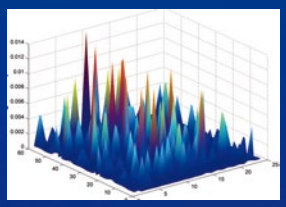
Gergana Vladova
ist wissenschaftliche Mitarbeiterin am Lehrstuhl für Wirtschaftsinformatik und Electronic Government der Universität Potsdam. Ihre Forschungsinteressen liegen im Bereich des (interkulturellen) Wissensmanagements, des Innovationsmanagements sowie der Unternehmenskommunikation.

DOI: 10.1365/s35764-012-0109-y

MathWorks®
Accelerating the pace of engineering and science

Do you speak MATLAB?

Über eine Million Menschen weltweit sprechen MATLAB. Ingenieure und Wissenschaftler in allen Bereichen – von der Luft- und Raumfahrt über die Halbleiterindustrie bis zur Biotechnologie, Finanzdienstleistungen und Geo- und Meereswissenschaften – nutzen MATLAB, um ihre Ideen auszudrücken. Sprechen Sie MATLAB?



Analyse der Intraday-Volatilität von Währungen – entwickelt von CalPERS.

Mehr Informationen:
www.mathworks.de/solutions

MATLAB®

The language of technical computing