Auf dem Weg zum vertrauensvollen, unternehmensübergreifenden automatisierten Datenaustausch von Maschinen – Identifikation von schützenswertem Wissen im Zeitalter von Industrie 4.0

Leon Adler, Andreas Frank, Henner Gimpel, Sebastian Heger, Niclas Nüske, Joachim Starke, Daniela Waldmann, Moritz Wöhl

Angaben zur Veröffentlichung / Publication details:

Adler, Leon, Andreas Frank, Henner Gimpel, Sebastian Heger, Niclas Nüske, Joachim Starke, Daniela Waldmann, and Moritz Wöhl. 2021. "Auf dem Weg zum vertrauensvollen, unternehmensübergreifenden automatisierten Datenaustausch von Maschinen – Identifikation von schützenswertem Wissen im Zeitalter von Industrie 4.0." *HMD Praxis der Wirtschaftsinformatik* 58 (6): 1521–34. https://doi.org/10.1365/s40702-020-00704-w.

HMD (2021) 58:1521–1534
https://doi.org/10.1365/s40702-020-00704-w

SPEKTRUM

Auf dem Weg zum vertrauensvollen, unternehmensübergreifenden automatisierten Datenaustausch von Maschinen – Identifikation von schützenswertem Wissen im Zeitalter von Industrie 4.0

Leon Adler · Andreas Frank · Henner Gimpel · Sebastian Heger · Niclas Nüske · Joachim Starke · Daniela Waldmann · Moritz Wöhl

Eingegangen: 20. Dezember 2019 / Angenommen: 19. Dezember 2020 / Online publiziert: 15. Januar 2021

Zusammenfassung Der unternehmensübergreifende Datenaustausch in der Welt von Industrie 4.0 birgt für Unternehmen immense Potenziale. So können Unternehmen wertvolles Wissen über den Einsatz ihrer Produkte gewinnen und ihren Kunden innovative Dienstleistungen anbieten. Umgekehrt können Kunden die Produkte

L. Adler · H. Gimpel · S. Heger · D. Waldmann · M. Wöhl
Kernkompetenzzentrum Finanz- & Informationsmanagement, Universität Augsburg, Augsburg, Deutschland

L. Adler
E-Mail: leon.adler@fim-rc.de

S. Heger
E-Mail: sebastian.heger@fim-rc.de

D. Waldmann
E-Mail: daniela.waldmann@fim-rc.de

M. Wöhl
E-Mail: moritz.woehl@fim-rc.de

A. Frank
Hufschmied Zerspanungssysteme GmbH, Bobingen, Deutschland
E-Mail: a.frank@hufschmied.net

H. Gimpel · S. Heger · N. Nüske · D. Waldmann · M. Wöhl
Projektgruppe Wirtschaftsinformatik des Fraunhofer FIT, Augsburg, Deutschland
E-Mail: niclas.nueske@uni-hohenheim.de

H. Gimpel (✉) · N. Nüske
Universität Hohenheim, Hohenheim, Deutschland
E-Mail: henner.gimpel@uni-hohenheim.de

J. Starke
BMW Group, München, Deutschland
E-Mail: Joachim.Starke@bmw.de

zielgerichteter einsetzen, wenn sie beispielsweise Produktions- und Materialdetails kennen. Doch dabei möchte kein Unternehmen für sich geschäftskritisches Wissen an einen Partner im Wertschöpfungsnetzwerk freigeben. Zu groß ist das Risiko, Einblicke in beispielsweise Forschungs- und Entwicklungsergebnisse zu gewähren oder dem Kunden eine Kostenkalkulation aufgrund des genauen Prozessablaufes zu ermöglichen. Es ergibt sich die Frage, welche Daten bedenkenlos ausgetauscht werden können und in welchen Daten implizit wertvolles Wissen enthalten ist. Aus diesem Grund stellt der vorliegende Beitrag ein Vorgehensmodell zur Identifikation von schützenswertem Wissen vor dem Hintergrund des unternehmensübergreifenden automatisierten Datenaustauschs von Maschinen über Netzwerkplattformen vor. Mit Hilfe des Modells lassen sich Daten und Wissen analysieren und auf Basis der Schutzbedarfe und enthaltenen Potenziale einstufen. Ein möglichst umfangreicher unternehmensübergreifender Datenaustausch bei möglichst geringem Verlust von Know-how soll ermöglicht werden. Anschließend wird die Erprobung des Modells im Rahmen eines Anwendungsbeispiels vorgestellt und ein Ausblick gegeben.

Schlüsselwörter Industrie 4.0 · Know-how-Schutz · Unternehmensübergreifende Vernetzung · Datenaustausch · Maschinendaten

Towards Trustworthy, Cross-Company, Automated Data Exchange Between Machines – Identification of Know-How Worthy of Protection in the Age of Industry 4.0

Abstract Cross-company data exchange in the world of industry 4.0 holds immense potential for companies. Companies can gain valuable knowledge about the use of their products and offer their customers innovative services. Conversely, customers can use their products in a more targeted way if they know production and material details, for example. But no company wants to share business-critical knowledge with a partner in the value creation network. The risk of providing insights into, for example, research and development results or enabling the customer to calculate costs based on the exact process flow is too great. The question arises as to which data can be exchanged without hesitation and which data implicitly contain valuable knowledge. For this reason, this article presents a process model for identifying knowledge worth protecting against the background of cross-company data networking. With the help of the model, data and knowledge can be analyzed and classified on the basis of protection requirements and contained potentials. The aim is to enable cross-company data exchange while preventing the violation of know-how. Subsequently, the testing of the model is presented in the context of an application example and an outlook is given.

Keywords IoT · Industry 4.0 · Knowledge protection · Value creation networks · Data exchange · Data security · Machine data

1 Ausgangslage und Zielsetzung

Die zunehmende Verfügbarkeit digitaler Technologien mit der Vision von durchgängig und vollständig vernetzten und virtualisierten Entitäten inner- und außerhalb von Unternehmen, entlang von Wertschöpfungsketten und Objektlebenszyklen bezeichnet man gemeinhin als vierte industrielle Revolution (Industrie 4.0). Diese unternehmensübergreifende Vernetzung besitzt Potenziale, die deutlich über das häufig angeführte Optimierungsvermögen zur Erschließung von Effizienz- bzw. Produktivitätsreserven (Emmrich et al. 2015) oder die Steigerung der unternehmensinternen Flexibilität (Kelkar et al. 2014) durch eine technologische Befähigung hinausreichen. Beispielsweise können Unternehmen nicht nur von der direkten Nutzung einer vernetzten Lösung profitieren, wie etwa einer adaptiven Prozessrouting-Lösung. Vielmehr entstehen durch den unternehmensübergreifenden Datenaustausch Potenziale für digitale Services, wie kontinuierliche Remote-Interaktionen und Analytik (Baltuttis et al. 2019). So können durch die Gewinnung von Prozessdaten aus der Fertigung eines Bauteilproduzenten deren Betriebsmittellieferanten (z. B. Werkzeughersteller) bei der Fehlerbehebung – nunmehr daten- und damit faktenbasiert – unterstützen und Beratungsleistung zum Einsatz der hauseigenen Produkte anbieten. Dies führt zu höheren Anlagenverfügbarkeiten auf Seiten des Bauteilproduzenten und somit einer Kostenreduktion. Anderseits können Betriebsmittellieferanten durch die Prozessdaten profitieren, indem sie Wissen über den Produkteinsatz ihrer Produkte erlangen und somit die eigene Produktentwicklung – auch zum Nutzen der datenbereitstellenden Kunden – profitiert. Darüber hinaus kann der übergreifende Austausch innovative Lösungen für Predictive Maintenance und Inline-Qualitätskontrollen ermöglichen, um nur einige Beispiele zu nennen. Auch aus diesen Gründen sehen über 80 % der Industrieunternehmen in wichtigen Industrienationen die verstärkte Nutzung von Daten in der Wertschöpfung als eine Top-Priorität (General Electric Company und Accenture Plc 2015). Der Großteil des Potenzials in Deutschland wird dabei dem Maschinenbau, der Automobilindustrie sowie Herstellern elektrischer Ausrüstung zugeschrieben. Damit ist die Auseinandersetzung mit Implikationen von Industrie 4.0 für produzierende, größtenteils mittelständische Unternehmen eine besonders wichtige Aufgabe (Bauer et al. 2014). Dieses immense Wertschöpfungspotenzial teilt sich in bislang unbekanntem Verhältnis zwischen den Fabrik- und Anlagenausrüstern (Anbietern von Industrie-4.0-Lösungen) und den Anwendern von Industrie-4.0-Lösungen. Die Unternehmen sind gefordert, sich proaktiv mit den möglichen Auswirkungen auf das Produkt- und Servicespektrum in ihrem Geschäftsfeld auseinanderzusetzen.

Jedoch sehen sich Unternehmen vor dem Hintergrund der absehbar zunehmenden, unternehmensübergreifenden Vernetzung einigen Herausforderungen gegenübergestellt. Insbesondere laufen Unternehmen Gefahr, dass durch die Bereitstellung von Daten geschäftskritisches und damit schützenswertes Wissen das Unternehmen verlässt, wie beispielsweise vertrauliche Firmeninformationen (Rannenberg 2000). Die stetige Weiterentwicklung von Methoden zur Analyse großer Datenmengen, Big Data Analytics, führt dazu, dass Unternehmen außerordentlich vorsichtig bei der Freigabe von Daten sind. Bis dato beschäftigen sich nur wenige Projekte und Initiativen mit der unternehmensübergreifenden Vernetzung und dem Austausch von

Daten in Wertschöpfungsnetzwerken (z. B. Gaia-X oder der Industrial Data Space). Insbesondere die Souveränität über die eigenen Daten stellt einen kritischen Erfolgsfaktor solcher Vorhaben dar (Otto et al. 2016; Bundesministerium für Wirtschaft und Energie 2019). Um diese jedoch zu erreichen, ist an erster Stelle ein Verständnis über die eigenen Daten notwendig.

Vor allem in Deutschland stellt der Datenschutz – also der Schutz von Daten vor Missbrauch, unberechtigter Einsicht oder Verwendung, Änderung oder Verfälschung (Pommerening 1991, S. 10) – ein relevantes und sensibles Thema dar. Dabei geht es nicht nur um den Schutz personenbezogener Daten, wie es beispielsweise in der EU-Datenschutzgrundverordnung vorgeschrieben ist, sondern insbesondere auch um Daten, bei denen der Schutzbedarf sich aus rein unternehmerischer Perspektive ergibt, da sie wettbewerbsrelevantes Wissen in sich tragen. Oftmals werden die Potenziale durch gezielten Datenaustausch bewusst nicht realisiert, um schwierig zu überschauende Risiken zu vermeiden. Aus diesem Grund stellt sich die Frage, welche Daten ein Unternehmen austauschen kann, ohne dabei geschäftskritisches Wissen zu gefährden und gleichzeitig einen Mehrwert im eigenen Unternehmen und im Wertschöpfungsnetzwerk zu schaffen.

Der vorliegende Beitrag präsentiert ein auf wissenschaftlichen Grundlagen beruhendes Vorgehensmodell mit direktem Praxisbezug zur Identifikation von schützenswertem Wissen und Potenzialen im Kontext unternehmensübergreifenden Datenaustauschs. So sollen die Potenziale des Datenaustauschs gehoben werden, ohne dass es dabei zu Know-how-Verletzungen kommt. In der Literatur findet sich bisher kein Vorgehensmodell, welches in diesem Kontext ohne Anpassung anwendbar wäre. Ein guter Ansatzpunkt für die Entwicklung eines passenden Vorgehensmodells findet sich aber in der Domäne des Wissensschutzes im Kontext von Produktpiraterie: Das von Bahrs et al. (2010) und Vladova et al. (2012) vorgeschlagene Vorgehen zum Wissensflussmanagement stellt deshalb die Grundlage für die Ableitung eines für den vorliegenden Kontext angepassten Vorgehensmodells dar. Dieses wurde in enger Zusammenarbeit von Wissenschaft und Praxis weiterentwickelt und validiert. Es ist das Ergebnis einer Reihe von Interviews und Workshops mit Wissenschaftlern und Vertretern zweier Industrieunternehmen – einem Fräswerkzeughersteller und einem Fräswerkzeugnutzer –, die in einer Kunden-Lieferanten-Beziehung stehen und partnerschaftlich den vertrauensvollen Austausch ausgewählter Daten entwickeln. Das Vorgehensmodell wird in der Kooperation der beiden Unternehmen angewendet.

Abschn. 2 beschreibt das Vorgehensmodell. Abschn. 3 demonstriert die Anwendbarkeit. Abschn. 4 gibt Handlungsempfehlungen und einen Ausblick.

2 Vorgehensmodell

Das angewandte Vorgehen basiert auf dem Modell von Bahrs et al. (2010) und Vladova et al. (2012), welches die Reduzierung von Produktpiraterie mithilfe von Wissensflussmanagement zum Ziel hat. Aus folgenden Gründen waren Anpassungen des Modells notwendig, damit dieses auf den Kontext des unternehmensübergreifenden Datenaustauschs anwendbar ist: Erstens steht, speziell im Industrie 4.0-Kontext, der Austausch von Daten und nicht von Wissen im Vordergrund. Daten werden aus Zei-

chen nach den Regeln einer Syntax gebildet. Ordnet man diesen Daten anschließend eine Bedeutung zu, werden Daten zu Informationen (Bodendorf 2006, S. 1). Trotz der Differenzierung von Daten und Informationen wird in diesem Beitrag der Einfachheit halber der Begriff ‚Daten' als Sammelbegriff für beide Konzepte verwendet. Wissen wird implizit mit den Daten übermittelt. Im Vorgehen von Bahrs et al. (2010) und Vladova et al. (2012) ist die Unterscheidung von Daten und Wissen nicht relevant. Da im Rahmen des unternehmensübergreifenden Datenaustauschs aber Daten geteilt und gleichzeitig kritisches Wissen geschützt werden sollen, ist diese Unterscheidung wichtig, weshalb Anpassungen in Schritt 1 und 2 des Vorgehensmodells notwendig sind[1,2]. Zweitens gehen Bahrs et al. (2010) und Vladova et al. (2012) in ihrem Modell davon aus, dass Wissen das Unternehmen bereits verlässt, und analysieren den Status Quo im Unternehmen, um den Wissensabfluss anschließend zu kontrollieren. Es werden also ex-post explizit Einzelfälle/Schnittstellen benannt, die einer Kontrolle des Wissensabflusses bedürfen. Im vorliegenden Falle steht beim unternehmensübergreifenden Datenaustausch dagegen nicht im Vordergrund, welches derzeit freigegebene Wissen nicht geteilt werden darf, sondern welche Daten zukünftig ausgetauscht werden können. Somit handelt es sich um eine generalistische, ex-ante Betrachtung, in welchen Daten implizit Wissen stecken könnte. Im Gegensatz zur Produktpiraterie handelt es sich hierbei um wesentlich tiefergehende kontinuierlich aufgezeichnete Prozessdaten mit hoher Abtastung. Dieser Perspektivenwechsel zeigt sich v. a. in Schritt 2 des Vorgehens. Letztlich ist der Ansatz von Bahrs et al. (2010) und Vladova et al. (2012) auf die Reduzierung von Produktpiraterie ausgerichtet und somit stehen ausschließlich Risiken im Vordergrund (Gronau 2011). Der unternehmensübergreifende Datenaustausch zwischen den Kooperationspartnern findet jedoch überhaupt erst wegen der möglichen resultierenden Vorteile statt, daher ist neben der Risikobewertung, welche nach wie vor relevant ist, auch

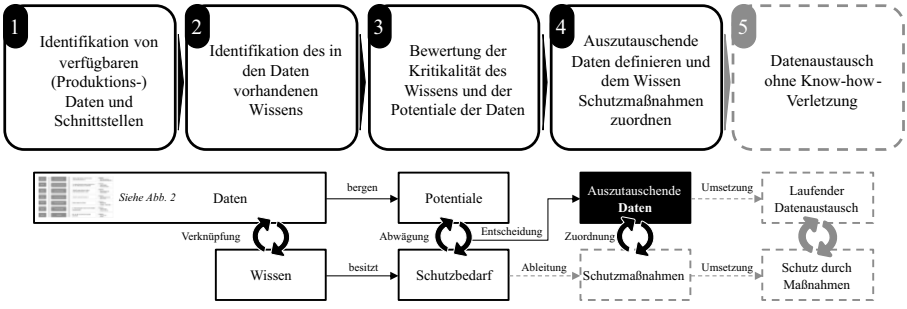

Abb. 1 Schematische Darstellung des Vorgehensmodells zur Identifikation von schützenswertem Wissen im Kontext des unternehmensübergreifenden Datenaustausches

[1] Schritt 1: Statt der Identifikation von Informations- und Wissensschnittstellen steht die Identifikation von verfügbaren und austauschbaren Daten im Fokus. Schnittstellen nach außen bestehen i. d. R. noch nicht.

[2] Schritt 2: Ein Wissensabfluss durch Datenaustauch existiert nicht, da noch keine Daten ausgetauscht werden, stattdessen ist die Verknüpfung von Daten und Wissen notwendig.

eine Bewertung der entstehenden Potenziale vonnöten. Deshalb findet sich auch in Schritt 3 des Vorgehensmodells eine dahingehende Anpassung[3].

Das vorliegende Modell zur Identifikation von schützenswertem Wissen im Kontext des unternehmensübergreifenden Datenaustauschs besteht aus vier Prozessschritten. In einem ersten Schritt sind die verfügbaren Daten zu identifizieren, ehe diese im zweiten Schritt mit dem ihnen innewohnenden Wissen verknüpft werden. Darauf aufbauend sind im dritten Schritt die Schutzbedarfe des Wissens und Potenziale der Daten zu ermitteln. Im vierten und letzten Schritt kann die Ableitung geeigneter Schutzmaßnahmen für die zum Austausch verfügbaren und relevanten Daten auf Grundlage des enthaltenen, schützenswerten Wissens erfolgen. In der vorliegenden Arbeit wird lediglich ein Ausblick auf diesen Prozessschritt gegeben. Abb. 1 fasst das Vorgehensmodell zusammen.

2.1 Schritt 1 & 2: Identifikation von Daten und Wissen

Nicht alle in einem Unternehmen potenziell verfügbaren Daten sind auch für Dritte, wie z. B. die Unternehmenspartner, wertvoll. Ebenso gilt, dass aufgrund rechtlicher, technischer, organisatorischer und wirtschaftlicher Rahmenbedingungen nicht alle potenziell für den Datenaustausch relevanten Daten verfügbar sind. Um zu beantworten, welche Daten Potenzial bergen und welche Daten schützenswertes Wissen enthalten, muss zuerst erhoben werden, welche Daten prinzipiell zur Verfügung stehen (Schritt 1).

Zur Identifikation und Erhebung von relevanten Daten werden in Schritt 1 die beteiligten Unternehmen in dem für den Austausch relevanten Teil des Wertschöpfungsnetzwerks systematisch betrachtet. Dazu erfolgt eine Analyse der beteiligten Unternehmen auf unterschiedlichen Ebenen in Anlehnung an Gimpel und Röglinger (2017), indem in den einzelnen Unternehmen die vorhandenen Daten identifiziert und erhoben werden. Dies geschieht in den beteiligten Unternehmen unabhängig voneinander und bedingt je nach Unternehmen unterschiedlich viel Aufwand aufgrund der individuellen Gegebenheiten. Dabei werden von jedem Unternehmen die für den jeweiligen Anwendungsfall sinnvollen Unternehmensdaten identifiziert (Ebene 1). Anschließend können in jedem Unternehmensbereich die relevanten Geschäftsprozesse (Ebene 2) und Prozesskomponenten (Ebene 3) erhoben werden. Jede Prozesskomponente kann nun auf die enthaltenen Informationsquellen (Ebene 4) analysiert werden und die verfügbaren Variablengruppen (Ebene 5) und einzelne Variablen (Ebene 6) erhoben werden[4]. Abb. 2 fasst das Ebenen-Modell zusammen und gibt Beispiele je Ebene an. Die Pfeile in der Abbildung verdeutlichen, dass die Analyse nicht Top-Down erfolgen muss. Auch eine Bottom-Up-Analyse, beginnend mit der Identifikation der einzelnen Variablen oder ein Einstieg beispielsweise von einem konkreten Geschäftsprozess ausgehend, kann durchaus sinnvoll sein.

[3] Es wird nicht nur die Kritikalität des implizit ausgetauschten Wissens bewertet, sondern auch das in den Daten steckende Potenzial.

[4] Das Anwendungsbeispiel in Abschn. 3 verdeutlicht die Analyse über die verschiedenen Ebenen an ausgewählten Prozessschritten der beiden Anwendungspartner.

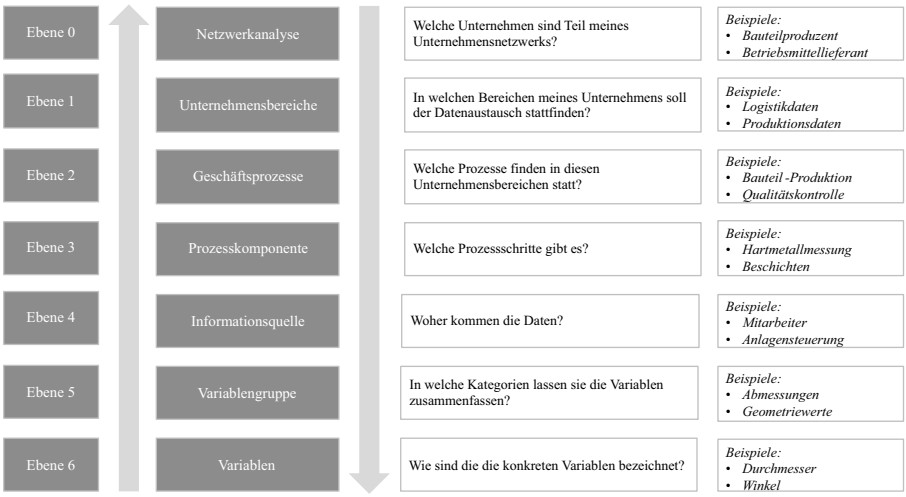

Abb. 2 Ebenen-Modell zur strukturierten Identifikation von Daten und Informationen. (In Anlehnung an Gimpel und Röglinger 2017)

Nachdem die vorhandenen Daten in den beteiligten Unternehmen erhoben wurden, wird anschließend das in ihnen enthaltene geschäftskritische Wissen erfragt (Schritt 2). Dazu werden die zur Identifikation der Daten untersuchten Geschäftsprozesse (Ebene 2) und deren Komponenten (Ebene 3) auf das benötigte Wissen in den Geschäftsprozessen hin untersucht. In Anlehnung an Bahrs et al. (2010) und Vladova et al. (2012) eignen sich dazu Interviews mit Vertretern der Unternehmen sowohl auf der Senderseite als auch der Empfängerseite der möglichen auszutauschenden Daten. Die Senderseite ist dabei das Unternehmen, welches Daten und Informationen zur Verfügung stellt. Die Empfängerseite stellt das Unternehmen dar, welches Daten und Informationen der Senderseite bezieht und daraus Potenziale erschließt. Da der unternehmensübergreifende Datenaustausch im Normalfall auf Gegenseitigkeit beruht und einen Austausch mit Nutzen auf beiden Seiten darstellt, ist jedes Unternehmen entsprechend Empfänger und Sender. Auf beiden Seiten werden dabei sowohl „Generalisten“, wie beispielsweise Führungskräfte, als auch „Spezialisten“, wie beispielsweise Entwicklungsingenieure, mittels semi-strukturierten Interviews entlang der Geschäftsprozesse, deren Komponenten und Informationsquellen detailliert nach dem vorhandenen Wissen befragt.

2.2 Schritt 3: Bewertung von Schutzbedarfen und Potenzialen

Wissen entsteht durch die Verknüpfung von Informationen und der Kenntnis über die Zusammenhänge (Bodendorf 2006). Deshalb liegt insbesondere auf der Senderseite der Fokus auf dem geschäftskritischen Wissen, welches in den identifizierten Daten beinhaltet ist. So möchten viele Unternehmen beispielsweise weder Wissen über die Produktionsauslastung oder Preisgestaltung ihrer Produkte teilen, noch Details zu Prototypen und damit verbundenes Wissen über neue Produkte preisgeben. Folglich muss die Senderseite sich zunächst bewusst werden, welches Wissen das

Unternehmen auf keinen Fall verlassen darf und nicht für den unternehmensübergreifenden Datenaustausch freigegeben ist. Im dritten Schritt wird aus diesem Grund das verfügbare Wissen dem Schutzbedarf entsprechend eingestuft. Dabei kann das enthaltene Wissen im Wesentlichen schützenswert, bedingt schützenswert und nicht schützenswert sein. Bedingt schützenswertes Wissen ist dabei definiert als das Wissen, welches unter bestimmten Auflagen und Restriktionen ausgetauscht werden kann und somit zur Verhandlungssache wird[5]. Als Anhaltspunkt zur Identifikation von Schutzbedarfen wird Wissen als Ressource betrachtet und das VRIN-Framework (Barney 1991) zum Einsatz gebracht, welches die von Bahrs et al. (2010) und Vladova et al. (2012) vorgeschlagenen Kriterien leicht erweitert. Gemäß des VRIN-Frameworks kann Wissen dann einen nachhaltigen Wettbewerbsvorteil bringen, wenn es vier Kriterien erfüllt:

- (I.) es muss wertvoll (*v*aluable) sein, in dem Sinne, dass es Chancen nutzt und/oder Bedrohungen im Umfeld eines Unternehmens neutralisiert,
- (II.) es muss selten (*r*are) im aktuellen und potenziellen Wettbewerb eines Unternehmens sein,
- (III.) es muss unvollkommen imitierbar (*i*mperfectly imitable) sein, und
- (IV.) es kann keinen strategisch gleichwertigen Ersatz (*n*on-substitutable) für diese Ressource geben, der wertvoll, aber weder selten noch unvollkommen nachahmbar ist.

Aus den Anfangsbuchstaben der englischen Namen der Kriterien ergibt sich das Akronym VRIN. Verletzt eine Variable eines dieser vier Attribute, kann dies ein

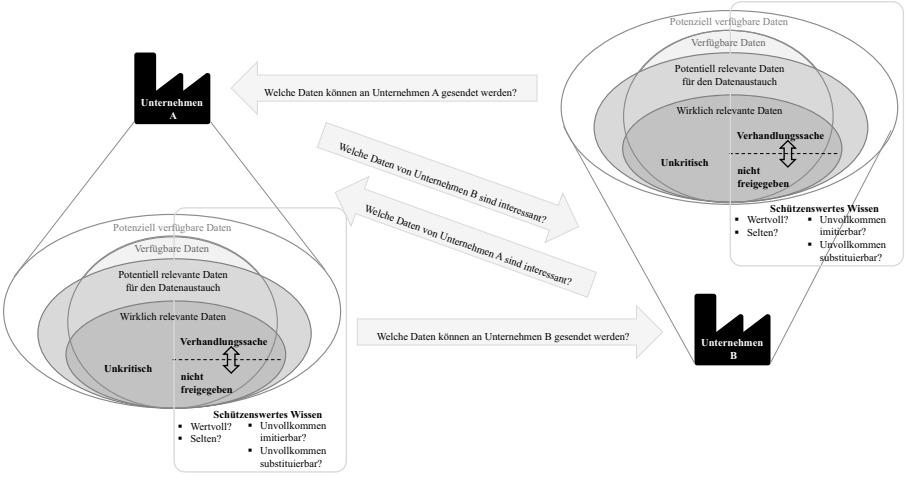

Abb. 3 Fragestellungen und Kriterien für den unternehmensübergreifenden Datenaustausch

[5] Beispielsweise können bestimmte Daten zeitlich begrenzt ausgetauscht werden, um etwa beanstandete Qualitätsmängel zügig und faktenbasiert behandeln zu können.

Anhaltspunkt für einen nur (bedingten) Schutzbedarf oder gar keinen Schutzbedarf sein.[6]

Auf der Empfängerseite liegt indes der Fokus auf der Analyse der enthaltenen Potenziale in den vorhandenen Daten. Steht abschließend fest, welches Wissen auf Senderseite ausgetauscht werden kann und welche Daten in welcher Form zur Verfügung stehen, gilt es zu identifizieren, welche Daten Potenziale für Erkenntnisse auf der Empfängerseite bieten. Dazu werden die identifizierten Daten analysiert und irrelevante Datenpunkte vernachlässigt, sodass sich die Menge aller verfügbaren Daten auf die wirklich relevanten Daten einschränkt.

Anschließend werden die Rollen (Sender und Empfänger) der Unternehmen entsprechend getauscht, so dass ein beidseitiges Bild entsteht (vgl. Abb. 3). Insgesamt ist zu beachten, dass sich Potenziale und Schutzbedarfe mit dem situativen Kontext der Unternehmen verändern können und keine allgemeingültigen konstanten Ausprägungen annehmen. Sowohl Potenziale als auch Schutzbedarfe können vom gleichen Unternehmen je nach Geschäftspartner und wirtschaftlicher Situation anders bewertet werden und unterliegen somit einer gewissen Dynamik.

2.3 Ausblick: Schutzmaßnahmen

Die Einstufung der Schutzbedarfe des enthaltenen Wissens in den relevanten Daten und Informationen zieht die Frage nach potenziellen Schutzmaßnahmen nach sich. Während unkritische Daten bedenkenlos ausgetauscht werden können und geschäftskritische Daten nicht zur Verfügung gestellt werden sollten, bilden bedingt austauschbare Informationen einen Trade-Off. Mit Hilfe geeigneter Schutzmaßnahmen lässt sich evaluieren, welche Daten unter gewissen Bedingungen ausgetauscht werden können. Beispielsweise gibt es eine Vielzahl an Methoden, um das enthaltene Wissen in Daten im Rahmen von Analysen zu schützen. Unter anderem sind dies vergleichsweise einfache Modifikationsmethoden, wie beispielsweise einem Hinzufügen von Rauschen, dem Blockieren ausgewählter Daten, der Aggregation von Daten zu Kennzahlen, oder der Kombination von Daten zu einer gröberen Kategorie. Es stehen aber in der wissenschaftlichen Literatur auch komplexe Methoden, wie heuristische, kryptographische oder rekonstruierende Techniken, zur Verfügung (Verykios et al. 2004). Moderne technische Ansätze finden sich in Themenfeldern wie etwa Privacy Preserving Data Mining oder Secure Multi-party Computation. Aber auch betriebswirtschaftliche, organisatorische und juristische Ansätze, wie eine vertrauenswürdige dritte Partei für das Matching der Daten aus beiden Unternehmen sowie deren Bewertung und vertragliche Absicherungen sind denkbar.

[6] Ein weiteres beim unternehmensübergreifenden Datenaustausch relevantes Kriterium kann der Datenschutz nach beispielsweise der EU-Datenschutzgrundverordnung oder dem Bundesdatenschutzgesetz darstellen. Da im Kontext der Industrie 4.0 allerdings keine personenbezogene Daten im Fokus stehen, wurde dieser bei der Bewertung der Kritikalität nicht beachtet.

3 Anwendungsbeispiel

Das beschriebene Vorgehensmodell wurde in einem Projekt erfolgreich angewendet, was Anwendbarkeit und Wirksamkeit des Vorgehensmodells untermauert. In dem Projekt arbeiten unter anderem zwei Industrieunternehmen zusammen, um den Austausch von Prozess- und Produktdaten zu etablieren. Dabei handelt es sich um das Unternehmen A aus der Automobilbranche, mit Fokus auf einen Teilbereich, in dem Umformwerkzeuge für die Karosserie produziert werden. Hierbei kommen unterschiedliche Werkzeuge des Unternehmens B zum Einsatz, welches sich auf die Herstellung von Fräswerkzeugen spezialisiert hat. Während Unternehmen A gemäß EU-Definition als Großunternehmen gilt, ist Unternehmen B ein mittleres Unternehmen (gemäß KMU-Definition). Beide Unternehmenspartner wurden im Rahmen des Projekts durch sowohl Führungskräfte wie auch ausgewiesene Experten aus der Produktentwicklung bzw. Produktion vertreten. Alle Mitarbeiter brachten dabei langjährige Berufserfahrung und Branchenexpertise mit ein.

3.1 Schritt 1 & 2: Identifikation von Daten und Wissen

Zunächst haben sich beide Unternehmen, die im Wertschöpfungsnetzwerk (Ebene 0) in einer Lieferanten-Kunden-Beziehung stehen, sich auf einen möglichen Umfang der Kooperation auf den Ebenen von Unternehmensbereichen (Ebene 1) und Geschäftsprozessen (Ebene 2) geeinigt und sich gegenseitig die dort enthaltenen Prozesskomponenten (Ebene 3) aufgezeigt, um einen ersten Eindruck möglicher Potenziale aus dem Datenaustausch zu bekommen. In Unternehmen B werden metallische Rohlinge, die im Wareneingang zuerst geprüft werden, zu Fräswerkzeugen geschliffen, beschichtet und endvermessen. Diese Fräswerkzeuge kommen anschließend in den Produktionsprozessen des Unternehmens A als Betriebsmittel zum Einsatz. Unternehmen A produziert Formwerkzeuge, welche auf Basis von CAD-Daten und unter Verwendung von CAM-Tools in Bearbeitungszentren gefräst werden. Diesem automatisierten Prozess folgen der manuelle Zusammenbau der gefrästen Komponenten zum Formwerkzeug sowie bei Bedarf weitere Veredelungsschritte. Durch Austausch von Produkt- (Fräswerkzeug) und Produktionsdaten (Formwerkzeugbau) erhoffen sich die beiden Unternehmen sowohl wertvolles Wissen beispielsweise für die Produktentwicklung (Fräswerkzeuge) als auch eine Kostenreduktion in der Produktion (z. B. erhöhte Standzeiten[7] und Vermeidung von Werkzeugbruch).

Sowohl Unternehmen A als auch Unternehmen B erstellten darauf aufbauend intern je eine Liste mit bestehenden Variablen (Ebene 6), welche für die zuvor genannten Ziele potenziell genutzt werden können. Trotz der vorherigen Einschränkung auf einzelne Prozesskomponenten war dies eine sehr aufwendige, detailreiche Aktivität. Über Informationsquellen (Ebene 4) nachzudenken half hierbei immer wieder,

[7] Unter dem Begriff Standzeit wird die die Nutzungsdauer des Fräswerkzeuges verstanden. Im Rahmen des Projektes konnte – nunmehr datenbasiert – die tatsächliche Nutzung eines Fräswerkzeuges ermittelt werden. Zugleich zeigte sich, dass nicht die Zeit, sondern der Weg, in dem eine spanende Bearbeitung erfolgt, der aussagekräftige Wert ist. Dieser Wert wird als Arbeitsweg bezeichnet und stellt somit den Weg dar, bei dem das Werkzeug, beispielsweise beim Schruppen, Schlichten oder Bohren, im Eingriff am Werkstück ist.

um eine Vollständigkeit der Variablen zu erreichen. Fragen waren beispielsweise, welche Daten aus der Maschinensteuerung des Bearbeitungszentrums ausgelesen werden können oder welche Daten in der Endqualitätskontrolle erfasst werden können. Es folgte die Herausforderung, die Daten digital verfügbar zu machen. In den Unternehmen lagen Daten zu Projektbeginn zum Teil nur analog, in unterschiedlichen Datenformaten und/oder lokal in unvernetzten Maschinen vor. Insbesondere ältere Maschinen mussten netzwerkfähig gemacht werden, um bestehende Sensorwerte abrufen zu können. Teils wurde Sensorik nachgerüstet.

Als Resultat von Schritt 1 entstand eine Liste mit je mehreren hundert potenziell für den Austausch relevanten Variablen (Ebene 6), die bei den Unternehmen im Rahmen der zuvor eingegrenzten Prozesskomponenten (Ebene 3) zur Verfügung stehen. Um die Komplexität zu reduzieren, wurden die Variablen gruppiert, um über ganze Variablengruppen diskutieren zu können (Ebene 5). Die Diskussion über Variablengruppen (Ebene 5) stellte sich als handhabbarer heraus als die Diskussion über einzelne Variablen (Ebene 6), aber auch als zielführender als eine Diskussion nur über Informationsquellen (Ebene 4). Das Wechselspiel der Analyse auf Ebenen 4, 5 und 6 brachte in einem iterativen Prozess immer wieder neue Ideen hervor, welche Daten existieren.

Im zweiten Schritt wurde erfasst, welches Wissen bei den Projektpartnern in Bezug auf die eigenen Produkte und die eigene Produktion vorhanden ist und potenziell geschützt werden muss. Dazu wurden Workshops mit je beiden Projektpartnern gesondert durchgeführt. Dabei ging es zunächst jeweils um die Frage, welches Knowhow bei den jeweiligen Unternehmen in der eigenen Produktion und Produktentwicklung besteht. Die Diskussionen wurden (analog zur Identifikation der Daten) entlang der zuvor definierten und betrachteten Produktionsprozesse (Ebene 2) und Prozesskomponenten (Ebene 3) geführt. Als Ergebnis entstand in beiden Unternehmen eine Auflistung von vorhandenem Wissen, welches im Folgenden auf die Schutzbedarfe hin analysiert werden konnte. Darüber hinaus zeigte die Durchführung des zweiten Schritts im Rahmen des Projekts, dass die integrierte Aufarbeitung von Daten und Wissen einen effektiven Ansatz darstellt. So unterstützt die Übersicht vorhandener Daten dabei, das vorhandene Wissen im Unternehmer umfassend und zielgerichtet erarbeiten zu können. Umgekehrt ermöglicht die Kenntnis über das vorhandene Wissen eine gute Priorisierung der vorhandenen Daten und welches Wissen in diesen steckt.

3.2 Schritt 3: Bewertung von Schutzbedarfen und Potenzialen

Im dritten Schritt lag der Fokus nunmehr darauf zu eruieren, inwiefern die identifizierten Wissenselemente geschäftskritisch sind und entsprechende Schutzbedarfe bestehen. Dies geschah in vier Workshops (siehe Abb. 3, ein Workshop je Pfeil). Das Ergebnis der ersten beiden Workshops zur Identifikation des schützenswerten Wissens zeigte ein klares Bild bei beiden Unternehmenspartnern. In den Unternehmen herrscht ein einheitliches Verständnis, welches Wissen als sensibel und welches als unkritisch angesehen werden kann. Grundsätzlich galt jedoch stets, die Kritikalität zu hinterfragen. Eine wesentliche Aufgabe der Workshopmoderatoren war es deshalb, ein Verständnis für die Kritikalität und den betriebswirtschaftli-

chen Wertbeitrag des Wissens zu entwickeln. Hierfür diente das VRIN-Framework. Dabei stellte sich heraus, dass nicht jedes Wissenselement grundsätzlich schützenswert ist. Beide Unternehmen schätzten das vorhandene Wissen tendenziell zuerst als schützenswert ein und schwächten ihre Einschätzung im Laufe der Diskussion zum Teil ab, wenn sie erkannten, dass ein oder mehrere der VRIN-Kriterien nicht erfüllt waren. Ein wichtiger Erfolgsfaktor der Diskussion war dabei die Einbindung von fachlichen Experten auf beiden Unternehmensseiten, um die Implikationen der Wissensübertragung offen zu diskutieren.

In den beiden weiteren Workshops wurde den Unternehmen anschließend jeweils die Frage nach den erhofften Potenzialen gestellt. Ziel der Workshops war es herauszufinden, welche Daten des jeweils anderen Projektpartners, für das Unternehmen wertvollen Input bedeuten können. Dabei lag der Fokus vor allem auf potenziellem Wissen zur Kostenreduktion in der Produktion (und damit Effizienzsteigerung) durch eine längere Fräswerkzeugnutzung, als auch der Produkt(weiter-)entwicklung des Fräswerkzeuges durch Erkenntnisse aus der Produktnutzung.

Nachdem die erlangten Erkenntnisse aus den Workshops aufbereitet wurden, trafen sich die Unternehmenspartner zu einem gemeinsamen Konsolidierungsworkshop. Dieser hatte zum Ziel, dass beide Unternehmen im Dialog ein gemeinsames Verständnis über den Austausch der Daten und darin enthaltenen Wissens erlangen. In diesem Rahmen wurde diskutiert, welche Wissenselemente auf Basis der diskutierten Einschätzungen bedenkenlos ausgetauscht werden können und welche Wissenselemente unter Auflagen bzw. welche Elemente nicht ausgetauscht werden sollen. Hierbei stellte sich wiederum die Einbindung der fachlichen Experten als wertvoll für die Diskussion heraus. Es entstand ein umfangreiches Bild, indem die Variablengruppen jedes Unternehmens in Kategorien einsortiert wurden: nicht schützenswerte (z. B. öffentliche) Daten, zum Teil schützenswerte Daten (für den bilateralen, vertrauensvollen Austausch oder Daten, die unter bestimmten Auflagen ausgetauscht werden), und schützenswerte Daten, die nicht ausgetauscht werden. Bei den Workshops stellte sich des Weiteren die situative Abhängigkeit der Bewertung von Potenzialen und Schutzbedarfen durch die beteiligten Unternehmen heraus. Gewisse Daten könnten im Rahmen der üblichen Geschäftstätigkeit beispielsweise als schützenswert und nicht auszutauschen eingeordnet werden. Die Bewertung könnte sich nach einer erneuten Abwägung der Chancen und Risiken allerdings ändern, wenn dadurch etwa eine teure Rückrufaktion vermieden oder eingedämmt werden könnte.

3.3 Ausblick: Schutzmaßnahmen

Im Anschluss an den Workshop verknüpften die Unternehmenspartner jeweils intern ihre Variablen mit den identifizierten Wissenselementen. Als Basis diente dazu die Klassifizierung des Wissens aus den Workshops. Als Ergebnis ist auf beiden Seiten eine Liste mit vorhandenen Variablen und einer Klassifizierung von Variablen, die (unter Auflagen) ausgetauscht werden können, entstanden. Für Variablen deren Austausch bestimmte Auflagen erfüllen muss, soll in den kommenden Schritten die Identifikation von geeigneten Schutzmaßnahmen erfolgen.

4 Ausblick & Handlungsempfehlungen

Dieser Beitrag stellt einen Ansatz zur Identifikation von schützenswertem Wissen in Daten für den unternehmensübergreifenden automatisierten Datenaustausch im Sinne Industrie 4.0 vor, um den berechtigten Produkt- und Know-how Schutz eines jeden Geschäftspartners zu wahren. In den ersten beiden Schritten werden dabei zuerst die verfügbaren Daten in den beteiligten Unternehmen identifiziert sowie das in den betrachteten Prozessen geschäftskritische Wissen erhoben. Im dritten Schritt werden anschließend sowohl Potenziale für den jeweiligen Unternehmenspartner wie auch Schutzbedarfe für das bereitstellende Unternehmen abgeleitet. Das Vorgehensmodell stellt einen Schritt auf dem Weg hin zu einer dynamischen und vernetzten Industrie dar. Insbesondere die Ergebnisse, welche im Rahmen des Anwendungsbeispiels entstanden, haben gezeigt, dass gewisse Produkt- und Produktionsdaten – zumeist nach Aufbereitung von Rohdaten – für den vor- bzw. nachgelagerten Unternehmenspartner durch ein Unternehmen bedenkenlos freigegeben werden und die Wertschöpfung erhöhen können. In diesem Sinne stellt dieser Beitrag einen sogenannten „Enabler“ dar, um die langfristige Vision durchgängig und vollständig vernetzter und virtualisierter Entitäten inner- und außerhalb von Unternehmen entlang von Wertschöpfungsketten und Objektlebenszyklen zu erreichen.

Das Vorgehensmodell muss in weiteren Praxis-Projekten angewendet und mit den resultierenden Erkenntnissen generalisiert und weiterentwickelt werden. Insgesamt herrscht heute noch ein Mangel an Konzepten und Standards, die den unternehmensübergreifenden Datenaustausch im Alltag ermöglichen. Neben Methoden zur Bewertung von Risiken und Potenzialen sind dies insbesondere Konzepte und Anreize welche die Wertschöpfung für alle beteiligten Unternehmen erhöhen. Herausforderungen stellen dabei insbesondere Legacysysteme und die Komplexität moderner Wertschöpfungsnetzwerke dar. Darüber hinaus ist das ökonomische Potenzial bisweilen nicht umfänglich quantifizierbar, bevor man den Datenaustausch erprobt hat und beispielsweise die Qualität von Machine-Learning-Ansätzen auf geteilten Daten demonstrieren kann. Eine integrierte techno-ökonomische Abwägung der Potenziale des unternehmensübergreifenden Datenaustauschs und der damit verbundenen Risiken setzt weitere Untersuchungen von Konzepten und Methoden voraus, die in weiteren Arbeiten angegangen werden sollten.

In Zukunft wird die Nachfrage nach dem Austausch von Daten entlang der Wertschöpfungsketten und die Vernetzung dieser miteinander weiter zunehmen. Dabei sollten Unternehmen nicht grundsätzlich eine protektionistische Haltung einnehmen und dem Austausch von Unternehmensdaten per se absagen, da der Austausch von Daten Wertschöpfungspotenziale verspricht. Hierbei ist darauf zu achten, sich einen Teil des Werts der eigenen Daten zu sichern und nicht unbedarft geschäftskritisches Wissen preiszugeben.

Funding Open Access funding enabled and organized by Projekt DEAL.

Literatur

Bahrs J, Vladova G, Gronau N (2010) Mit Wissensflussmanagement Produktpiraterie unterbinden; Koordinierte Geheimhaltung in Werschöpfungsnetzwerken. ZFO 79:368

Baltuttis D, Häckel B, Oberländer AM, Röglinger M, Seyfried J (2019) Towards effective monetization of the Internet of things—a conceptual model to assess the value of IoT-solutions in an industrial context (Working Paper)

Barney J (1991) Firm resources and sustained competitive advantage. J Manage 17:99–120. https://doi.org/10.1177/014920639101700108

Bauer W, Schlund S, Marrenbach D, Ganschar O (2014) Industrie 4.0 – Volkswirtschaftliches Potenzial für Deutschland. BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien eV, Berlin/Fraunhofer Institut für Arbeitswirtschaft und Organisation IAO, Berlin (Studie)

Bodendorf F (2006) Daten und Wissen. In: Bodendorf F (Hrsg) Daten- und Wissensmanagement. Springer, Berlin, Heidelberg, S 1–5

Bundesministerium für Wirtschaft und Energie (Hrsg) (2019) Das Projekt GAIA-X; Eine vernetzte Dateninfrastruktur als Wiege eines vitalen, europäischen Ökosystems. https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.html. Zugegriffen: 17.11.2020

Emmrich V, Döbele M, Bauernhansl T, Paulus-Rohmer D, Schatz A, Weskamp M (2015) Geschäftsmodell-Innovation durch Industrie 4.0: chancen und Risiken für den Maschinen-und Anlagenbau. Dr. Wieselhuber & Partner, Fraunhofer IPA, München, Stuttgart

General Electric Company, Accenture Plc (2015) Industrial internet insights report for 2015

Gimpel H, Röglinger M (2017) Disruptive Technologien – Blockchain, Deep Learning & Co. Wirtschaftsinformatik Manag 9:8–15

Gronau N (Hrsg) (2011) Handbuch gegen Produktpiraterie; Prävention von Produktpiraterie durch Technologie, Organisation und Wissensflussmanagement. Gito, Berlin

Kelkar O, Heger R, Dao D-K (2014) Studie Industrie 4.0 – Eine Standortbestimmung der Automobil- und Fertigungsindustrie

Otto B, Jürjens J, Schon J, Auer S, Menz N, Wenzel S, Cirullies J (2016) Industrial Data Space; Digitale Souveränität über Daten (www.industrialdataspace.org)

Pommerening K (1991) Datenschutz und Datensicherheit. BI-Wissenschaftsverlag, Mannheim, Wien, Zürich

Rannenberg K (2000) Mehrseitige Sicherheit – Schutz für Unternehmen und ihre Partner im Internet. Wirtschaftsinformatik 42:489–497

Verykios VS, Bertino E, Fovino IN, Provenza LP, Saygin Y, Theodoridis Y (2004) State-of-the-art in privacy preserving data mining. Sigmod Rec 33:50. https://doi.org/10.1145/974121.974131

Vladova G, Bahrs J, Gronau N (2012) Managing knowledge distribution to prevent product imitation and counterfeiting. Int J Intell Inf Technol 8:14–30. https://doi.org/10.4018/jiit.2012040102