Vahlens Handbücher der Wirtschafts- und Sozialwissenschaften

Logistik

Wege zur Optimierung der Supply Chain

von
Dr. Christof Schulte

6. Auflage

Thematische Gliederung:

Entwicklung und Produktion, Logistik – Produktion und Logistik

Verlag Franz Vahlen München 2013

Verlag Franz Vahlen im Internet:
www.vahlen.de
ISBN 978 3 8006 3995 3

Inhaltsverzeichnis: Logistik – Schulte

3.9.3.2 Expertensysteme

Expertensysteme sind intelligente Computerprogramme, die das Wissen von Fachleuten und Inferenzverfahren benutzen, um komplexe Probleme zu lösen.

Den Schwerpunkt der logistischen Expertensysteme bilden Anwendungen in der Produktionslogistik, wobei Systeme zur Unterstützung der Produktionsplanung und -steuerung besonders stark vertreten sind (vgl. *Mertens* 1999, S. 128). Ein weiteres Anwendungsfeld ist die Betriebsmittel- und Fabriklayoutplanung. In der Distributionslogistik werden Expertensysteme eingesetzt für die Transportdurchführungsplanung sowie die Transportsteuerung und -kontrolle. Im zahlenmäßig schwächsten Einsatzbereich von logistischen Expertensystemen finden sich solche für die Lieferantenauswahl und -bewertung, die Ermittlung optimaler Sicherheitsbestände und Lagerbestandsprognosen.

Expertensysteme setzen sich aus folgenden Teilsystemen zusammen:

- Wissensbasis, die Fakten und Regeln enthält.
- Problemlösungskomponente, die die Fakten und Regeln verknüpft sowie die Abarbeitung steuert.
- Wissenserwerbskomponente, um neues Wissen einzugeben oder bestehendes Wissen zu verändern.
- Dialogkomponente zur strukturierten Kommunikation mit dem Benutzer.
- Erklärungskomponente zur Erläuterung und Begründung gewählter Problemlösungen.

Insgesamt ist aber zu konstatieren, dass der Einsatz von Expertensystemen für logistische Fragestellungen in Deutschland relativ wenig verbreitet ist.

3.9.3 Führungsinformationssysteme

Führungsinformationssysteme dienen zur Unterstützung von Planungs-, Entscheidungs- und Kontrollaufgaben. Sie setzen auf den Daten auf, die in der Anwendungssoftware zur Verfügung stehen.

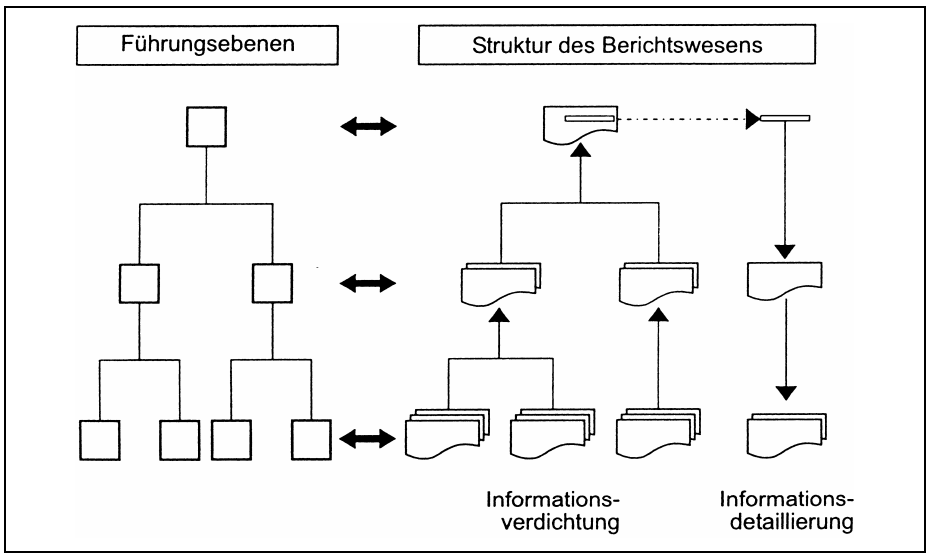

Abb. 3–50: Führungsebenen und Strukturen des Berichtswesens (Kargl 1998, S. 89)

Um dem spezifischen Informationsbedarf der Führungskräfte Rechnung zu tragen, muss ein Führungsinformationssystem sowohl ebenenspezifische Informationsverdichtung als auch Informationsdetaillierungen vornehmen können (vgl. Abb. 3–50).

Führungsinformationssysteme unterscheiden sich hinsichtlich der Nutzungsmodalitäten. Benutzerinaktive Führungsinformationssysteme stellen Informationen bereit, die nach Art, Inhalt und Darstellungsform vorbestimmt sind, so dass der Benutzer in der Regel nur die Möglichkeit hat, diese Information am Bildschirm sequentiell „durchzublättern“. Im Gegensatz zu diesen veralteten Führungsinformationssystemen ermöglichen benutzeraktive Systeme

- gezielt auf die gewünschten Informationen nach unterschiedlichsten Selektionskriterien zuzugreifen,
- Berechnungen durchzuführen (z. B. Parametervariation, Wirkungsanalyse) sowie
- Ergebnisse in verschiedenen Formen zu präsentieren.

3.10 IT-Sicherheitsmanagement

Größe und Komplexität der IT-Systeme haben in den letzten Jahren ständig zugenommen. Die Menge der bearbeiteten Daten wächst permanent in allen Unternehmen. Durch den Informationsaustausch über das Internet nimmt die Offenheit und damit Verwundbarkeit an den Systemgrenzen zu. Die größten **Gefahren** für die IT-Sicherheit liegen in Virenangriffen, Datenverlust und -diebstahl, Wirtschaftsspionage, Sabotage und Missbrauch. Beispielsweise können Datenverluste infolge fehlender oder unzureichender Datensicherung, eines unzureichenden Berechtigungskonzeptes, des Defekts eingesetzter Betriebsmittel, fehlender Katastrophenvorsorge (z. B. Brand), fehlender datenschutzgerechter Entsorgung von Datenträgern, Viren, Sabotage etc. auftreten.

Folgen von auftretenden Sicherheitsproblemen umfassen:

- Vertrauensverlust bei Kunden und Mitarbeitern,
- Verschlechterung der Wettbewerbsposition,
- Personen- und Sachschäden,
- Verstoß gegen Gesetze, Vorschriften und Verträge,
- Unternehmensgefährdung im schlimmsten Fall.

Vor diesem Hintergrund ist ein bewusster Umgang mit den genannten Risiken erforderlich. Es gilt die relevanten Gesetze, Vorschriften und Verträge einzuhalten. Hierbei ist stets die Angemessenheit bzw. Wirtschaftlichkeit der durchzuführenden Sicherheitsmaßnahmen zu beachten.

Vom Bundesamt für Sicherheit in der Informationstechnik (BSI) wurde ein Vorgehensmodell zum Schutz unternehmenskritischer Infrastrukturen entwickelt, das als Grundlage zur Etablierung eines IT-Sicherheitsmanagements dienen kann. Es umfasst folgendes Phasen- sowie Aktivitätenschema:

1. „Festlegung einer Unternehmensstrategie für den Umgang mit unternehmenskritischen Infrastrukturen
2. Zusammenstellen aller IT-Verfahren und IT-Komponenten unter Berücksichtigung von gegenseitigen Abhängigkeiten

3. Ermittlung und Festlegung der jeweiligen Kritikalität
   - Feststellen der möglichen Schwachstellen
   - Beurteilen der Wahrscheinlichkeiten des Schadenseintritts
   - Abschätzen von Auswirkungen und Schadenshöhe unter Berücksichtigung von Verfügbarkeit, Vertraulichkeit und Integrität
   - Festlegen der Kritikalitätskategorie (unkritisch, kritisch, hochkritisch)
4. Verifizierung und Entscheidung
   - Verbesserung der Objektivität durch Vergleich und Ranglisten
   - Beurteilung der Beeinflussbarkeit der Bereiche
   - Schwerpunktsetzung, ggf. auch durch bewusste Inkaufnahme weniger hoch geschützter Bereiche
   - abschließende Beurteilung/Entscheidung durch das Management unter Berücksichtigung der möglichen unternehmenskritischen Folgen
5. Maßnahmen und Konzepte
   - Bereitstellen der notwendigen Ressourcen (Budget, Personal, Zeit, Ausbildung)
   - Sicherstellen und Überprüfen der grundlegenden IT-Schutzmaßnahmen (siehe IT-Grundschutzhandbuch)
   - Erstellen eines Maßnahmenkatalogs zur Verbesserung des Schutzes der als hochkritisch (ggf. kritisch) eingestuften Systeme
   - Erstellen und Fortschreiben von Notfallplänen/Krisenmanagementabläufen
   - Durchsetzung und Kontrolle der Maßnahmen und Konzepte“ (*Heinrich/Lehner* 2005, S. 265 f.).

Die wesentlichen **Sicherheitsanforderungen** umfassen:

- Sicherheitspolitik als Grundlage,
- Zugangs- und Zugriffsschutz,
- Klimatisierung und Brandschutz,
- Datenschutz und -sicherung,
- Authentizität, d. h. eindeutige Zuordnung zum Absender bzw. Besitzer von Daten,
- Vertraulichkeit, d. h. Schutz von Daten gegen unbefugtes Lesen,
- Integrität, d. h. Validität von Daten und Sicherstellung, dass diese während der Übertragung nicht verändert worden sind,
- Verfügbarkeit, d. h. Sicherstellung, dass Anwendungen und Daten für den berechtigten Nutzer in einer adäquaten Antwortzeit erreichbar sind,
- Verbindlichkeit, d. h. Rechtsgeschäfte über das Internet dürfen nicht abstreitbar sein.

Nachfolgend können lediglich ein paar grundlegende Sicherungsmaßnahmen skizziert werden.

Organisatorische Maßnahmen zur Verhinderung unbefugten Daten- und Systemzugriffs umfassen Diebstahlsicherung durch Zutritts- und Zugangskontrolle. Zugangsmöglichkeiten von außen sind adäquat zu sichern und auf dem aktuellen Stand zu halten.

Die **Authentifizierung** ist der Prozess, einen Anwender oder eine Nachricht auf der Basis des Nutzernamens und eines Passwortes oder einer Dateisignatur zu identifizieren. Möglichkeiten zur Authentifizierung sind

- das Passwort, das der Anwender weiß,
- ein token oder eine Smartcard, die der Anwender besitzt sowie
- der Fingerabdruck, der Teil des Nutzers ist.

Während bei der Authentifizierung die Frage nach dem „Wer?“ gestellt wird, geht es bei der **Authorisierung** um die Erlaubnis. Letztere umfasst den Prozess, Anwendern auf Basis ihrer Identität den Zugriff zu Systemen zu geben. Hierbei hängt der Systemzugang von den Rollen ab, die dem Einzelnen zugeordnet wurden. Der Systemadministrator hinterlegt diese Berechtigungen im System. Konkrete Lösungsansätze sind hierbei Directory Services und Single Sign On.

Kryptographische Methoden haben die Aufgabe, Nachrichten unverständlich zu machen, um die Nachricht zu verbergen. Mithilfe von Verschlüsselungstechniken wird die Nachricht des Senders in eine verwandelt, die nur der Empfänger verstehen kann.

Für die Erhöhung der Sicherheit von Netzinfrastrukturen werden **Firewalls** eingesetzt. Firewalls sind spezielle Kommunikationsrechner mit Anschlüssen an mehrere Teilnetze, die diese verbinden und dabei nur genau spezifizierte Verbindungen zulassen. Diese Rechner werden insbesondere als einzige Verbindung zwischen dem Internet und dem LAN (Intranet) geschaltet. Dabei analysieren Firewalls den Datenstrom zwischen Internet und LAN auf verschiedenen Datenebenen und lassen nur als sicher eingeschätzte Daten durch. Eine Firewall soll sowohl das Eindringen von unerwünschten Personen verhindern, als auch sicher stellen, dass nicht alle internen Daten nach außen gelangen können.

Die allgemeinen Ziele von Firewall-Systemen sind folgende: Zugangskontrolle auf Netzwerkebene, Zugangskontrolle auf Benutzerebene, Zugangskontrolle auf Datenebene, Rechteverwaltung, Kontrolle auf der Anwendungsebene, Beweissicherung und Protokollauswertung, Alarmierung und Verbergen der internen Netzstruktur.

Ein Firewall-System wird quasi als Schranke zwischen das zu schützende und das unsichere Netz geschaltet, so dass der ganze Datenverkehr zwischen den beiden Netzen nur über das Firewall-Element möglich ist. Es stellt den „Common Point of Trust“ für den Übergang zwischen unterschiedlichen Netzen dar.

Auf der Firewall werden Mechanismen implementiert, die die ganzen Transaktionen sicher und beherrschbar machen sollen. Dazu analysiert das Firewall-System die Kommunikationsdaten, kontrolliert die Kommunikationsbeziehungen und Kommunikationspartner, reglementiert die Kommunikation nach einer Sicherheitspolitik, protokolliert Ergebnisse und alarmiert gegebenenfalls bei bestimmten Verstößen den Sicherheits-Administrator.

Firewalls werden in erster Linie genutzt, um die Anbindung an das Internet in vielerlei Hinsicht sicherer zu machen. Doch auch das Aufteilen in Segmente oder Subnetze ist sinnvoll, insbesondere bei großen Netzwerken.

Es sind zwei grundsätzlich verschiedene Funktionsweisen (Firewall-Sicherheitsregeln) von Firewalls zu unterscheiden:

- Default Deny: Hierbei lässt die Firewall nur vordefinierte Datentypen durch, alles andere wird verworfen. Mit anderen Worten: Alles, was nicht ausdrücklich erlaubt ist, ist verboten.
- Default Permit: Diese Firewall konfiguriert man mit Regeln, die in einem Abblocken der Daten resultieren. Sämtliche Daten, die nicht von den Sicherheitsregeln abgedeckt werden, werden durchgelassen. Mit anderen Worten: Alles, was nicht ausdrücklich verboten ist, ist erlaubt.

Beide Vorgehensweisen weisen sowohl Vorteile als auch Nachteile auf, das heißt, man kann mit beiden Typen sowohl sichere als auch unsichere Firewalls bauen. Am sichersten ist jedoch die Methode des *default deny,* wenn man sich gut überlegt, welche services man

freigibt. Bei *default permit* muss man wesentlich mehr Aufwand in die Definition der Abweisungsregeln stecken.

Häufig wird eine Kombination von Firewalls und anderen Netzwerksicherheitskomponenten (z. B. Secure Routers) benutzt, um eine DMZ (Demilitarized Zone) zu ermöglichen. Eine DMZ ist für die Einrichtung einer „Trusted Zone" zwischen dem (unsicheren) Internet und dem (vertraulichen) LAN sinnvoll, um eine höhere Sicherheit zu gewährleisten (vgl. Abb. 3–51).

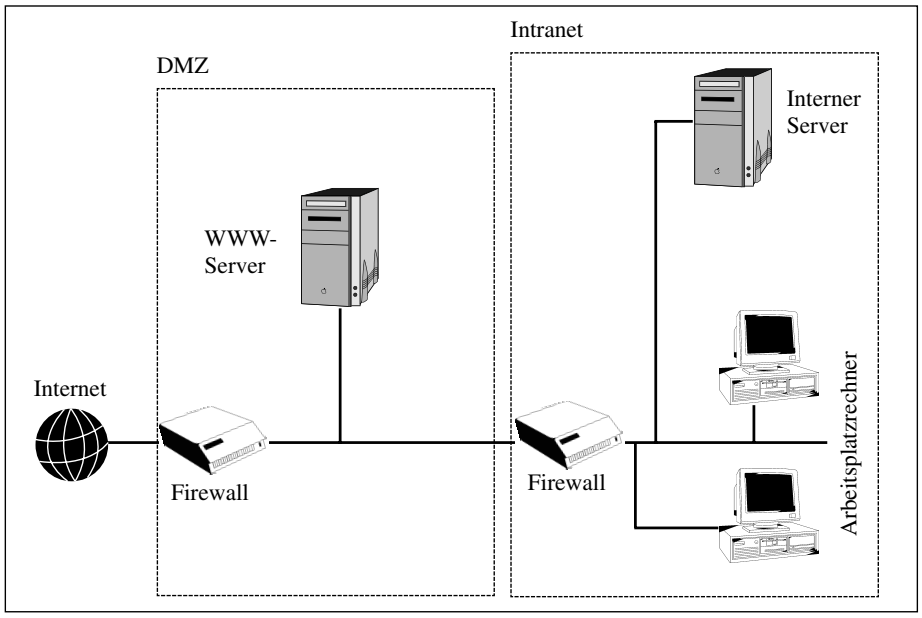

Abb. 3–51: Netzstrukturierung (Teufel/Erat 2001, S. 231)

Diese Konstruktion ist sinnvoll, wenn man neben dem LAN zusätzlich einen Webserver nutzt. Dabei wird sowohl der Webserver als auch das LAN durch die Firewall gesichert. Den Mitarbeitern ist der Zugriff auf den Webserver und das Internet möglich, jedoch können Internetuser über die Firewall nur auf den Webserver zugreifen.

3.11 Electronic Commerce

3.11.1 Definition und Merkmale von Electronic Commerce

Der Begriff **Electronic Commerce** wird in Wissenschaft und Praxis uneinheitlich verwendet. Die Ursache hierfür liegt in der Vielfalt der Einsatzbereiche des Electronic Commerce. Je nach Betrachtungsperspektive reichen die Facetten des Electronic Commerce vom elektronischen Einkaufen (Electronic Shopping bzw. Online Shopping) bis hin zur komplexen Vernetzung von Unternehmen und ihren Partnern. „Aus einer allgemeinen Perspektive versteht man unter Electronic Commerce alle Formen der **elektronischen Geschäftsabwicklung** über öffentliche und private Computer-Netzwerke (z. B. Internet)" (*Hermanns/Sauter* 1999, S. 14).

Die Abwicklung von Geschäften über elektronische Medien erfordert die Ausgestaltung zahlreicher Kommunikations- und Entscheidungsprozesse zwischen Transaktionspartnern. Hierbei lassen sich verschiedene Phasen unterscheiden, von der Information des Transaktionspartners über die Abwicklung von Bestell- und Kaufvorgängen, der Bezahlung und Auslieferung von Waren bis zum After-Sales-Service (vgl. Abb. 3–52), wobei im Fall materieller Produkte eine Online-Distribution natürlich nicht möglich ist.

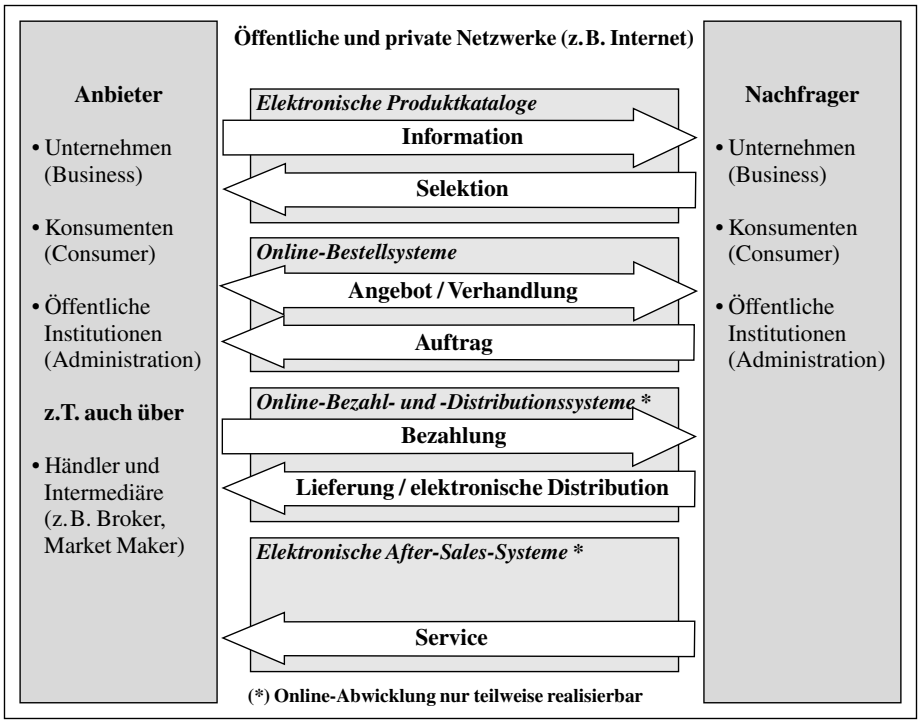

Abb. 3–52: Phasen der digitalen Geschäftsabwicklung beim Electronic Commerce (Hermanns/Sauter 1999, S. 16)

E-Commerce zeichnet sich durch fünf Elemente aus:

– Digitalisierung
– Vernetzung
– Interaktivität
– Unmittelbarkeit
– Standardisierung.

Aufbauend auf diesen Prinzipien entstand E-Commerce in verschiedenen Ausprägungen, wobei nachfolgend die Bereiche B2B (Business-to-Business) und B2C (Business-to-Consumer) im Vordergrund stehen (vgl. Abb. 3–53).

Die Gegenüberstellung der Merkmale einer stationären Verkaufsfläche und eines Online-Shops verdeutlicht die wesentlichen Unterschiede zwischen beiden Geschäftsansätzen (vgl. Abb. 3–54).

Anbieter der Leistung	*Nachfrager der Leistung*		
	Consumer	**Business**	**Administration**
Consumer	**Consumer-to-Consumer** z.B. Internet-Kleinanzeigenmarkt	**Consumer-to-Business** z.B. Jobbörsen mit Anzeigen von Arbeitsuchenden	**Consumer-to-Administration** z.B. Steuerabwicklung von Privatpersonen (Einkommenssteuer etc.)
Business	**Business-to-Consumer** z.B. Bestellung eines Kunden in einer Internet-Shopping Mall	**Business-to-Business** z.B. Bestellung eines Unternehmens bei einem Zulieferer per EDI	**Business-to-Administration** z.B. Steuerabwicklung von Unternehmen (Umsatzsteuer, Körperschaftssteuer etc.)
Administration	**Administration-to-Consumer** z.B. Abwicklung von Unterstützungsleistungen (Sozialhilfe, Arbeitslosenhilfe etc.)	**Administration -to-Business** z.B. Beschaffungsmaßnahmen öffentlicher Institutionen im Internet	**Administration -to-Administration** z.B. Transaktionen zwischen öffentlichen Institutionen im In- und Ausland

Abb. 3–53: Markt- und Transaktionsbereiche des Electronic Commerce

Stationäre Verkaufsfiliale	**Online-Shop**
Reklamations- und Umtauschhandling via Filiale an Zentrale	Reklamations- und Umtauschhandling via Callcenter und Postversand
Persönliches Einkassieren, Bargeldhandling, Ladendiebstähle	Elektronisches Inkasso, Bonitätsprüfung, evtl. Nachnahme, Debitorenverluste
Persönlicher Verkauf in der Filiale, Continous Replenishement	Personalisierte digitale Verkaufs- und Kundenbindungsmaßnahmen, CRM
Wareneingang Filiale, Verteilung, verkaufsgerechte Warenpräsentation, Deko	Kosten durch mehrfache oder erfolglose Zustellung, evtl. Pick-Up-Service
Wenige Sammellieferungen an Filialen	Viele Einzelversendungen als Paket an Kunden
Waren in filialgerechte Einheiten komissionieren, auszeichnen	Waren endkundengerecht komissionieren, verpacken, versenden
Mietkosten der Verkaufsfilialen (beinhalten die Passantenfrequenz)	Promotionsmaßnahmen für den E-Shop
Verkaufsfilialen einrichten u. unterhalten, Inventar kalkulatorisch abschreiben	E-Commerce-Informatikinfrastruktur einrichten, unterhalten, kalk. abschreiben
Finanzierung Warenlager Zentrale und Filialen	Finanzierungszeiten Warenlager Zentrale
Unternehmenszentrale mit modernem ERP-System, zentrales Management, eigene Logistikinfrastruktur mit Zentrallager, Stammdatenpflege	

Abb. 3–54: Stationäre Verkaufsfiliale versus Online-Shop (Schubert u.a. 2001, S. 31)

3.11.2 Electronic Commerce und Logistik

Für die Beurteilung der strategischen Implikationen von E-Commerce auf die Logistik sind drei wesentliche Effekte relevant (vgl. Abb. 3–55) (vgl. *Schmitt* 2003, S. 174): Erstens wird der bislang bestehende Reichhaltigkeits-Reichweiten-Kompromiss der Informationsübermittlung durchbrochen. In der Vergangenheit war es möglich entweder wenig reichhaltige Informationen an einen großen Empfängerkreis (z. B. Werbeinformationen) zu distribuieren oder aber reichhaltige interaktive Informationen mit geringer Reichweite (z. B. Außendienstgespräche) zu verteilen. Mithilfe von E-Commerce lassen sich nunmehr reichhaltige Informationen mit hoher Reichweite distribuieren, was insbesondere Auswirkungen auf die Vertriebsaktivitäten hat. Zweitens führt E-Commerce aufgrund einer generellen Verringerung der Transaktionskosten zu einer Bedeutungsverschiebung zwischen den drei grundsätzlichen Transaktionsmechanismen Märkte, Kooperationen und Organisationen. Der hierarchische Austauschmechanismus Organisation verliert gegenüber den beiden anderen an Bedeutung, was dazu führt, dass organisatorische Grenzen neu gestaltet werden. Externer Bezug von bislang unternehmensintern erstellten Leistungen wird wirtschaftlich zunehmend sinnvoll. Zum dritten wirkt sich E-Commerce auf die Ressourcenposition von Unternehmen aus. Wettbewerbsrelevante Ressourcen können infolge von E-Commerce leichter transferiert werden. Demzufolge sind bisher stabil erscheinende Geschäftsmodelle neuen Bedrohungen ausgesetzt und es entstehen neue Geschäftsmodelle.

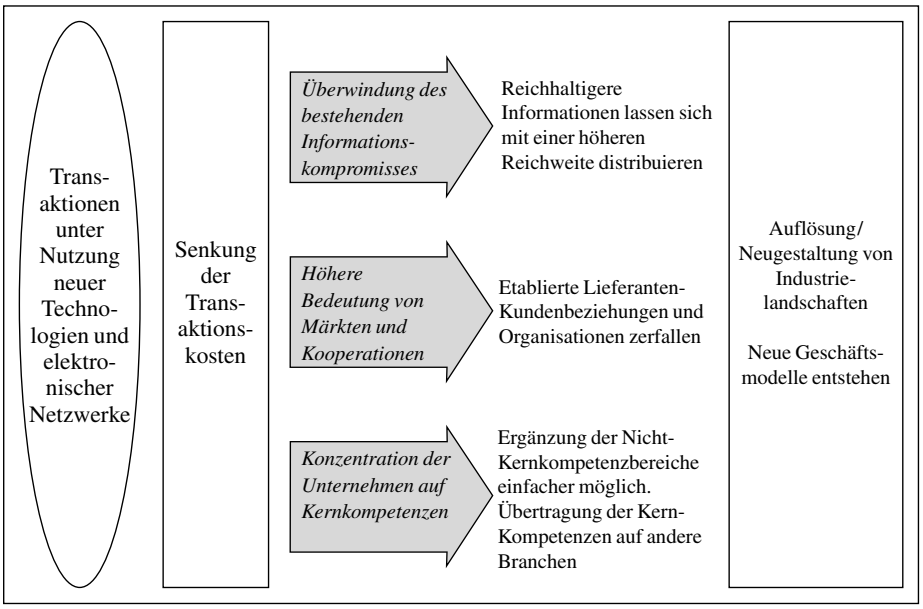

Abb. 3–55: Strategische Auswirkungen des E-Commerce (vgl. Weber u. a. 2002, S. 54)

Für die Logistik sind vier generelle Entwicklungsrichtungen relevant, die durch E-Commerce neu entstehen oder beschleunigt werden (vgl. Abb. 3–56) (vgl. hierzu *Schmitt* 2003, S. 180 ff.):