September 2003

IT-Risikomanagement in dynamischen und flexiblen Wertschöpfungsnetzwerken

Peter Laing
Forschungsinstitut für Rationalisierung (FIR e.V.) an der RWTH Aachen

Tomaso Forzi
Forschungsinstitut für Rationalisierung (FIR e.V.) an der RWTH Aachen, Forzi@fir.rwth-aachen.de

In: Uhr, Wolfgang, Esswein, Werner & Schoop, Eric (Hg.) 2003. *Wirtschaftsinformatik 2003: Medien - Märkte - Mobilität*, 2 Bde. Heidelberg: Physica-Verlag

ISBN: 3-7908-0111-9 (Band 1)
ISBN: 3-7908-0116-X (Band 2)

IT-Risikomanagement in dynamischen und flexiblen Wertschöpfungsnetzwerken

Peter Laing, Tomaso Forzi

Forschungsinstitut für Rationalsierung (FIR e.V.) an der RWTH Aachen

Zusammenfassung: Wertschöpfungsprozesse werden vermehrt betriebsübergreifend in einem dynamischen Umfeld durchgeführt. Eine überbetriebliche Wertschöpfung bietet jedoch nicht nur viele Vorteile wie mehr Flexibilität, sondern ist auch mit zahlreichen Netzwerkrisiken verbunden. Neben Schwierigkeiten, das Verhalten von Netzwerkpartnern vorherzusagen oder zu lenken, sind auch IT-Sicherheitslücken beim Austausch von Informationen und elektronischen Dokumenten als Bedrohung in Betracht zu ziehen. Unternehmen, deren Geschäftsmodell auf die Unterstützung zwischenbetrieblicher Informationsflüsse zielt, auch Informationsintermediäre genannt, müssen nicht nur ein kundenorientiertes Geschäftsmodell entwickeln, sondern auch IT-Risiken sicher erfassen und beherrschen, um vom Markt akzeptiert zu werden. Im Rahmen dieses Beitrags wird ein Risikomanagementansatz zur Erfassung und Bewältigung sowie für das Controlling von IT-Risiken in (dynamischen) Unternehmensnetzwerken vorgestellt.

Schlüsselworte: Risikomanagement, IT-Sicherheit, Geschäftsmodelle, Wertschöpfungsnetzwerke

1 Dynamische Wertschöpfungsnetzwerke

Der Austausch von Gütern und Dienstleistungen wird zunehmend durch den Einsatz neuer Technologien und Standards unterstützt, so dass die Transaktionskosten sinken und die Dynamik des überbetrieblichen Handels deutlich zunimmt – im Unternehmensumfeld entstehen neue Chancen wie auch Risiken (vgl. [Luc+02a] [Pic+01] [Wirt00]). Geschäftsfelder ändern sich schneller als in der Vergangenheit, neue Kommunikationstechnologien und –standards führen zu dynamischeren Kunden-Lieferanten-Beziehungen und der stetig steigende Wettbewerb zwingt Unternehmen, sich mehr und mehr auf die eigenen Kernkompetenzen zu konzentrieren [AfTu01] [Bens97] [BrKa00] [HaSi99] [Klein95] [Pic+01] [Port01] [Scho00] [Timm00] [Wirt00]. Sofern Unternehmen Zwischenprodukte und Dienstleistungen dauerhaft zu niedrigeren Kosten beschaffen als intern herstellen bzw. erbringen können, so sind Outsourcing-Entscheidungen und ein verstärktes Engagement in Unternehmensnetzwerken eine häufige Folge; die Unternehmens-

grenzen verändern sich aufgrund sinkender Transaktionskosten [Coas37] [Pic+01] [Will75]. Weiterhin zwingen der Wettbewerb sowie der technische Fortschritt Unternehmen, kontinuierlich innovative Produkte und Dienstleistungen zu entwickeln und neue Geschäftsfelder zu erschließen [EvWu00] [HaSi99] [Krcm00] [Teub99].

Derzeit lässt sich, nachdem im vergangenen Jahrzehnt die Optimierung innerbetrieblicher Abläufe im Vordergrund stand, eine zunehmende Verbesserung unternehmensübergreifender Geschäftsprozesse beobachten [Pic+01]. Unternehmen nutzen mehr und mehr das Internet, um sich zu vernetzen. Insbesondere die Einführung von Standards (z.B. eCl@ss; BMEcat oder das altbekannte EDIFACT) schafft dabei eine wesentliche Voraussetzung, um Daten und Informationen schnell und einfach auszutauschen, so dass Wertschöpfungsaktivitäten zukünftig vermehrt in *dynamischen* Unternehmensnetzwerken erfolgen können [Paro99]; vgl. Abbildung 1 [FoLu02]. Internet-Intermediäre, die den überbetrieblichen Vernetzungsprozess durch die Entwicklung und Pflege einheitlicher Datenaustauschformate sowie geeigneter Dienstleistungen unterstützen, haben dabei eine wichtige Rolle [Luc+02b].

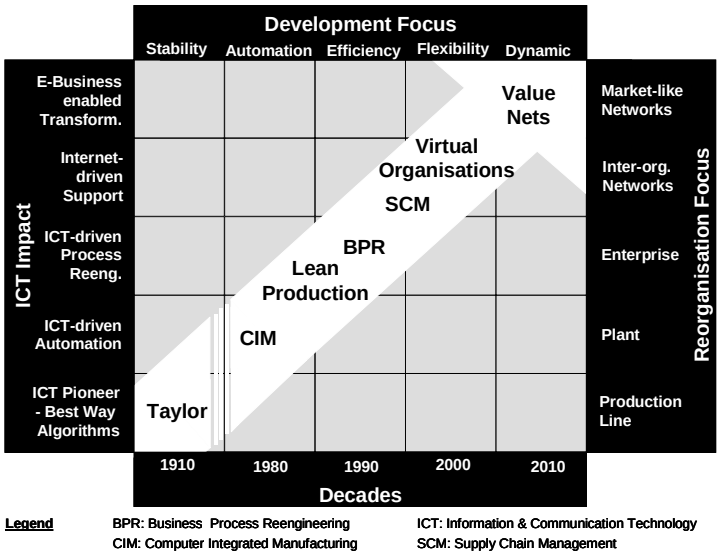

Abbildung 1: Die Entwicklung hin zu dynamischen Unternehmensnetzwerken (Value Nets)

Anwender akzeptieren nur dann einen elektronischen Austausch betrieblich relevanter Daten, wenn ihre Sicherheitsanforderungen ernst genommen und berücksichtigt werden (vgl. z.B. [Ecke01] [Pohl96] [Rann98b]). Falls Informationen bzw. Dokumente mit vertraulichen Inhalten in vernetzten Strukturen verschickt werden, so ist ein Sicherheitsmaß zu gewährleisten, das einerseits den Schutzbedürfnissen der Anwender Rechnung trägt und andererseits weder die eigentlichen Geschäftsprozesse behindert noch unnötig hohe Kosten verursacht. Internet-

Intermediäre müssen, um erfolgreich zu sein, ein vom Markt akzeptiertes Geschäftsmodell ableiten und gleichzeitig über ein tragfähiges IT-Risikomanagement verfügen.

2 Geschäftsmodelle in vernetzten Wertschöpfungsstrukturen

2.1 Beschreibung von Geschäftsmodellen

In der Literatur wird der Begriff „Geschäftsmodell“ unterschiedlich verwendet und beschrieben (z.B. [AfTu01] [FoLa03] [OsPi02] [Port01] [ReKl01] [Timm00] [WiKl00]). Ein Geschäftsmodell ist, allgemein ausgedrückt, die Darstellung externer Leistungs- und Informationsflüsse, um *Nutzen*beziehungen zwischen den beteiligten Akteuren – das sind z.B. Kunden, Wertschöpfungspartner, Investoren oder Gläubiger – transparent zu machen. Weiterhin ist ein Geschäftsmodell ein wesentlicher Ausgangspunkt der Unternehmensentwicklung, so dass die Beschreibung nicht nur ein hohes Abstraktionsniveau zur externen Kommunikation haben sollte, sondern gleichzeitig so aufbereitet und strukturiert sein muss, dass organisatorische Maßnahmen abgeleitet werden können. Ein Geschäftsmodell kann jedoch erst dann Basis der Organisationsentwicklung sein, wenn auch eine passende Unternehmensstrategie vorliegt bzw. abgeleitet wird.

Ein Hauptziel jeder Unternehmung ist die langfristige Steigerung des Unternehmens(mehr)wertes durch eine nachhaltige Gewinnerzielung bzw. angemessene Verzinsung des eingesetzten (Eigen-)Kapitals (vgl. z.B. [Hint97] [Port85] [Port01]). Die unternehmerische Strategie definiert, *wie* dieses Ziel zu erreichen ist und *welche* Vorraussetzungen erfüllt sein müssen. Klare Wettbewerbsvorteile, eine effektive Wertschöpfungskette, eine Kontinuität der Unternehmensausrichtung und schließlich eine nachhaltige Rentabilität kennzeichnen eine erfolgreiche strategische Unternehmenspositionierung (vgl. [Port85]).

Die Beschreibung bzw. Strukturierung eines Geschäftsmodells kann durch die fundierte Bildung sogenannter Partialmodelle, die wiederum betriebswirtschaftliche Teilanalysen eines Unternehmens ermöglichen, erfolgen [AfTu01] [Wirt00]; vgl. auch Abbildung 2 [LaFo01]. Relevante Teilmodelle sind (1) das *Marktmodell* (Kunden wie auch potentielle Wettbewerber), (2) das *Leistungsmodell* (Befriedigung von Kundenbedürfnissen durch geeignete Produkte und Dienstleistungen), (3) das *Preis-Umsatzmodell* (fundierte Beschreibung und Schätzung von Einnahmenarten und -höhen sowie deren Preiselastizität), (4) das *Leistungserbringungsmodell* (Produktionssystematik für das Produkt- bzw. Dienstleistungsportfolio), (5) das *Netzwerk- und Informationsmodell* (Konfiguration überbetrieblicher Wertschöpfungsstrukturen und Darstellung der Leistungs- und Informati-

onsflüsse) und (6) das *Finanzierungsmodell* (Kapitalbedarf; potentielle Kapitalgeber; Risikobewertung der erwarteten Profite). Diese Einteilung in Partialmodelle ist allgemein gültig und eignet sich sowohl für die Beschreibung traditioneller (z.B. Maschinen- und Anlagenbau) als auch neuer bzw. Internet-gestützter Geschäftsmodelle (z.B. Informationsintermediäre).

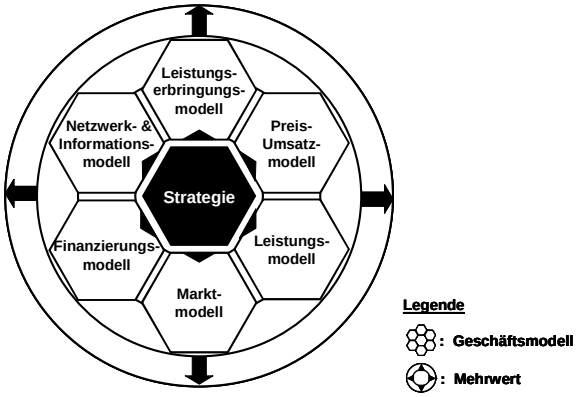

Abbildung 2: Strategie, Geschäftsmodell und Mehrwert

IT-Sicherheit bildet kein eigenes Partialmodell, da die Entwicklung und Umsetzung eines Sicherheitskonzeptes nicht direkt Wert schöpfend ist. Die Realisierung eines allgemein akzeptierten Sicherheitsniveau ist jedoch bei Internet-Geschäftsmodellen ein zentraler und oft auch wettbewerbsentscheidender Erfolgsfaktor; die Akzeptanz eines Internet-Dienstes hängt häufig vom Vertrauen der Anwender ab. IT-Risiken müssen somit gemanagt, d.h. erfasst, bewertet und bewältigt werden, indem ein geeignetes IT-Sicherheitskonzept implementiert wird. Externe wie auch interne Angriffe müssen erfolgreich abgewehrt werden, die Beweisbarkeit elektronischer Transaktionen ist z.B. durch den Einsatz digitaler Signaturen sicherzustellen, und neben technischen müssen auch organisatorische sowie personenbezogene Sicherheitsvorkehrungen getroffen werden. IT-Sicherheit ist bei Informationsintermediären, anders als in der traditionellen Industrie, ein Querschnittsthema, das *alle* Partialmodelle betrifft. Bei Unternehmen der „Old Economy“ können IT-Sicherheit und IT-Risikomanagement dem Partialmodell *„Netzwerk und Information“* zugeordnet werden.

2.2 Methodische Geschäftsmodellierung

Die Folgen einer übereilten und lediglich auf Kreativitätstechniken beruhenden Geschäftsmodelldefinition konnten in der “dot.com”-Krise Ende 2000 gut beobachtet werden [AfTu01] [EvWu00] [Port01] [ReKl01] [Timm00] [WiKl00]. Eine Vielzahl zuvor gefeierter und mit reichlich Kapital ausgestatteter Unternehmen war nicht in der Lage, eine akzeptable Rendite oder überhaupt Gewinne zu erzie-

len [FoLu02], so dass eine größere Marktbereinigung in der „New Economy“ folgte.

Unternehmen müssen sich aufgrund der Globalisierung des Wettbewerbs und der steigenden Markttransparenz und –dynamik auf Preiskämpfe einstellen oder mit neuen und schwer zu kopierenden Produkten und Dienstleistungen die Bedürfnisse der Kunden befriedigen [Bala96] [Webb+00]. Eine besondere Herausforderung ist dabei, dauerhafte Wettbewerbsvorteile zu schaffen und ein tragfähiges Geschäftsmodell zu entwickeln bzw. ein existierendes anzupassen. Eine fehlende methodische Unterstützung dieser komplexen Aufgabe motivierte das Forschungsinstitut für Rationalisierung (FIR), eine Vorgehensweise zur *kundennutzen-*, *zielkosten-* und *netzwerk*orientierten Geschäftsmodellierung zu entwickeln: das „House of Value Creation“ (HVC); vgl. Abbildung 3 [LaFo01].

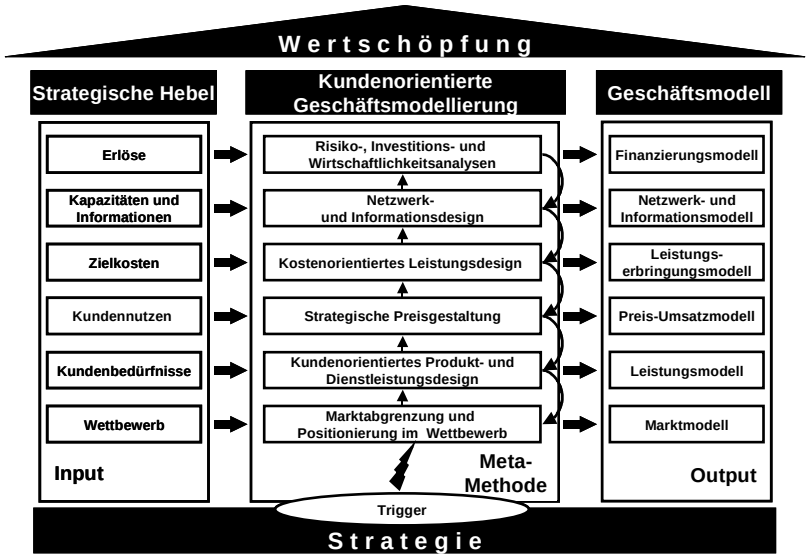

Abbildung 3: Das “House of Value Creation”

Das HVC ist eine Meta-Methode und besteht aus drei logischen Säulen (Input, Methodeneinsatz, Output) und sechs Prozessschichten (jede Schicht erfordert den Einsatz ausgewählter Methoden). Der Informationsfluss im HVC verläuft grundsätzlich von links nach rechts (Input – Methode- Output) und von unten nach oben.

Ausgangspunkt der Geschäftsmodellierung sind u.a. neue Ideen, technische Innovationen oder gravierende Veränderungen wirtschaftlicher Rahmenbedingungen (z.B. Öffnung der Energie- und Telekommunikationsmärkte). Bevor die bereits vorgestellten Partialmodelle im Einzelnen gestaltet werden, ist in einem vorgelagerten Methodenschritt zunächst die Strategie zu überprüfen und ggf. zu adaptieren. Wenn alle sechs Ebenen bzw. Schichten des HVC erfolgreich durchlaufen

wurden – ggf. nach einer oder mehreren Iterationen – kann das übergeordnete Ziel einer nachhaltigen Wertschöpfung erreicht werden; vgl. Abbildung 3. Die einzelnen Methodenschritte sind:

1. Marktabgrenzung und Positionierung: Zunächst ist festzulegen, mit welchen Produkt- und/oder Dienstleistungsarten Kundenbedürfnisse befriedigt werden sollen. Die Festlegung auf bestimmte Produktarten hat dabei weitreichende Folgen. So sind beispielsweise die Produkte „Automobil" und „individuelle Mobilität" substantiell verschieden. Die eigentliche Marktabgrenzung und die Positionierung im Wettbewerb können nach einer Analyse aller relevanten Marktteilnehmer (Lieferanten, Kunden und potenzielle Wettbewerber) durchgeführt werden. Dabei sollten auch Branchenrentabilität und -rivalität berücksichtigt werden. *Ergebnis:* Marktabgrenzung (z.B. nach Produktkategorie oder geographischen Gesichtspunkten) und Kurzprofil wichtiger Marktteilnehmer (Nachfrager und Wettbewerber).

2. Kundenorientiertes Produkt- und Dienstleistungsdesign: Nachdem Märkte definiert und wichtige Kunden(gruppen) sowie Wettbewerber identifiziert sind, sind beim Produkt- und Dienstleistungsentwurf die Kundenbedürfnisse in den Mittelpunkt zu stellen. Eine bewährte Methode zur kundenorientierten Produktgestaltung ist das „Quality Function Deployment" (QFD) [Akao90]. *Ergebnis:* Portfolio Kundennutzen maximierender Produkte und Dienstleistungen.

3. Strategische Preisgestaltung: Bei der strategischen Preiskalkulation ist sowohl vom bewerteten (monetären) Kundennutzen – das ist gleichzeitig die natürliche Preisobergrenze – als auch vom Wettbewerb – eine ebenfalls Preis limitierende Größe – auszugehen. Ein rein kostenorientierter Ansatz birgt die Gefahr, sich entweder durch überhöhte Preise „aus dem Markt zu rechnen" oder durch unnötig niedrige Preise auf potenzielle Erlöse zu verzichten [KiMa00]. Je nach Anwendungskontext ist zusätzlich eine Aufteilung zwischen Transaktions- und Grundgebühren erforderlich. *Ergebnis:* Preismodelle und Preiselastizitäten.

4. Zielkostenorientiertes Leistungserbringungsdesign: Die erwarteten preisabhängigen Einnahmen bilden eine absolute Obergrenze für die gesamten (geschätzten) Kosten der Güterproduktion und -distribution. Es ist daher eine Produktions- bzw. Dienstleistungserbringungssystematik abzuleiten, die es ermöglicht, das Angebot unterhalb der Zielkosten zu produzieren. *Ergebnis:* Leistungserbringungsmodell bzw. vollständige Produktions- bzw. Dienstleistungssystematik.

5. Netzwerk- und Informationsdesign: Ausgehend vom Leistungserbringungsmodell ist festzulegen, welche Wertschöpfungsaktivitäten intern und welche unter Einbeziehung externer Partner durchgeführt werden sollen. Diese überbetriebliche Vernetzung und die damit verbundenen In- und Outsourcing-Entscheidungen sind u.a. unter Berücksichtigung der eigenen Kernkompetenzen, vorhandener Kapazitäten, der Güterdistribution sowie kultureller und handelsrechtlicher Barrieren und Besonderheiten zu fällen. Sofern die Zusammenarbeit mit externen Partnern einen umfangreichen Informationsaustausch erfordert, ist auch ein ausdifferenziertes Informationsmodell zu entwickeln. Dieses umfasst überbetriebliche Informations-

ströme, Datenstrukturen, Informations- und Kommunikationstechnologien sowie bei herkömmlichen Geschäftsmodellen das IT-Sicherheitskonzept [Blec+02]. *Ergebnis:* Unternehmensnetzwerk, überbetriebliche Geschäftsprozesse und deren elektronische Unterstützung.

6. Investitions-, Risiko- und Wirtschaftlichkeitsanalysen: Nachdem alle Informationen (Preis-Umsatz-Modell sowie Leistungserbringungs- und Netzwerkmodell) zur fundierten Schätzung der Erlöse vorliegen, ist die Wirtschaftlichkeit der notwendigen Investitionen zu analysieren und über szenariobasierte Risikoanalysen zu bewerten [Fink+00]. Ein aussagekräftiges und tragfähiges Finanzierungsmodell, das Zielkosten voraussetzt und gleichzeitig bewertete Risiken enthält, bildet u.a. eine gute Ausgangsbasis, um gemäß Basel II die Kreditkosten zu minimieren (vgl. [KoWi02]). *Ergebnis:* Finanzierungs- und ggf. Beteiligungsstruktur.

3 IT-Risikomanagement in Unternehmensnetzwerken

3.1 Netzwerkrisiken

In der Praxis scheitern aufgrund vielfältiger Ursachen, z.B. zu ehrgeizige Entwicklungsvorhaben oder ein mangelhaftes Projektmanagement, viele überbetriebliche Kooperationen – Ziele werden nicht eingehalten [Crow99] [Drag01] [Kars98] [Nich+01] [RaSu02]. Ein wesentlicher und sehr häufig auftretender Grund für Störungen bzw. Probleme bei der überbetrieblichen Wertschöpfung ist die nicht ausreichende Berücksichtigung von sogenannten (Netzwerk-)Risiken, die bei der überbetrieblichen Zusammenarbeit auftreten können. Bedeutende Netzwerkrisiken ergeben sich beispielsweise aus opportunistischen Verhaltensweisen von Netzwerkpartnern wie auch beim nicht ausreichend geschützten Informationsaustausch.

Unternehmens*interne* Organisationseinheiten unterliegen der direkten Disposition des Unternehmers bzw. des Managers und die resultierenden Planungsrisiken sind verhältnismäßig gering. Netzwerkpartner bzw. *externe* Faktoren sind dagegen in ihrem Verhalten nur sehr eingeschränkt vorhersagbar, so dass z.B. bei kooperativen Projekten in der Auftrags- und Projektplanung die sich ergebenden Netzwerkrisiken mit einbezogen werden müssen (vgl. [Lück00] [Merk99] [Voß02]). Hinzu kommt, dass Defizite von Netzwerkpartnern direkt auf den Projekterfolg bzw. die fristgerechte Leistungserstellung durchschlagen können (vgl. [Stra01]).

Ergänzend zur Sicherstellung eines stabilen internen IT-Systembetriebs müssen Unternehmen zunehmend auch Aspekte des elektronischen bzw. digitalen Informations- und Dokumentenaustausches über die eigenen Grenzen hinweg berück-

sichtigen. Der Austausch von Informationen entlang der Wertschöpfungskette oder in Unternehmensnetzwerken ist dabei mit sehr unterschiedlichen Risiken verbunden. Es muss beispielsweise sichergestellt werden, dass Daten bei der Übertragung von Dritten weder gelesen noch manipuliert werden. Auch muss ein Dokument rechtsverbindlich einer juristischen oder natürlichen Person zugeordnet werden können. Hierfür gibt es leistungsfähige kryptographische Verfahren.

Die Zusammenarbeit in informationsintensiven Unternehmensnetzwerken kann wesentlich verbessert und die Gefahr eines Versagens deutlich reduziert werden, wenn ein leistungsfähiges IT-(Netzwerk-)Risikomanagement entwickelt und implementiert wird (vgl. [Klei00] [Vaug97]). Unterschiedliche Formen einer überbetrieblichen Zusammenarbeit (Virtuelle Organisation, Value Net, Netzwerk mit oder ohne Broker, vertikale oder horizontale Netzwerke usw.) sind mit unterschiedlichen IT-Risiken verbunden. Unterschiedliche Netzwerkstrukturen bzw. –typen müssen daher im jeweiligen Anwendungskontext mit berücksichtigt werden (vgl. [DaMa93]).

3.2 Aufgaben und Ansätze des Risikomanagements

Zu den Aufgaben des Risikomanagement zählt im Wesentlichen die systematische und vollständige *Risikoanalyse* und *–bewertung* sowie die *Risikobewältigung* und das *Risikocontrolling* (vgl. [Brüh80] [Glei02]). In der *Risikoanalyse* werden aus der Vielzahl der auf das Unternehmen einwirkenden Risiken die wichtigsten identifiziert, hinsichtlich der Wirkungszusammenhänge analysiert und anschließend *bewertet* (vgl. [Brüh01] [Erde01] [Klei00]); z.B. in einem Risiko-Portofolio (vgl. Abschnitt 3.3.2). *Risikoanalyse* und *–bewertung* sind von besonderer Bedeutung, da nur erkannte Risiken wirkungsvoll bewältigt werden können. Eine wesentliche Herausforderung ist dabei die Früherkennung von Risiken, die sich nur schwach abzeichnen, sich jedoch zu einer ernsthaften Bedrohung entwickeln können. Anhand eines Entscheidungsprofils können Maßnahmen zur *Risikobewältigung* abgeleitet werden, die im abschließenden *Risiko-Controlling* hinsichtlich ihrer Wirksamkeit überprüft werden (vgl. [Glei02] [Mann89] [Neub89] [Stra01]). Zu Beginn eines Risikomanagement-Prozesses muss von den Entscheidern die Risikostrategie festgelegt werden, die nach jedem Durchlauf hinsichtlich der Richtigkeit zu überprüfen ist.

Abbildung 4: Kernaufgaben des Risikomanagements

3.3 Netzwerkorientiertes IT-Risikomanagement

Die bisher bekannten Verfahren und Ansätze zur Identifikation und Bewältigung von Risiken sind im Hinblick auf die Herausforderungen und damit verbundenen Chancen und Risiken in Unternehmensnetzwerken bzw. beim überbetrieblichen Informationsaustausch unzureichend. So bieten z.B. die Spiel- und die Systemtheorie Ansatzpunkte zur Darstellung und Gestaltung von Kooperationen bzw. Hinweise zur Vermeidung opportunistischen Verhaltens, jedoch brauchen Unternehmen einen integrierten Ansatz zur, Erfassung (Analyse) und Beherrschung (Bewältigung) von IT-Netzwerkrisiken. Das Aachener IT-Sicherheitsmodell, vgl. Kapitel 3.3.3 schafft die Grundlagen eines fundierten netzwerkorientierten IT-Risikomanagements. Diese Risiken können dann als exogene Faktoren im klassischen Risikomanagement berücksichtigt werden.

3.3.1 IT- Risikoanalyse

Neben den Grundkriterien der Systemsicherheit *„Integrität“*, *„Vertraulichkeit“*, *„Authentizität“* und *„Verfügbarkeit“* müssen vor allem allgemeine Bedrohungen und Risiken sowie die Anforderungen beteiligter Unternehmen berücksichtigt werden. Daher ist die Beschreibung von Bedrohungen bzw. Angriffsszenarios von grundsätzlicher Bedeutung. Die Identifizierung der Bedrohungen kann erfolgen, indem im Einzelfall geprüft wird, inwiefern der Verlust der Authentizität, der Vertraulichkeit, der Integrität und der Verfügbarkeit einen Schaden darstellt. Weiterhin hat sich in der Praxis bewährt, bereits vorgefertigte Gefährdungskataloge zu verwenden. Derartige Kataloge beinhalten für verschiedene Risikokategorien wie „Höhere Gewalt“, „Organisatorische Mängel“, „Menschliche Fehlhandlungen“, „Technisches Versagen“ und „Vorsätzliche Handlungen“ eine meist recht umfangreiche Auflistung allgemeiner Risiken (vgl. auch [N.N.02]). Bei der Risikoanalyse in überbetrieblich vernetzten IT-Strukturen sollte ferner noch untersucht werden, wer bzw. welche Organisation potenzieller Angreifer ist und was mögliche Motive sind. Angriffsszenarios werden so transparent.

3.3.2 IT-Risikobewertung

Im Rahmen einer IT-Risikobewertung hat sich die Unterscheidung zwischen Schadenshäufigkeit und –höhe bewährt [Hors00] [LaPo03] [N.N.02]. Mit Hilfe sogenannter Risikoportfolios für die einzelnen Risikokategorien, vgl. Abschnitt 0, können Einzelrisiken entsprechend qualitativ eingeordnet werden; vgl. Abbildung 5. Alle Risiken, die sich im vierten Quadranten (hohe Schadenshäufigkeit und –höhe) befinden, müssen über geeignete Maßnahmen zur Risikobewältigung so beeinflusst werden, dass das Restrisiko in einem vertretbaren Rahmen bleibt. Bei hoher Schadenshäufigkeit (Quadrant II) oder –höhe (Quadrant III) ist im Einzelfall abzuwägen, ob Schutz- oder Vorsorgemaßnahmen zur Risikobewältigung anzustrengen sind.

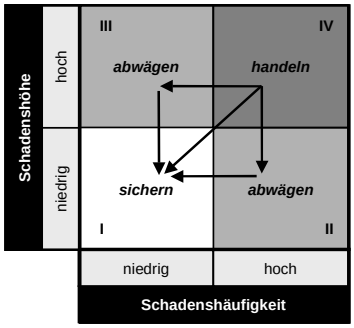

Abbildung 5: Qualitative Bewertung von IT-Risiken

3.3.3 IT-Risikobewältigung

Ziel der Risikobewältigung ist die Konkretisierung und Implementierung von Maßnahmen, um sämtliche als kritisch eingestufte Risiken (Abbildung 5, Quadrant IV und ggf. II und III) auf ein akzeptiertes Restrisiko zu reduzieren. Sämtliche Maßnahmen und Vorgehensweisen sind Bestandteil eines IT- Sicherheitskonzeptes.

Das IT-Sicherheitskonzept eines Internet-Intermediärs muss gewährleisten, dass (a) allgemeine Bedrohungen und Risiken, (b) die Unternehmensanforderungen sowie (c) die Grundkriterien der Systemsicherheit als *Sicherheitsvorgaben* berücksichtigt werden und dass nach Definition einer Sicherheitspolitik geeignete Vorkehrungen auf der Basis von Sicherheitskriterien getroffen werden. Schadenshäufigkeit und mögliche Schadenshöhen können mit dem Aachener IT-Sicherheitskonzept, wie gefordert, auf ein niedriges Maß reduziert werden; vgl. Abbildung 6.

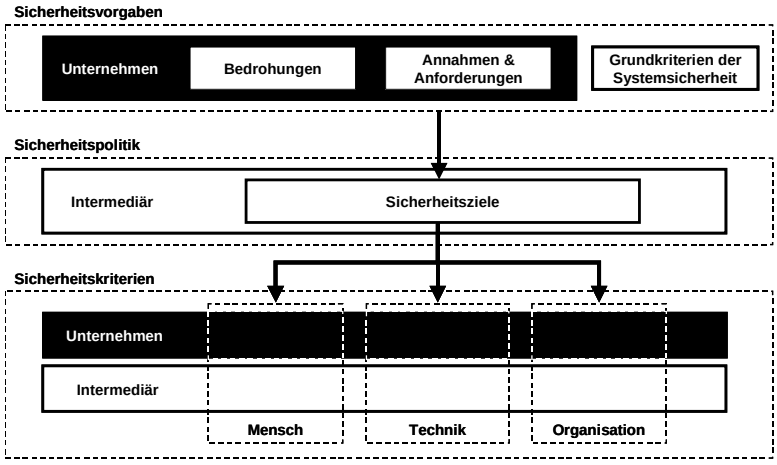

Abbildung 6: Aachener-IT-Sicherheitskonzept zur IT-Risikobewältigung

Die *Sicherheitspolitik* dient der richtungsweisenden Verankerung des erfolgskritischen Themas Sicherheit in der internen Organisation der intermediären Zeugnisplattform, deren technischer Umsetzung sowie in der externen Kommunikation. Ein vorrangiges Ziel der Sicherheitspolitik ist die Schaffung der notwendigen Akzeptanz des avisierten Sicherheitsniveaus der Zeugnisaustauschplattform bei den metallerzeugenden und –verarbeitenden Unternehmen. Sicherheitspolitiken müssen, um den Auftrag der internen und externen Kommunikation zu genügen, praxisnah und verständlich sein und Hilfestellung bei der Ableitung organisatorischer Regelungen, Verfahren, Praktiken oder Richtlinien zum Thema Sicherheit leisten [Rann98a] [Rann98b]. Eine Sicherheitspolitik muss somit, verglichen mit einer mathematisch-wissenschaftlichen Definition des Begriffs Sicherheit, greifbar und einfach nachvollziehbar sein.

Sicherheitskriterien und -maßnahmen können den Bereichen Mensch, Technik und Organisation (MTO) zugeordnet werden [N.N.02] . Begleitend zu den technischen Maßnahmen und Kriterien müssen auch Pflichten, Zuständigkeiten und Verhaltensweisen in unterschiedlichen (Bedrohungs-) Szenarien definiert werden. Eine wichtige Eigenschaft eines intermediären Internet-Geschäftsmodells ist der unternehmensübergreifende Charakter. Daher müssen auch auf der Seite der teilnehmenden Unternehmen entsprechende MTO-Maßnahmen umgesetzt werden.

Ein Grundproblem ist, dass nicht alle Bedrohungen im Vorfeld bekannt sind, so dass ein Schadenseintritt nicht vollständig ausgeschlossen werden kann. Diese Tatsache führt zu der Notwendigkeit, auch Notfallpläne und Notfallaktivitäten im Vorfeld zu entwickeln, um im Ernstfall den Schaden begrenzt zu halten.

3.3.4 IT-Risikocontrolling

Die Balanced Scorecard (BSC) ist ein umfassendes und erprobtes Instrumentarium, um die Unternehmensstrategie organisatorisch zu verankern und gezielt mit Maßnahmen auszugestalten [KaNo96] [Nive02]. Die klassische Form der BSC sieht dabei die vier Perspektiven *„Lernen und Entwicklung“, „Interne Geschäftsprozesse“ „Finanzen“* sowie *„Kunden“* vor [KaNo96]. Aufgrund der wachsenden Bedeutung vernetzter Wertschöpfungsstrukturen wird ein Engagement in Unternehmensnetzwerken sowie die operative Ausgestaltung überbetrieblicher Geschäftsprozesse mit Partnern und Lieferanten zunehmend erfolgskritisch, so dass die externe Perspektive „Kunden“ der BSC zu erweitern ist. Daher wird hier die Netzwerkperspektive eingeführt, die, anders als die Kundensichtweise, *alle* überbetrieblichen Wertschöpfungsaktivitäten (Kunden, Lieferanten, Partner – horizontal wie auch vertikal) zusammmenfasst; vgl. auch Abbildung 7.

Unternehmerische Entscheidungen müssen grundsätzlich Potenziale (z.B. Gewinn oder Umsatz) wie auch die damit verbundenen Risiken gleichermaßen berücksichtigen. Ein erfolgreiches IT-(Netzwerk-)Risikocontrolling zeichnet sich daher durch eine ausbalancierte Gegenüberstellung von Chancen und Risiken aus. Unternehmen, die sich in vernetzten Strukturen engagieren, sollten daher einerseits

die in einem Unternehmensnetzwerk verfolgten Ziele klar formulieren, diese soweit möglich mit messbaren Kennzahlen hinterlegen und geeignete Maßnahmen zur Zielerreichung festlegen. Die Voraussetzungen, Erfolgspotenziale zu nutzen, werden so geschaffen. Andererseits schafft die Gegenüberstellung der mit einer überbetrieblichen Vernetzung verbundenen IT-Risiken eine tragfähige Entscheidungsunterstützung und hilft auch, Fehlentwicklungen bzw. Gefahren frühzeitig zu erkennen; vgl. Abbildung 7.

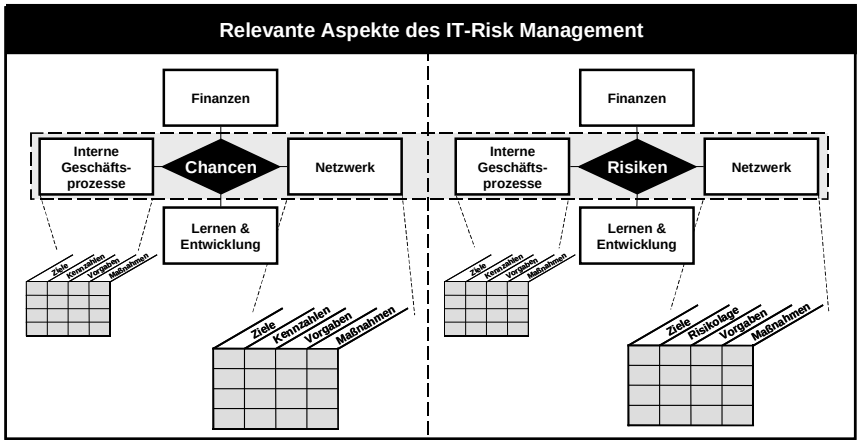

Abbildung 7: Relevante Aspekte des IT-Risikomanagements

4 Fallstudie: Risikomanagement für einen Informationsintermediär in der Metallindustrie

Die Metallindustrie in Deutschland und Europa ist ein nach wie vor wesentlicher Wirtschaftsfaktor. In den vergangenen Jahren hat sich die Branche der Metallerzeuger und -verarbeiter zunehmend auf die Entwicklung und Produktion von Spitzenstählen spezialisiert, um sich von der Billigkonkurrenz aus Osteuropa und Fernost zu differenzieren. Besteller hochwertiger Stahlsorten verlangen im Regelfall eine genaue Dokumentation von zuvor spezifizierten Eigenschaften in sogenannten Materialzeugnissen. In der Metall erzeugenden und verarbeitenden Industrie ist der Handel mit Erzeugnissen daher meist auch mit dem Austausch von Materialzeugnissen verbunden. Anhand dieser Zeugnisse werden die Eigenschaften der Produkte für Lieferant und Besteller verbindlich festgehalten. In der Vergangenheit sind sowohl die Zahl der Materialzeugnisse, die der Lieferant auf Anforderung des Bestellers bereitstellen muss, als auch die qualitativen Anforderungen an diese Zeugnisse stetig gestiegen. Ein weiterer wesentlicher Grund für das stark zunehmende Zeugnisaufkommen ist die flächendeckende Einführung von

Qualitätsmanagementsystemen und die Bedeutung der Produkthaftung für die Lieferanten. Die eindeutige Zuordnung und Rückverfolgbarkeit von metallischen Werkstoffen bis zur Erzeugung aus der flüssigen Schmelze hat deshalb heute einen sehr hohen Stellenwert. Diese Problematik hat nicht nur eine nationale sondern auch eine internationale Bedeutung wie z.B. *europäische* Normen zu metallischen Erzeugnissen und grenzüberschreitende Geschäftstätigkeiten von Unternehmen der Metallindustrie belegen (DIN 1990).

Die konventionelle Bereitstellung von wenig standardisierten Materialzeugnissen auf dem Postweg, per Fax oder begleitend zum Materialversand führt zu vielfältigen Problemen. Infolge manueller Bearbeitungsschritte, beispielsweise bei der Archivierung papierbasierter Dokumente, entstehen hohe Prozesskosten. Eine standardisierte Weiterverarbeitung ist aufgrund unterschiedlich aufgebauter Zeugnisse schwierig und zeitaufwendig, und besonders nachteilig wirkt sich ein verspäteter Zeugniseingang beim Besteller aus, da Produktionsverzögerungen drohen. Es sind daher Ansätze erforderlich, die die Metallindustrie beim schnellen, weltweiten, *flexiblen* und *sicheren* Zeugnisaustausch unterstützen; vgl. Abbildung 8.

Eine intermediäre internetbasierte Zeugnissaustauschplattform ist in der Lage, die spezifischen Probleme im Zusammenhang mit dem Austausch und der Verwaltung von Materialzeugnissen zwischen den Unternehmen durch einheitliche Übertragungs- und Verarbeitungsstandards zu beheben. Eine derartige Austauschplattform als mögliche Geschäftsidee („Trigger"; vgl. auch Abbildung 3) wurde im vom Bundesministerium für Wirtschaft und Arbeit geförderten Projekt *„Z-Online – Elektronischer Austausch von Materialzeugnissen in der Metallbranche"* unter Einbeziehung von 10 Unternehmen der Metallindustrie sowie des TÜV Rheinland Berlin Brandenburg realisiert. Ein für diesen Anwendungsfall optimiertes IT-Sicherheitskonzept wird im Projekt *„iSig – Digitale Signaturen im elektronischen Materialzeugniswesen"* (gefördert durch das Ministerium für Wirtschaft und Arbeit des Landes Nordrhein-Westfalen) entwickelt und umgesetzt, so dass dann ein von der Metallbranche akzeptierter „Zeugnisaustauschdienst" angeboten werden kann.

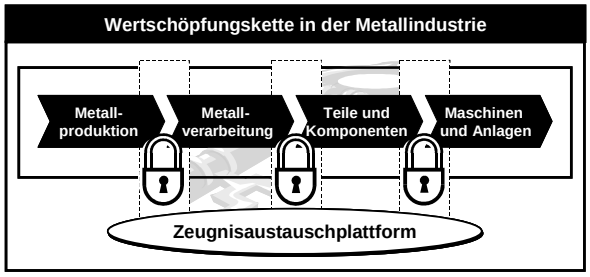

Abbildung 8: Sichere Zeugnisaustauschplattform in der Metallindustrie

Beim elektronischen Zeugnisversand ergeben sich sowohl interne (z.B. Sabotage und Fehlbedienungen) als auch externe (Angriff von Außen; z.B. Hacker) Bedro-

hungen der IT-Sicherheit. Analysen haben gezeigt, dass die Authentizität und Integrität elektronischer Materialzeugnisse sowie die Vertraulichkeit der Geschäftsbeziehungen gewährleistet werden müssen und Datenbestände nicht verloren gehen dürfen. Die Unternehmen der Metallindustrie fordern ein hohes Sicherheitsmaß, ohne präzise Anforderungen zu formulieren, so dass hier für die Ableitung eines tragfähigen Sicherheitskonzeptes Bedrohungsanalysen und die Grundkriterien der IT-Systemsicherheit anzulegen sind.

4.1 Relevante IT-Risiken und Sicherheitsvorgaben

Die Identifizierung der Bedrohungen erfolgt hier, indem in Einzelfällen geprüft wird, inwiefern der Verlust der Authentizität, der Vertraulichkeit, der Integrität und der Verfügbarkeit (Grundkriterien der Systemsicherheit) einen Schaden darstellt. Ein Grundproblem ist allgemein, dass ein Schadenseintritt niemals vollständig ausgeschlossen werden kann. Daher müssen auch Notfallpläne und Notfallaktivitäten im Vorfeld entwickelt werden, so dass im Ernstfall ein Schaden immer begrenzt bleibt.

In den Unternehmen der Metallindustrie kommen mehrere Mitarbeiter aus unterschiedlichen Abteilungen mit Materialzeugnissen in Berührung. Die Erstellung, Prüfung sowie Analyse dieser Zeugnisse erfolgt in der Qualitätsstelle, bevor eine Freigabe durch den Leiter oder dessen Vertreter erfolgt. Ausgewählte Sachverständige dokumentieren vor der Freigabe die Prüfergebnisse in Zeugnisformularen und bestätigen die Korrektheit mit einem eigenen Prüfzeichen. Auch für diese Prüfzeichen ist ein elektronisches, sicheres Äquivalent bereitzustellen. Im Einzelfall kann es notwendig sein, auch diesen Workflow rechtsverbindlich mit elektronischen Signaturen abzubilden. Dies ist insbesondere dann der Fall, wenn externe Prüforganisationen beteiligt sind. Auch muss durch das Sicherheitskonzept gewährleistet sein, dass sämtliche Abteilungen wie Ein- und Verkauf sowie Wareneingang und -ausgang, einen *lesenden* Zugriff auf die zu einem Geschäftsvorfall gehörenden Zeugnisse haben.

Um die Rechtsverbindlichkeit papierbasierter Materialzeugnisse auch elektronisch herzustellen, ist ferner ein sogenanntes Schriftformäquivalent gefordert; d.h. die Vorgaben, die sich aus dem Signaturgesetz und der Signaturverordnung ergeben, müssen erfüllt werden. Auch vergleichbare internationale Anforderungen sind zu prüfen und ggf. zu berücksichtigen. Weiterhin ist der Nachweis von Integrität und Authentizität für mehr als 10 Jahre sicherzustellen, da bestimmte metallische Bauteile eine Lebensdauer von z.T. mehr als 50 Jahren haben; z.B. Pumpengehäuse. Daher wird mitunter auch eine akkreditierte Signatur eingesetzt. Eine besondere *rechtliche* Bedeutung haben hier die Grundkriterien „Authentizität“ und „Integrität“, da im Haftungsfall exakt und zweifelsfrei nachvollziehbar sein muss, welcher Hersteller welche Daten in den relevanten Materialzeugnissen hinterlegt hat. Eine vornehmlich *wirtschaftliche* Relevanz haben hier die Grundkriterien „Vertraulich-

keit“ (Schutz von Betriebsgeheimnissen) und „Verfügbarkeit“ (stabile Geschäftsprozesse).

4.2 Anforderungen an das IT-Risikomanagements

Die Sicherheitspolitik dient der richtungsweisenden Verankerung der IT-Sicherheit in der internen Organisation der intermediären Zeugnisplattform, der externen Kommunikation sowie als Vorgabe bei der technischen Umsetzung. Ein vorrangiges Ziel der Sicherheitspolitik ist die Realisierung des avisierten Sicherheitsniveaus und somit der notwendigen Akzeptanz der Zeugnisaustauschplattform in der Metallindustrie. Die Sicherheitspolitik der intermediären Zeugnisplattform ergibt sich aus der Beantwortung des folgenden Fragenkonstruktes zur operativen Beschreibung des Begriffes IT-Sicherheit:

- *Was ist zu schützen?* Zu schützen sind die Integrität und die Vertraulichkeit der in der Plattform eingestellten elektronischen *Materialzeugnisse* sowie das Funktionieren des *Materialzeugnisaustausches* zwischen den beteiligten Unternehmen. Eine hohe Verfügbarkeit ist mit entscheidend für den Erfolg der Plattform, da der zeitnahe Versand bzw. Empfang von Materialzeugnissen für die Metallerzeuger und –verarbeiter von wettbewerbsentscheidender Bedeutung ist. Auch die *Geheimhaltung der Geschäftsbeziehungen* zwischen den Unternehmen ist ein schützenswertes Gut.
- *Wer soll es schützen?* Hauptverantwortlich für die Sicherheit ist der *Betreiber* der Zeugnisaustauschplattform. Dieser muss ein fundiertes *Sicherheitskonzept* vorlegen und auch den *Unternehmen*, die ebenfalls ihren Beitrag zur Schaffung eines hohen Sicherheitsstandards leisten müssen, die notwendigen Werkzeuge und Mechanismen für den sicheren Zeugnisaustausch bereitstellen. Externe Partner überprüfen regelmäßig die Sicherheitsstandards und verwalten die elektronischen Signierschlüssel.
- *Wogegen ist es zu schützen?* Die schützenswerten Güter der Zeugnisplattform (Materialzeugnisse, deren Austausch sowie die *Geschäftsbeziehungen*) müssen gegen Angriffe von *außen* und *innen*, Fehlbedienungen bzw. Fehlern beteiligter und berechtigter Personen sowie höhere Gewalt geschützt werden.
- *Wie ist es zu schützen?* Die Schutzmaßnahmen müssen auf den Ebenen Mensch, Technik und Organisation *wirken*, damit dem gesamten Bedrohungsspektrum effektiv begegnet werden kann. Ein Datenverlust muss durch *geeignete* Backup- und Archivierungsmaßnahmen ausgeschlossen werden, so dass mögliche Schäden begrenzt bleiben.
- *Was ist im Notfall zu unternehmen?* Die Umsetzung eines fundierten und detaillierten Sicherheitskonzeptes reduziert das *Restrisiko* auf ein insgesamt vertretbares Maß. Im Umkehrschluss bedeutet dies, dass Notfälle, z.B. Angriffe, *Netzausfall* oder Brand, grundsätzlich auftreten können und nicht auszuschlie-

ßen sind. Daher müssen, ergänzend zu den präventiven Maßnahmen, auch Notfallaktivitäten entwickelt werden, damit ein eingetretener Schaden insgesamt begrenzt bleibt. So muss beispielsweise die schnelle Wiederherstellung der Systemverfügbarkeit (z.B. durch redundante Infrastrukturen für einen Notfall) jederzeit gewährleistet sein. Alle Aktivitäten sind aufzuzeichnen, so dass Notfälle ausgewertet werden können, um konkrete Verbesserungen des Sicherheitskonzeptes abzuleiten.

4.3 Sicherheitsmaßnahmen zur Risikobewältigung

Nur wenn auf Mitarbeiter-, auf technischer sowie auf organisatorischer (MTO) Ebene Sicherheitsmaßnahmen umgesetzt werden, kann auch tatsächlich ein sicherer Systembetrieb gewährleistet werden. Ein Mitarbeiter, der mit seinem Passwort nicht verantwortungsbewusst umgeht, ist trotz weitreichender, technischer Maßnahmen ein Sicherheitsrisiko. Das IT-Sicherheitskonzept sieht daher auf allen drei MTO-Ebenen geeignete Kriterien und Maßnahmen vor. Eine weitere Detaillierung der Sicherheitsmaßnahmen und -kriterien ist jedoch erst nach einer genaueren Beschreibung der Betriebsorganisation möglich.

- *Faktor Mensch:* Menschliches Handeln ist, neben Anpassbarkeit und Flexibilität, auch durch eine hohe Fehleranfälligkeit gekennzeichnet. Größere Schäden durch Fehlbedienungen bzw. fehlerhaftes Verhalten können verhindert werden, indem alle Benutzer, egal ob Personal des Plattform-Betreibers *oder* der teilnehmenden Unternehmen, existierende Datensätze weder löschen noch verändern können. Die verschiedenen Teilnehmer bzw. Mitarbeiter nehmen in den Unternehmen Rollen mit unterschiedlichen Rechten ein. Ein Rechtekonzept muss sicherstellen, dass ein Anwender nur die Aktionen ausführen kann, für die er auch eine Befugnis hat. Die betriebliche Praxis zeigt, dass beim konventionellen Zeugnisversand gelegentlich Prüfbescheinigungen freigegeben und verschickt werden, die nicht mit den Spezifikationen aus der Bestellung übereinstimmen. Derartige Probleme können auch beim elektronischen Zeugnisversand auftreten, so dass hier geeignete Vorkehrungen zu treffen sind. Ein bereits eingestelltes Zeugnis muss für ungültig erklärt und durch ein neues, fehlerfreies ersetzt werden können (Revision), ohne dass das ungültige Zeugnis gelöscht wird. Fehlbedienungen führen bei einer vollständigen Unterbindung schreibender Zugriffe auf bestehende Zeugnisse (auch bei einer Revision) zu keinem Datenverlust, so dass das Risiko insgesamt minimiert wird. Der Betreiber muss weiterhin sicherstellen, dass, soweit technisch realisierbar, Fehler von Benutzern – egal ob auf Betreiber- oder Anwenderseite – nicht zu einem Systemzusammenbruch führen.
- *Faktor Technik:* Elektronische Materialzeugnisse müssen mindestens den gleichen bzw. übertragbaren Sicherheitsanforderungen genügen wie die papierbasierte Form, damit auch elektronisch die notwendige gerichtliche Verwertbar-

keit vorliegt. Die Realisierung eines ausreichenden Sicherheitsmaßes für elektronische Materialzeugnisses erfordert daher technische *Vorkehrungen*, die, neben Zugangskontrollen und dem Schutz vor Viren etc. (z.B. durch eine Firewall), insbesondere kryptographische Verfahren und den Einsatz einer digitalen Signatur umfassen [Fumy+95] [Rive+78]. Zur Realisierung einer digitalen Signatur im Sinne des *Signaturgesetzes (SigG)* und der Verordnung zur digitalen Signatur *(Signaturverordnung - SigV)* müssen leistungsstarke Kryptoalgorithmen verwendet werden (BSI 2001), da die Sicherheit primär von der Stärke der zugrunde liegenden Kryptoalgorithmen abhängt [Baue00]. Die Rechtssicherheit und das notwendige Vertrauen in die Plattform können so hergestellt werden. Der Einsatz einer akkreditierten Signatur wird auch geprüft, da diese den Vorteil hat, Integrität und Authentizität für mind. 30 Jahre zu garantieren und dass im Ernstfall vor Gericht nicht das Vorhandensein einer qualifizierten Signatur (nach SigG und SigV) bewiesen werden muss. Die Sicherheit auf technischer Ebene umfasst auch die dauerhafte und verlässliche Archivierung der Daten auf nicht-flüchtigen Medien. Sämtliche Zeugnisse müssen über (automatische) Archivierungsalgorithmen z.B. auf CD oder DVD gebrannt werden. Um die Sicherheit der Zeugnisse für den gesamten „Lebenszyklus“ zu gewährleisten, müssen auch die archivierten Bescheinigungen verschlüsselt und signiert sein und an einem oder ggf. mehreren geeigneten Orten aufbewahrt werden. Zusätzlich sollten sämtliche Hard- und Softwarekomponenten, die sicherheitsrelevant sind, an verschiedenen Orten redundant vorgehalten werden. Der Schutz der internen Datenbank wird, abgesehen von einer Verschlüsselung, technisch durch den Einsatz einer Firewall sowie durch Virenschutzprogramme gewährleistet, die u.a. Typen wie Bootsektorviren, Dateiviren, Makroviren, Trojaner, Würmer, polymorphe Viren oder Hoaxes erkennen. Zusätzlich müssen *alle* Aktivitäten und Transaktionen auf der Plattform gespeichert werden, so dass jederzeit nachvollzogen werden kann, welcher Mitarbeiter bzw. Teilnehmer zu welcher Uhrzeit/Datum was gemacht und verändert hat.

- *Faktor Organisation:* Den unterschiedlichen Rollen der mit der Zeugnisaustauschplattform interagierenden Personen müssen auch organisatorische Maßnahmen Rechnung tragen. Sowohl der Plattform-Betreiber als auch die teilnehmenden Unternehmen müssen klar festlegen, welche Mitarbeiter Zeugnisse anlegen, lesen, freigeben, revidieren und verwalten dürfen und welche *Rechte* an eine bestimmte *Rolle* geknüpft sind. Ein Zeugnisempfänger erhält, im Gegensatz zum Hersteller, lediglich Lese- und Rechercherechte. Um sicherzustellen, dass *niemand* (!) Daten manipulieren oder vollständig löschen kann, ist es erforderlich, Schlüsselverwaltung und Systemadministration organisatorisch konsequent zu trennen. Daher wird nicht nur eine Zertifizierungsstelle eingeschaltet, sondern auch geregelt, *wie* der Systemadministrator auf Backups zurückgreift, um zu vermeiden, dass dieser z.B. gesicherte Daten löschen kann.

5 Zusammenfassung und Ausblick

Unternehmen bewegen sich in einer zunehmend dynamischeren Umgebung und engagieren sich vermehrt in Wertschöpfungsnetzwerken. Eine wesentliche Herausforderung ist dabei, die Konkurrenzfähigkeit zu sichern und den Unternehmenswert langfristig zu steigern. Diese strategische Aufgabe erfordert u.a. eine permanente Überprüfung und ggf. auch eine Anpassung des eigenen Geschäftsmodells. Die in diesem Beitrag vorgestellte Meta-Methode *House of Value Creation* zeigt die relevanten strategischen Faktoren auf, die bei der Gestaltung der Partialmodelle eines Geschäftsmodells besonders zu berücksichtigen sind und führt den Anwender durch den gesamten Prozess der Geschäftsmodellierung. Dabei werden auch bekannte und bewährte Methoden in den einzelnen Schritten eingesetzt. Bei Unternehmensnetzwerken und Internet-Geschäftsmodellen müssen, sofern wichtige Dokumente ausgetauscht oder online Verträge geschlossen werden, zusätzlich die Schutzbedürfnisse der Kunden über ein geeignetes IT-Risikomanagement berücksichtigt werden. Das hier vorgestellte *Aachener-IT-Sicherheitskonzept* ist eine praxistaugliche Grundlage für die fundierte Bewältigung von IT-Risiken in Netzwerken. Aufgrund der positiven Erfahrungen planen wir, die wissenschaftliche Validität der Modelle in weiteren Anwendungsfeldern zu prüfen.

Literatur

[AfTu01] Afuah, A.; Tucci, C.L.: Internet Business Models and Strategies: Text and Cases. McGraw-Hill/Irwin, New York 2001.

[Akao90] Akao, Y.: Quality Function Deployment: Integrating Customer Requirements into Product Design. Productivity Press, Portland, Origon 1990.

[Atre+02] Atreya, M.; Hammond, B.; Starrett, P.; Paine, St.; Wu, St.: Digital Signatures. McGraw-Hill Osborne, 2002.

[Bala96] Balakrishnan, S.: Benefits of customer and competitive orientations in industrial markets. In: Industrial Marketing Management, 25(1996)4, S. 257-269.

[Baue00] Bauer, F.: Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie. Springer-Verlag, 2000.

[Bens97] Bensaou, M.: Interorganizational Cooperation - The Role of Information Technology: An Empirical Comparison of US and Japanese Supplier Relations. In: Information Systems Research, 8(1997)2, S. 107-124.

[Blec+02] Bleck, S.; Forzi, T.; Laing., P.; Stich, V: The Path from Business Modeling to Technology Management. In: Proceedings of the International Conference on Advanced Production Management Systems (APMS 2002), Eindhoven (NL), 8-13 September, 2002, S. 34-46.

[Brüh01] Brühwiler, B.: Einführung eines unternehmensweiten Risk-Managements. In: io management, (7/8), 2001, S. 54-59.

[Brüh80] Brühwiler, B. : Risk-Management – eine Aufgabe der Unternehmensführung, Verlag Paul Haupt, Bern Stuttgart, 1980.

[BrKa00] Brynjolfsson, E.; Kahin, B.: Understanding the Digital Economy. MIT Press, Boston 2000.

[Coas37] Coase, R.H.: The Nature of the Firm. In: Economica, (1937), S. 386-405.

[Crow99] Crowley, S.: Identification of failed R&D Projects (working paper), December 1999. Download: http.//www.stevencrowley.com/FailedRD.htm am 02.07.02.

[DaLe84] Daft, R.; Lengel, R.: Information Richness: A New Approach to Managerial Behaviour and Organization Design. In: Research in Organizational Bd. 6, (1984), S. 191-233.

[DaMa93] Davidow, W.; Malone, M.: Das virtuelle Unternehmen. Campus Verlag, Frankfurt am Main, New York 1993.

[DIN95] DIN (Hrsg.): DIN-EN 10 204: Metallische Erzeugnisse: Arten von Prüfbescheinigungen. Beuth Verlag, Berlin, August 1995.

[Drag01] Drage, R.: ITCF Summative Evaluation Project – Partnership and Collaborative Working, July 2001. Download: http.//www.peoplesnetwork.gov.uk/ content/partner.asp am 02.07.02.

[Ecke01] Eckert, C.: IT-Sicherheit. Konzepte, Verfahren, Protokolle. Oldenbourg, 2001.

[Erde01] Erdenberger, C.: Risikomanagement – Möglichkeiten einer pragmatischen Umsetzung in mittelständischer Unternehmen. In: Controller Magazin, (1) 2001, S. 13-16.

[EvWu00] Evans, P.; Wurster, T.: Blown to Bits: How the New Economies of Information Transforms Strategy. Harvard Business School Press, Boston, Massachusetts 2000.

[Fink+00] Fink, A.; Schlake, O.; Siebe, A.: Wie Sie mit Szenarien die Zukunft vorausdenken. Harvard Business Manager, (2000)2, S. 34-47.

[Fisch97] Fischer, J.: Mehrseitige Sicherheit in der Kommunikationstechnik, Bd.1, Verfahren, Komponenten, Integration. Dt. Universitätsverlag, 1997.

[FoLa02] Forzi, T.; Laing, P.: Business Modeling for E-Collaboration Networks. In: Proceedings of the 2002 Information Resources Management Association International Conference (IRMA 2002), Seattle, WA (USA), 19-22 Mai, 2002, S. 961-963.

[FoLu02] Forzi, T.; Luczak, H.: E-Business: Status Quo and Perspectives. In: Proceedings of the 6th International Conference on Work With Display Units (WWDU 2002) "World Wide Work". Hrsg.: Luczak, H.; Cakir, A.E.; Cakir, G., Berchtesgaden, 22-25 Mai, 2002, S. 494-496.

[FoLa03] Forzi, T.; Laing, P.: E-Business Modeling. In: Albalooshi, F. (Ed.), Virtual Education: Cases in Learning & Teaching Technologies, IRM Press, Hershey, London, Melbourne & Singapore, 2003, S. 113-138.

[Fumy+95] Fumy, W.; Horster, P.; Kraaibeek, P.: Standards und Patente zur IT-Sicherheit. Oldenbourg, 1995.

[Glei02] Gleißner, W.: Ratschläge für ein leistungsfähiges Risikomanagement. In: http://www.krisenkommunikation.de/akfo53-d.htm (Zugriff am 20.06.2002).

[HaSi99] Hagel III, J.; Singer, M.:. Unbundling the Corporation. In: Harvard Business Review, 77(1999)2, S. 133-141.

[Hint97] Hinterhuber, H.H.: Strategische Unternehmungsführung – II Strategisches Handeln. 6. Aufl. Walter de Gruyer, Berlin, New York 1997.

[HiGi92] Hirschhorn, L.; Gilmore, T.: The New Boundaries of the "Boundaryless" Company. In: Harvard Business Review, (1992)3, S. 104-115.

[Hoer99] Hoeren, Sch.: Rechtsfragen der digitalen Signatur. Erich Schmidt Verlag, 1999.

[Hors99] Horster, P.: Sicherheitsinfrastrukturen. Grundlagen, Realisierung, rechtliche Aspekte, Anwendungen. Vieweg-Verlag, 1999.

[Hors00] Horster, P.: Systemsicherheit. Vieweg Verlag 2000.

[KaNo96] Kaplan, R.S.; Norton, D.P.: The Balanced Scorecard: Translating Strategy into Action. Harvard Business School Press, September 1996.

[KeWo00] Kersten, H.; Wolfenstetter, K. D.: Handbuch der Informations- und Kommunikationssicherheit. Gefahren. Standards. Szenarien. Deutscher Wirtschaftsdienst, 2000.

[Kars98] Karsten, H.: Collaboration and Collaborative Information Technology: what is the nature of the relationship? Proceedings of the Conference „Information Systems: Current Issues and Future Changes" , Helsinki (SF), December 10th-13th, 1998; S. 231-254.

[KiMa00] Kim, C.; Mauborgne, R.: Knowing a Winning Business Idea When You See One. In: Harvard Business Review, 78(2000)5, S. 129-138.

[Klein95] Klein, S.: Interorganisationssysteme und Unternehmensnetzwerke - Wechselwirkungen zwischen organisatorischer und informationstechnischer Entwicklung. Habilitationsschrift Univ. St. Gallen 1995.

[Klei00] Kleitsch, D.: Risikomanagement. Schäffer-Poeschl Verlag, Stuttgart, 2000.

[KoWi02] Kolbeck, Ch.; Wimmer, R.: Finanzierung für den Mittelstand. Trends, Unternehmensrating, Praxisfälle. Dr. Th. Gabler Verlag, Wiesbaden 2002.

[Krcm00] Krcmar, H.: Informationsmanagement. 2. Aufl., Springer Verlag, Berlin, New York 2000.

[LaFo01] Laing P.; Forzi T.: E-Business and Entrepreneurial Cooperation. In: Proceedings of the 1st International Conference on Electronic Business (ICEB 2001), Hong Kong, Dezember 19-21, 2001, S. 7-9.

[LaFo02a] Laing, P.; Forzi, T.: Challenges for Business Modeling in the New Communication Era. In: Proceedings of the 31st Annual Meeting of the Western Decision Sciences Institute (WDSI 2002), April 2–5, 2002, Las Vegas, S. 434-436.

[LaFo02b] Laing, P.; Forzi, T.: Management of shared information within Manufacturing Networks. In: Proceedings of the 18th International Conference on CAD/DAM, Robotics and Factories of the Future (CARs&FOF'2002), Porto (P), 3-5 Juli 2002, S. 459-466.

[LaPo03] Laing, P.; Pohlmann, N.: Digitale Signaturen im elektronischen Materialzeugniswesen. In: Proceedings der DACH Security 2003, Erfurt, 25-26 März 2003.

[Luc+02a] Luczak, H.; Bleck, S.; Hoeck, H.: Elektronische Marktplätze - Voraussetzungen und Erfolgsfaktoren für den elektronischen Handel mit C-Dienstleistungen. In: Jahrbuch Dienstleistungsmanagement. Hrsg.: Stauss, B.; Bruhn, M. Gabler Verlag, Wiesbaden 2002, S. 149-176.

[Luc+02b] Luczak, H.; Bleck, S.; Forzi, T.; Laing, P.: A Holistic Approach for E-Business Engineering. In: Proceedings of the 2nd International Conference on Electronic Business (ICEB 2002) "Global E-Business in Knowledge-Based Economy: Management, Practice, and Opportunities", Taipei (Taiwan), Dezember 10–13, 2002, S. 222-224.

[Lück00] Lück, W.: Managementrisiken. In: Dörner, Horváth, Kagermann (Hrsg.): Praxis des Risikomanagements, Schäffer-Poeschl Verlag, Stuttgart, 2000.

[Malo+87] Malone, T.; Yates, J.; Benjamin, R.: Electronic Markets and Electronic Hierarchies: Effects of Information Technology on Market Structure and Corporate Strategies. In: Communications of the ACM, 30(1987)6, S. 484-497.

[Mann89] Mann, R.: Praxis strategisches Controlling. Verlag moderne Industrie, Landsberg, 1989.

[Merk99] Merkle, M.: Bewertung von Unternehmensnetzwerken – Eine empirische Bestandsaufnahme mit der Balanced Scorecard, Dissertation der Universität St. Gallen (HSG), Difo-Druck OHG, Bamberg, 1999.

[Mint79] Mintzberg, H: The Structuring of Organizations. Prentice-Hall, New Jersey 1979.

[Neub89] Neubürger, K. W.: Chancen- und Risikobeurteilung im strategischen Management. Poeschel Verlag, Stuttgart, 1989.

[Nich+01] Nichols, D.M; Thomson, K.; Yeates S.A.: Usability and open source development. Working Paper of the Dept. of Computer Science, Univ. of Waikato, Hamilton (NZ), 2001.

[Nive02] Niven, P.N.: Balanced Scorecard Step-by-Step: Maximizing Performance and Maintaining Results, 1st edition. John Wiley & Sons, 2002.

[N.N.99] N.N.: Certified-based mechanisms. In: SO/IEC 14888-3: Information technologiy Security techniques – Hash functions – Part 3, 1999.

[N.N.98] N.N.: Dedicated hash functions. In: SO/IEC 10118-3: Information technology – Security techniques – Hash functions – Part 3, 1998.

[N.N.02] N.N.: IT-Grundschutzhandbuch. Hrsg.: BSI – Bundesamt für Sicherheit in der Informationstechnik. Bundesanzeiger-Verlag, 2002.

[OECD00] OECD: OECD Information Technology Outlook: ICTs, E-Commerce and the Information Economy, Paris, 2000

[OsPi02] Osterwalder, A.; Pigneur, Y.: An e-Business Model Ontology for Modeling e-Business. In: Proceedings of the 15th Electronic Commerce Conference “e-Reality: Constructing the e-Economy, Bled (SLO), 17 –19 Juni 2002.

[Paro99] Parolini, C.: The Value Net: A Tool for Competitive Strategy. John Wiley & Sons Ltd, New York 1999.

[Pic+01] Picot, A.; Reichwald, R.; Wigand, R.T.: Die grenzenlose Unternehmung. 4. Aufl. Gabler Verlag, Wiesbaden 2001.

[Pic+96] Picot, A.; Rippenberger; T., Wolf, B.: The Fading Boundaries of the Firm: The Role of Information and Communication Technology. In: Journal of Institutional and Theoretical Economics, 152(1996)1, S. 65-79.

[Pohl96] Pohlmann, N.: Datenschutz. Sicherheit in öffentlichen Netzen. Hüthig, 1996.

[Port85] Porter, M.E.: Competitive Advantage – Creating and Sustaining Superior Performance. Free Press, New York 1985.

[Port01] Porter, M.E.: Strategy and the Internet. Harvard Business Review, 79(2001)3, S. 63-68.

[RaSu02] Rajagopalan, B.; Subramani, M.R.: Lessons from New Product Development for Managing Knowledge in Software Engineering, IEEE Software, Special Issue on Knowledge Management in Software Engineering, 2002.
Download: http://www.ids.csom.umn.edu/Faculty/Mani/Homepage/Papers/Rajagopalan_Subramani_IEEESW.pdf am 02.07.02.

[Rama96] Ramaswamy, R. (1996). Design and Management of Service Processes - Keeping Customers for Life. Addison-Wesley Publishing Company.

[Rann98a] Rannenberg, K.: Sicherheitszertifizierung – Probleme, Trends und Chancen. In: Datenschutz und Datensicherheit: Sicherheitszertifizierung, Heft4/1998.

[Rann98b] Rannenberg, K.: Zertifizierung mehrseitiger IT-Sicherheit. Kriterien und organisatorische Rahmenbedingungen. Vieweg Verlagsgesellschaft, 1998.

[ReKl01] Rentmeister, J.; Klein, S.: Geschäftsmodelle in der New Economy. Das Wirtschaftsstudium, 30(2001)3, S. 354-361.

[Rigg98] Riggers, B.: Value System Design – Unternehmenswertsteigerung durch strategische Unternehmensnetzwerke, Dissertation der Universität St. Gallen (HSG), Difo-Druck, Bamberg, 1998.

[Rive78] Rivest, Shamir, Adleman: A method for obtaining digital signatures and public keycryptosystems. In: Communications of the ACM, vol. 21 no. 2, 1978.

[Röhm+99] Röhm, A.; Fox, D.; Grimm, R.; Schoder, D.: Sicherheit und Electronic Commerce. Konzepte, Modelle und technische Möglichkeiten. Vieweg-Verlag, 1999.

[Rose98] Rose, F.: The economics, concept, and design of information intermediaries; a theoretic approach. Dissertation Universität Frankfurt 1998.

[Scho00] Schoder, D.: Die ökonomische Bedeutung von Intermediären im Electronic Commerce. Habilitation Universität Freiburg 2000.

[Stra01] Strack, J.: Controlling virtueller Unternehmen, Dissertation der Universität St. Gallen (HSG), Shaker Verlag, Aachen, 2001.

[Teub99] Teubner, R.A.: Organisations- und Informationssystemgestaltung: theoretische Grundlagen und integrierte Methoden. Dissertation Universität Münster. Gabler Verlag, Wiesbaden 1999.

[Timm00] Timmers, P. (2000). Electronic Commerce. New York: John Wiley & Sons Ltd.

[Vaug97] Vaughan, E.J.: Risk Management. John Wiley & Sons, New York, 1997.

[Voß02] Voß, W.: Ganzheitliche Bewertung von Unternehmensnetzwerken – Konzeption eines Bewertungsmodells, Verlag Peter Lang, Frankfurt a.M. u.a., 2002.

[Webb+00] Webb, D.; Webster, C.; Krepapa, A.: An exploration of the meaning and outcomes of a customer-defined market orientation. In: Journal of Business Research – New York, 48(2000)2, S. 101-112.

[Will75] Williamson, O.E.: Markets and Hierarchies: Analysis and Anti-trust Implications. Free Press, New York 1975.

[WiKl00] Wirtz, B. W.; Kleinecken, A.: Geschäftsmodelltypologien im Internet. In: Das Wirtschaftsstudium, 29(2000)11, S. 628-635.

[Wirt00] Wirtz, B.W.: Electronic Business. Gabler Verlag, Wiesbaden 2000.