Nummer 5

Hrsg. Frank Straube

Philipp Bensel, Markus Richter, Stefan Vogeler

Diffusion von Vertrauen in unternehmens-übergreifenden RFID-Anwendungen

Digitale Schriftenreihe Logistik der Technischen Universität Berlin

Bereich Logistik

Bensel, P.; Richter, M.; Vogeler, S.
Diffusion von Vertrauen in unternehmensübergreifenden RFID-Anwendungen
Nr. 5
Mai 2008

Frank Straube (Hrsg.)
Digitale Schriftenreihe Logistik Technische Universität Berlin
Universitätsverlag der Technischen Universität Berlin

ISSN 1865-5726

© Bereich Logistik Technische Universität Berlin

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

Inhaltsverzeichnis

Inhaltsverzeichnis I
Abbildungsverzeichnis II
1 Ausgangssituation 1
2 Vertrauen - Begriffsfindung und -konkretisierung 1
3 RFID-basiertes SCEM braucht Vertrauen 3
4 Diffusionsmodell 5
5 Zusammenfassung 7
Literaturverzeichnis 8

Abbildungsverzeichnis

Abbildung 1: Charakteristika der Vertrauensbeziehung aus Sicht des Vertrauensgebers 2

Abbildung 2: Diffusionsmodell des Vertrauens in Netzwerken 6

1 Ausgangssituation

In dem dynamischen Umfeld globaler Unternehmensnetzwerke gewinnt die kollaborative Zusammenarbeit zwischen Unternehmen an Bedeutung. Schwerpunkte hierbei bilden die Verbesserung von Planungsverfahren, die Integration von IT-Systemen und der Einsatz von neuen Technologien.[1] Eine dieser Technologien ist die zu den AutoID-Technologien zählende *RFID*[2]-Technologie, die eine große Anzahl von Anwendungsmöglichkeiten ermöglicht. Durch unternehmensübergreifende Implementierung und den unternehmensübergreifenden Datenaustausch kann eine höhere Effizienz der Prozesse und der Koordination erreicht werden. Dabei setzten sich die Beteiligten ungewollt dem Risiko des Datenmissbrauchs aus, dem sie aufgrund der mangelnden Kontrollmöglichkeiten mit Vertrauen entgegentreten müssen.

2 Vertrauen - Begriffsfindung und -konkretisierung

In der Literatur werden grundsätzlich zwei Hauptrichtungen des Phänomens „Vertrauen“ unterschieden. Ökonomisch-rationale, insbesondere spieltheoretische Ansätze betrachten Vertrauen als Phänomen sichtbaren kooperativen Verhaltens.[3] Soziologische und psychologische Ansätze verstehen Vertrauen hingegen primär als subjektive Erwartungshaltung. Im Folgenden soll die Definition von RIPPERGER (1998) verwendet werden. RIPPERGER (1998) betrachtet Vertrauen aus einer funktionalen Sichtweise als „Mechanismus zur Stabilisierung unsicherer Erwartungen und zur Verringerung der damit einhergehenden Komplexität menschlichen Handelns“.[4]

Vertrauen ist notwendig zur Koordination von Akteuren in Situationen mit herrschenden endogenen Risiken und fehlender Situationskontrolle.[5] Dabei liegen dem Vertrauensgeber Informationen über das Verhalten der Vertrauensnehmer nicht oder nur zu prohibitiv hohen Kosten vor.[6] Im Falle der kollaborativen Zusammenarbeit sind dies meist Informationen über den Umgang mit sensiblen Daten, der nur zu prohibitiv hohen Kosten kontrollierbar wäre. Aufgrund der unsicheren Situation muss der Vertrauensgeber in Erwartung eines positiven Ergebnisses mit dem Vertrauensvorschuss in Vorleistung gehen, womit die Vertrauensbeziehung einen reziproken Charakter erhält.[7]

Der Vertrauensgeber als rational handelnder Akteur wägt die ökonomischen Konsequenzen, die durch opportunistisches Verhalten des Vertrauensnehmers entstehen können, im Vorfeld der Handlung ab. Der durch Missbrauch entstehende Schaden kann den erwarteten Nutzen weit übertreffen.[8] Der Vertrauensnehmer wird als vertrauenswürdig betrachtet, wenn der erwartete Nutzen des Handlungsergebnisses stark positiv von der Norm abweicht, und opportunistisches Verhalten seinerseits ausgeschlossen werden kann. [9]

Vertrauenswürdigkeit wird im diesem Kontext hauptsächlich durch die drei Charakteristika Reputation, Commitment und Bereitschaft zur

[1] Vgl. Straube et al. (2005), S. 19.
[2] *Radio Frequency Identification Technology.*
[3] Vgl. Ripperger, T. (1998), S. 6.
[4] Ripperger (1998), S. 9.
[5] Vgl. Baumgarten, H.; Krystek, U.; Richter, M. (2004), S. 116.
[6] Vgl. Pelzmann, L. (2004), S. 208
[7] Vgl. Baumgarten, H.; Krystek, U.; Richter, M. (2004), S. 116.
[8] Vgl. Yang, G.; Jarvenpaa, S. L. (2005), S. 5
[9] Vgl. Pieper, J. (2000), S. 37 f.; Vgl. Baumgarten, H.; Krystek, U.; Richter, M. (2004), S. 116.

Informationsweitergabe bestimmt.[10] Die Reputation ist ein Annahmebündel über Ruf und Ansehen, die der Vertrauensnehmer bezüglich seiner Bereitschaft und Fähigkeit zum Aufbau und zur Erhaltung einer Vertrauensbeziehung besitzt.[11] Sie wird in der Vertrauensbeziehung zu einem immateriellen Pfand, da bei Vertrauensbruch die Zerstörung der Reputation droht. Commitment ist eine wechselseitige Abhängigkeit der Akteure durch gegenseitige Verpflichtung, z. B. durch das Tätigen einer Investition in ein spezifisches System. Durch Commitment entstehen Wechselkosten, die die Bindung durch die Glaubhaftigkeit des Vertrauensnehmers stabilisieren.[12] Die Bereitschaft zur Weitergabe von Informationen steht in wechselseitiger Beziehung zum Vertrauenskonstrukt, da sie einerseits eine Determinante des Vertrauensaufbaus ist und andererseits die Bereitschaft das gegenseitige Vertrauen voraussetzt. Abbildung 2 zeigt die Charakteristika der Vertrauensbeziehung aus Sicht des Vertrauensgebers.

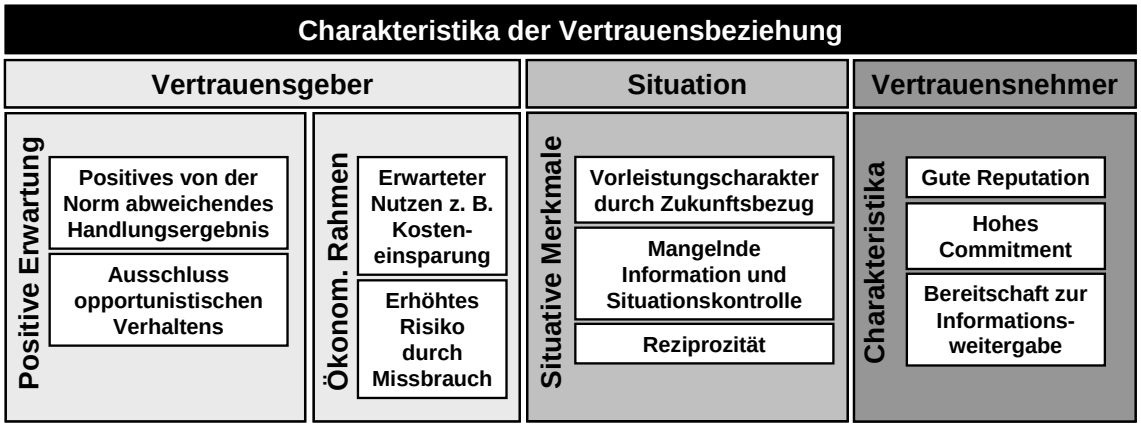

Abbildung 1: Charakteristika der Vertrauensbeziehung aus Sicht des Vertrauensgebers

Der Vertrauensaufbau zwischen Vertrauensgeber und Vertrauensnehmer stellt sich somit als iterativer Prozess dar, der auf Erfahrungswerten aus vergangenen sowie anhaltenden (Geschäfts-) Beziehungen und damit der Vorhersagbarkeit des Verhaltens eines Partners aufbaut. Diese Art des Vertrauensaufbaus basiert auf bilateralen existierenden Beziehungen und wird als „expirienced“ oder „knowledge based trust“ bezeichnet.[13] Nach PELZMANN (2004) bestimmen die Determinanten „Dauer der Geschäftsbeziehung mit einem Partner“, „Legitimation der Verhandlungspartner“ und „Spielregeln“ über den Erfolg oder Misserfolg der Entstehung von Vertrauen.[14] Im Rahmen zeitlich begrenzter Beziehungen oder extremer Machtasymmetrien ist demnach eher mit opportunistischem Verhalten zu rechnen, als bei andauernden Geschäftsbeziehungen oder ausbalancierten Machtverhältnissen. Können Partner frei verhandeln und sind nicht an ein bestimmtes Ergebnis gebunden, steigt die Bereitschaft in Vertrauen zu investieren. Einfache Spielregeln fördern den Aufbau von Vertrauen, insbesondere wenn klar geregelt wird, welche Sanktionen im Falle eines Missbrauchs greifen.[15]

[10] Vgl. Pieper, J. (2000), S. 139.
[11] Vgl. Pieper, J. (2000), S. 141 ff.
[12] Vgl. Pieper, J. (2000), S. 151 ff.
[13] Yang, G.; Jarvenpaa, S. L. (2005), S. 6
[14] Pelzmann, L. (2004), S. 210
[15] Vgl. Pelzmann, L. (2004), S.212f

3 RFID-basiertes SCEM braucht Vertrauen

RFID-Systeme können nach ihrer Reichweite in lokal oder kollaborativ geschlossene und global offene Systeme unterteilt werden.[16] Das SCEM in einer unternehmensübergreifenden Ausbaustufe kann den kollaborativ geschlossenen Systemen zugeordnet werden. Ziel des SCEM ist die Schaffung von unternehmensübergreifenden Visibilität und Transparenz. Visiblität ist dann gegeben, wenn einem Entscheider zum Zeitpunkt der Entscheidung alle relevanten Daten vorliegen.[17] Es ist die Aufgabe des Supply Chain Event Managements aus Verlaufsdaten über den Wertschöpfungsprozesses entscheidungsrelevante Informationen für die Koordination bei Planungsabweichungen zu generieren, in der Erwartung Folgekosten und Reibungsverluste der Koordination zu minimieren. Dabei sind sowohl die Qualität und die Granularität der Daten als auch die Echtzeitfähigkeit des Systems von Bedeutung.[18] Eine höhere Datenqualität und -granularität in Echtzeit kann durch den Einsatz von RFID erreicht werden.

Grundsätzlich wird zwischen einer Datenspeicherung auf dem RFID-Chip (Data-on-Tag) selbst oder in einer zentralen oder dezentralen Datenbank (Data-on-Network) unterschieden. Bei beiden Varianten muss der Missbrauch durch unbefugte Parteien, z.B. Konkurrenten, mit Sicherungsmaßnahmen, z.B. der Kryptologie, verhindert werden.

Ein SCEM-System kann in die Funktionen Datenerhebung, Datenanalyse und -bewertung und die Aufarbeitung und Auswertung unterteilt werden.[19] Bei der Datenerhebung werden Ist-Daten über den Prozessverlauf erhoben, die in der Analyse mit Planungsdaten verglichen werden. Im Falle von Abweichung werden in der Auswertungsphase auf vordefinierten Eskalationspfaden anhand von Kontextinformationen Handlungsempfehlungen generiert. Die dazu benötigten Daten müssen bei unternehmensübergreifenden Entscheidungen von den Partnern zur Verfügung gestellt werden. Dabei setzten sich die Partner zum einem dem Risiko aus, dass eigene Prozessdefizite durch den Einsatz von SCEM-Systemen offengelegt werden.[20] Zum anderen kann es sich bei den benötigten Daten um wettbewerbsrelevante Daten, z.B. Einkaufspreise, handeln, deren Missbrauch durch opportunistisches Verhalten schwerwiegende Folgen hätte. Daher setzt die Einführung eines SCEM-Systems weitgehendes Vertrauen in die beteiligten Partner voraus. Kooperationswillige Partner müssen sich durch eine gute Reputation, z.B. durch erfolgreiche Zusammenarbeit in der Vergangenheit, und Commitment, hier der Aufbau des RFID-Systems, profilieren, um glaubwürdig Vertrauenswürdigkeit zu signalisieren.

Die Einführung eines RFID-basierten SCEM-Systems kann nach Yang et al. als „kollektive Handlung“ aufgefasst werden.[21] Es ist im Interesse der Akteure möglichst viele Lieferstufen in das System zu integrieren, da der Nutzen des Systems durch Netzwerkeffekte mit zunehmender Teilnehmerzahl steigt.[22]. Zudem ist auch der Umfang der Datenbasis abhängig von der Anzahl der partizipierenden Akteure. Aus diesem Kontext heraus ist die Betrachtung von

[16] Vgl. Strassner, M. (2005), S. 126
[17] Vgl. Otto, A. (2003), S. 3 f.
[18] Vgl. Dittmann, L. (2006), S. 23.
[19] Vgl. Schmidt, D. (2006), S. 23 f.
[20] Bretzke et al. (2002), S. 26.
[21] Vgl. Yang, G.; Jarvenpaa, S. L. (2005), S. 1.
[22] Vgl. Shapiro, C.; Varian, H. R. (1999), S. 179 ff.

Einzelbeziehungen unzureichend und es muss auf die Untersuchung von Netzwerken übergegangen werden. Das fallweise Fehlen von direkten Geschäftsbeziehungen der Partner verschiedener Wertschöpfungsstufen untereinander verhindert dabei die Generierung von bilateralem Vertrauen. Hieraus resultieren Unsicherheiten zumal die einzelnen Unternehmen einer logistischen Kette unterschiedliche Zielstellungen und Erwartungen mit der Technologie verbinden. Dadurch ist die Erzeugung einer Vertrauensatmosphäre eine unumgängliche Bedingung für den Erfolg eines wertschöpfungskettenweiten SCEM. Zur Minimierung des Investitionsrisikos sollte der Aufbau eines SCEM-Systems innerhalb eines Netzwerkes stufenweise realisiert werden.[23] Mit einem stufenweisen Vorgehen kann zudem ein kontrollierter Aufbau von Reputation und Commitment durch die Partner erfolgen. Im Folgenden soll ein Diffusionsmodell bezüglich der Integrationstiefe eines SCEM mit dem Ziel einer übergreifenden Vertrauensatmosphäre vorgestellt werden.

[23] Vgl. Strassner, M.; Fleisch, E. (2005), S. 45.

4 Diffusionsmodell

Ein Netzwerk besteht aus Akteuren unterschiedlicher Lieferstufen, die untereinander bilateral durch Waren-, Informations- und Finanzströme verknüpft sind. Durch die wiederholte Abwicklung der Geschäftsbeziehung kann durch die Bestätigung der positiven Erwartungen an die Beziehung zwischen den einzelnen Akteuren Vertrauen entstehen. Dieses Vertrauen ist jedoch bilateraler Natur und führt daher nicht zwangsläufig zu einer übergreifenden „Vertrauensatmosphäre" im gesamten Netzwerk. Eine „Vertrauensatmosphäre" besteht in einem sozialen System, wenn für die in diesem System eingegangenen Vertrauensbeziehungen opportunistisches Verhalten mit großer Wahrscheinlichkeit ausgeschlossen werden kann. Die Vertrauensatmosphäre hat Einfluss auf die Erwartungsbildung eines potenziellen Vertrauensgebers, indem er die Erfahrung Dritter aus vergangenen Transaktionen innerhalb des sozialen Netzes auf den potenziellen Vertrauensnehmer extrapoliert.[24]

Ein Diffusionsmodell versucht die Verbreitung eines Phänomens ausgehend von einer Einzelerscheinung zu erklären. Das hier vorgestellte Diffusionsmodell zur Entstehung einer Vertrauensatmosphäre versucht im Kontext eines SCEM die Entstehung einer allgemeinen Vertrauensatmosphäre ausgehend von einer bestehenden bilateralen Vertrauensbeziehung herzuleiten.

Bei der Etablierung innovativer Konzepte sind „Promotoren" von herausragender Bedeutung. Unter Promotoren werden Personen/ Organisationen verstanden, „die einen Innovationsprozess aktiv und intensiv fördern".[25] Im SC-Umfeld treten meist fokale Unternehmen als „Machtpromotoren" auf, die durch „hierarchisches Potenzial"[26] die Rolle eines Promotors ausfüllen können. Bei der Einführung von RFID im Handel tritt z. B. die Metro Group als Machtpromotor auf, indem sie ihren Lieferanten die Einführung von RFID vorschreibt. Die Beziehungen der Promotoren zu ihren direkten Netzwerkpartnern werden den Ausgangspunkt der Beschreibung des Diffusionsmodells bilden. Als Beispiel soll hier die Automobilindustrie dienen, in der die Automobilhersteller als fokale Unternehmen angesehen werden können.[27]

Die wichtigsten Lieferanten der OEM sind die System- und Modullieferanten auf der ersten Zulieferstufe, zu denen meist langfristige und vertrauensvolle Beziehungen gepflegt werden. Um die Koordination der Partner untereinander zu optimieren eignet sich die Intensivierung des Datenaustausches im Zuge der Implementierung eines unternehmensübergreifenden SCEM (Commitment). Durch einen vertrauensvollen, nicht opportunistischen Umgang mit dem Partner können beide Unternehmen ihre Reputation auch nach außen hin stärken.

In der zweiten Phase des Modells hilft die aufgebaute Reputation neue Partner für das SCEM-System zu gewinnen. Hierfür kommen vornehmlich direkte Lieferanten und Kunden der bereits partizipierenden Akteure in Frage, da mit diesen oftmals bereits Informationsaustausch, z.B. in Form von Prognosedaten, besteht. Die zu diesem Zeitpunkt akquirierten Partner haben zu mindestens einem der ursprünglichen Partner nur eine indirekte Beziehung, wodurch die Bildung bilateralen Vertrauens erschwert wird. Die potenziellen Partner treffen ihre Partizipationsentscheidung auf Grundlage der guten Erfahrung mit ihren direkten

[24] Vgl. Ripperger, T. (1998), S. 99.
[25] Witte, E. (1999), S. 15.
[26] Witte, E. (1999), S. 16.
[27] Vgl. Pieper, J. (2000), S. 122 ff.

Partnern und der Reputation der indirekten Partner. Dies kann als erste Entwicklungsstufe einer Vertrauensatmosphäre oder auch als „Vertrauenskette“ angesehen werden.

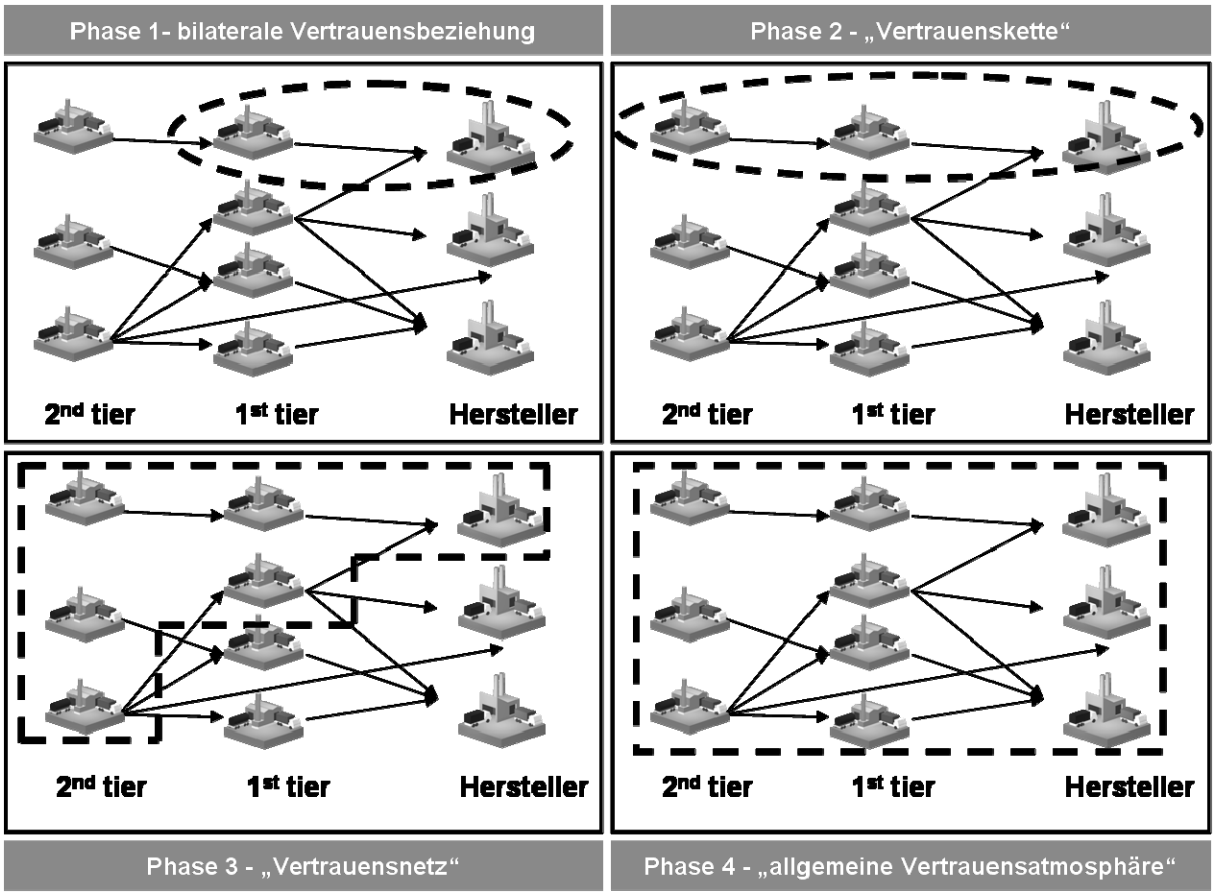

Abbildung 2: Diffusionsmodell des Vertrauens in Netzwerken

Der Ausbau des Teilnehmerkreises (Phase 3) läuft dann analog zur Phase 2 ab, bis entweder alle Zulieferer eines OEM partizipieren oder die wirtschaftlichen Grenzen des Systems erreicht sind. Am Ende dieser Entwicklung deckt das System das Lieferantennetzwerk eines OEM bis an die wirtschaftliche Grenze ab. Sind mehrere OEMs in einem Netzwerk beteiligt kann es beim Aufbau von separaten Systemen aufgrund der Konkurrenzsituation zu Problemen führen. Daher müssen bei einer horizontalen Erweiterung eines SCEM-Systems Maßnahmen gefunden werden die den Missbrauch von Informationen ausschließen. Dies könnte z.B. durch Integration eines neutralen Intermediärs als Betreiber des SCEM realisiert werden. Werden solche Maßnahmen erfolgreich implementiert, kann auch unter Konkurrenten Vertrauen entstehen (Phase 4). Dies führt zur Ausbildung einer Vertrauensatmosphäre, indem die Erfahrung Dritter, hier der Lieferanten, aus vergangenen Transaktionen innerhalb des sozialen Netzes auf den potenziellen Vertrauensnehmer, hier konkurrierende OEMs, extrapoliert werden.

5 Zusammenfassung

Vertrauen ist in Wertschöpfungspartnerschaften immer dann nötig, wenn das Verhalten des Partners nicht oder nur zu prohibitiv hohen Kosten kontrolliert werden kann. Vertrauensvolle Partner zeichnen sich aus durch Commitment, Reputation und die Bereitschaft zur Weitergabe von Information. Im Zuge einer Implementierung eines SCEM-Systems wird Commitment in Form der RFID-Technologie und Reputation, durch uneigennützige Verwendung der preisgegebenen Daten, aufgebaut. Durch eine stufenweise Einführung kann das Investitionsrisiko verringert und der Reputationsaufbau kontrolliert vorangetrieben werden. Durch die Übertragung guter Reputation von direkten Partnern auf deren Partner kann eine Vertrauensatmosphäre entstehen. Noch zu klären ist welche Mechanismen die Teilnahme konkurrierender Unternehmen in einem SCEM-System ermöglichen und regulieren können.

Literaturverzeichnis

Baumgarten, H.; Krystek, U.; Richter, M. (2004):

„Vertrauensbasiertes Controlling für die Supply Chain Collaboration"; in: Wolf-Kluthausen, H. (Hrsg.), Jahrbuch Logistik 2004, free beratung GmbH, Korschenbroich 2004, S. 114-121.

Bretzke, W.-R., Stölzle, W., Karrer, M., Ploenes, P. (2002):

Vom Tracking & Tracing zum Supply Chain Event Management – Aktueller Stand und Trends; KPMG Consulting AG; 2002

Dittmann, L. (2006):

Der angemessene Grad an Visibilität in Logistik-Netzwerken, Deutscher Universitäts-Verlag, Wiebaden 2005

Kuhn, A.; Hellingrath, H. (2002):

Supply Chain Management – Optimierte Zusammenarbeit in der Wertschöpfungskette, Springer, Berlin et al. 2002

Otto, A. (2003):

„Supply Chain Event Management: Three Perspectives"; in: International Journal of Logistics Management, Nr. 2, 14. Jg., S. 1-13

Pelzmann L. (2004):

Vertrauen in Geschäftsbeziehungen. In: M. Held, G. Kubon-Gilke, R. Sturn (Hrsg.): Normative und institutionelle Grundfragen der Ökonomik (Jahrbuch 4: Reputation und Vertrauen), Metropolis, Marburg 2004, S. 207-229

Pieper, J. (2000):

Vertrauen in Wertschöpfungspartnerschaften – Eine Analyse aus der Sicht der Neuen Institutionenökonomie, Gabler, Wiesbaden 2000

Ripperger, T. (1998):

Ökonomik des Vertrauens : Analyse eines Organisationsprinzips, Mohr, Tübingen 1998

Schmidt, D. (2006):

RFID im Mobile Supply Chain Event Management, Gabler, Wiesbaden 2006

Schneider, S. (2003):

Elektronische Verträge und Vertrauen im Internet, Denk! Institut Verlag, Wiesbaden 2003

Shapiro, C.; Varian, H. R. (1999):

Information rules - a strategic guide to the network economy, Harvard Business School Press, Boston (MASS) 1999

Strassner, M. (2005):

RFID im Supply Chain Management, Deutscher Universitäts-Verlag, Wiebaden 2005

Strassner, M.; Fleisch, E. (2005):

„Innovationspotenzial von RFID für das Supply Chain Management"; in: Wirtschaftsinformatik, Nr. 1, 47. Jg., S. 45-54.

Straube et al. (2005):

Trends und Strategien in der Logistik – Ein Blick auf die Agenda des Logistik-Manaements 2010, Deutscher Verkehrs-Verlag, Hamburg 2005

Wiesenfeld et al. (1998):

Communication Patterns as Determants of Organizational Identification in a virtual Organization, Journal of Computer-Mediated Communication, 3. Jg., Heft 4. S. 1-22

Witte, E. (1999):

„Das Promotoren-Modell"; in: Hauschildt, J.; Gemünden, G. (Hrsg.): Promotoren, 2. Auflage, Gabler, Wiesbaden 1999, S. 11-41.

Yang, G.; Jarvenpaa, S. L. (2005):

Trust and Radio Frequency Identification (RFID) Adoption within an Alliance; IEEE: Proceedings of the 38th Hawaii International Conference on System Science - 2005