Supply-Chain-Management:

IT-Sicherheitsmanagement wird immer wichtiger

Dipl.-Kfm. (FH)/B.A. David Oing ist Prokurist bei der Demes Logistics GmbH & Co. KG in Stadtlohn und dort verantwortlich für das Ressort Business Controlling und Information Technology (IT). Darüber hinaus forscht David Oing als externer Doktorand am Institut für Wirtschaftsinformatik, insbesondere Informationsmanagement, an der Universität Leipzig unter der Leitung von Prof. Dr. Bogdan Franczyk. Forschungsbereiche sind: RFID, Logistik und Supply Chain Management.

Kontakt:

Demes Logistics GmbH & Co. KG
Boschstraße 27
D-48703 Stadtlohn
Tel.: +49 (0) 25639302-28
Fax: +49 (0) 25639302-37
E-Mail: david.oing@demes-logistics.com
Website: www.demes-logistics.com

Supply Chain Management:

IT-Sicherheitsmanagement wird immer wichtiger

Von Dipl.-Kfm. (FH)/B. A. David Oing

Die Umsetzung von modernen Logistikkonzepten in Beschaffung, Produktion und Distribution ist globalisierungsbedingt zu einem wichtigen Wettbewerbsfaktor geworden. Um die langfristige Existenz eines Logistikunternehmens zu gewährleisten, ist die Informationstechnologie (IT) und das damit verbundene Sicherheitsmanagement in der Unternehmenspraxis inzwischen unverzichtbar. Wobei der zeitnahe Informationsaustausch sowohl in geschlossenen als auch in offenen Systemen von Logistikunternehmen einen elementaren Eckpfeiler des Erfolges einer Supply Chain darstellt.

Lange Zeit galt die IT als zweitrangig und wurde primär unter Kostenaspekten betrachtet. Seit einigen Jahren wächst ihre Bedeutung jedoch rasant. IT ist ein entscheidender Faktor für den zukünftigen Unternehmenserfolg. Aktuell ermöglicht vor allem das Internet bzw. der auf Informationstechnik basierende Austausch von Informationen in Logistikunternehmen die Einbindung in die Supply Chain. Mit dem Austausch derartiger Informationen geht jedoch auch ein Anstieg von Risiken einher. Dies trifft zu, wenn zum Beispiel die Vertraulichkeit, Verfügbarkeit oder Integrität der Informationen verletzt werden, da bei der Konzeption des Internets den angeführten Schutzzielen nur wenig Beachtung beigemessen wurde. IT stellt einen wichtigen Enabler von Supply Chains dar. Aber erst ein adäquates Sicherheitsmanagement führt diese zum Erfolg.

Vor diesem Hintergrund ist es zwingend erforderlich, Risiken, die bei dem Einsatz von IT-Systemen auf Grund von Gefährdungen bestehen, durch angemessene Maßnahmen zu begegnen. Beim Aufbau eines IT-Sicherheitsniveaus muss organisiert und unternehmensübergreifend vorgegangen werden, da die IT-Sicherheit weit über die Grenzen des eigenen Unternehmens hinausgeht.

Deshalb sollten von den Entscheidungsträgern im Logistikunternehmen aller in eine Supply Chain integrierten Unternehmen ausreichend finanzielle und personelle Ressourcen bereitgestellt werden. Nur dadurch kann ein abgestimmtes IT-Sicherheitsniveau erreicht und vor allem gehalten werden.

Bei der Erstellung eines IT-Sicherheitskonzepts und der Auswahl von sicheren IT-Elementen kann das IT-Sicherheitsmanagement eines Logistikunternehmens auf vielfältige Standards und Kriterien zurückgreifen. Basierend auf IT-Grundschutzkatalogen und dem Standard 100 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) lässt sich eine Vorgehensweise bzw. ein Erfolg versprechendes Verfahren zur Erreichung der IT-Sicherheit in Logistikunternehmen realisieren.

Der Bewertungsansatz auf Basis der ‚Fuzzy-Sets-Theorie' gewährleistet, dass auch das schwächste Glied in dem betrachteten IT-Verbund adäquat Berücksichtigung findet. Die Umsetzung kann zum Beispiel mit Hilfe des Tools Test-ITS erleichtert werden. Dadurch lassen sich Schwachstellen und unter Beachtung der Ressourcen auch die Maßnahmen ermitteln, die für eine Optimierung des Sicherheitsniveau im IT-Verbund sorgen.

Mit Blick auf einen zukünftigen Ausbau der IT-Sicherheit dürfen Logistikunternehmen allerdings nicht den Fehler begehen, das einmal erarbeitete IT-Sicherheitsniveau für eine Art Erfolgsgarantie zu halten. Das IT-Sicherheitsmanagement muss ein Innovationsmotor in ökonomischer Hinsicht sein. Nur ein permanentes Hinterfragen angewandter Kriterien und Standards ist ein Garant für erfolgreiches IT-Sicherheitsmanagement.

Praxistipps für Logistiker

Um sich mit dem Thema IT-Sicherheitsmanagement schnell und effizient vertraut zu machen, empfiehlt das BSI die Beachtung folgender zehn Kriterien:

- *Verantwortliche für IT-Sicherheit:*
  Logistikunternehmen sollten die Verantwortlichkeiten und Kompetenzen eindeutig regeln. Für jede identifizierte Aufgabe muss festgelegt werden, wer die Verantwortung dafür übernimmt. Dabei kommt der Vertretungsregelung eine große Bedeutung zu.
- *Schutz vor Schadsoftware:*
  Der Schutz gegen Computerviren, Spams oder Trojanische Pferde muss auf allen IT-Systemen mit höchster Priorität versehen werden. Dies schließt die Vergabe von minimalen Berechtigungen ein. Auch auf Rechnern ohne Internet-Anschluss sind entsprechende Schutzprogramme Pflicht.
- *Datensicherung:*
  Eine regelmäßige Datensicherung im Unternehmen ist unerlässlich. Dabei ist es wichtig, dass durch entsprechende Tests auch die ordnungsgemäße Datensicherung erfolgt.
- *Sicherheitsrichtlinien:*
  Die Erarbeitung von Sicherheitsrichtlinien steht am Anfang eines Sicherheitskonzepts. Stetige Anpassungen an die aktuellen Entwicklungen sollten dabei Berücksichtigung finden. Ebenso muss sichergestellt sein, dass alle Betroffenen die Sicherheitsrichtlinien kennen.
- *Netz-Trennung:*
  Gerade für Logistikunternehmen ist es wichtig, dass die Übergänge zu fremden Netzen zum Beispiel durch Firewalls geschützt sind. Mobile Endgeräte wie Laptops und Mobiltelefone bilden eine große Schwachstelle mit hohem Schutzbedarf.
- *Update und Patches:*
  Durch regelmäßiges Einspielen von Updates in die IT-Systeme des Logistikunternehmens lassen sich bekannte Schwachstellen auf ein Minimum reduzieren.

- *Dokumentation:*

Gerade im Mittelstand besteht nach Expertenmeinung ein großer Handlungsbedarf in Richtung IT-Dokumentation. Insbesondere in Notfällen ist eine aussagekräftige Dokumentation über die IT-Systemlandschaft unabdingbar.

- *Schulung und Sensibilisierung der Mitarbeiter:*
  Vor allem Schulungen für die Mitarbeiter durch so genannte ‚Awareness-Kampagnen' sind mit überschaubaren Investitionen zu realisieren. Deshalb sollten regelmäßige Maßnahmen durchgeführt werden, um das Sicherheitsbewusstsein bei allen Beteiligten zu fördern.
- *Benutzerverwaltung und Zugriffsberechtigungen:*
  Die strikte Vergabe von Zutritts- und Zugriffsberechtigungen minimieren das Risiko vor möglichen Schäden. Eine systematische Benutzerverwaltung sollte deshalb zum Standard-Prozess im Unternehmen gehören.
- *Schutz sensibler Informationen:*
  Der Schutz von sensiblen Unternehmensdaten ist selbstverständlich. Den Unternehmen steht heute eine Reihe von Möglichkeiten zur Verfügung, um den physischen und technischen Schutz zu gewährleisten.

Werden diese vom BSI empfohlenen Kriterien beachtet und umgesetzt, haben auch international agierende Logistikunternehmen viel für ihr IT-Sicherheitsmanagement geleistet.

In Theorie und Praxis herrscht Einigkeit darüber, welches die Schutzziele von Informations- und Kommunikationssystemen sind, die nach besonderem Schutz in Logistikunternehmen verlangen. Dabei handelt es sich um Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Zurechenbarkeit, Rechtssicherheit und Revisionsfähigkeit sowie Verbindlichkeit.

Vertraulichkeit und Integrität

Informationen innerhalb von Logistikunternehmen sind meistens vertraulich und müssen geschützt werden. Der Aufbau des IT-Systems sollte in der Art und Weise erfolgen, dass ein Zugriff nur für berechtigte Personen zulässig ist. Der Unversehrtheit bzw. Integrität von Daten ist dadurch Rechnung zu tragen, dass Informationen, Systeme und Netze nicht unbemerkt modifiziert werden. Die Beschaffenheit des IT-Systems muss grundsätzlich so gestaltet sein, dass Modifizierungen offensichtlich sind.

Verfügbarkeit und Authentizität

Die Verfügbarkeit der Informationen, Systeme und Netze ist sicherzustellen. Das IT-System muss bei einer Informationsanforderung bzw. dem Zugriff in einem kurzen Zeitraum antworten oder bestimmte Anordnungen durch den Anwender ausführen. Mit der Authentizität ist auf die Echtheit der Identität von Kommunikationspartnern und der Informationen, etwa in einem Logistik-Netzwerk, zu achten. Dabei gilt es zu beweisen, „dass Informationen wirklich von der angegebenen Quelle stammen und die Identität korrekt ist“.

Zurechenbarkeit und Verbindlichkeit

Aus der Authentizität resultiert die Zurechenbarkeit, die zu gewährleisten ist. Informationen und Aktionen können im Regelfall einer auslösenden Instanz, zum Beispiel einer bestimmten Quelle, die Informationen an eine Senke sendet, zugerechnet werden. In diesem Zusammenhang ist schließlich die so genannte Verbindlichkeit als Schutzziel anzuführen, bei der die Nachweisbarkeit des Sendens und Empfangens von Informationen in Kombination mit dem Nachweis der Identität sicherzustellen ist. Dadurch entsteht eine Verbindlichkeit der ausgetauschten Informationen zwischen den Kommunikationspartnern, die unter anderem für elektronische Vertragsabschlüsse erforderlich ist.

Aus dem letztgenannten Aspekt ergeben sich die zu schützenden Aspekte Rechtssicherheit und Revisionsfähigkeit. Das bedeutet, alle für den Rechtsverkehr im IT-System zum Einsatz kommenden Informationen und Aktionen sind gegenüber Dritten nachzuweisen. Wie die zu schützenden Ziele zeigen, umfasst IT-Sicherheit nicht nur technische Merkmale von IT-Systemen, auch organisatorische Maßnahmen und rechtliche Aspekte kommen eine große Bedeutung zu.

IT-Risiken in der Wertschöpfungskette

Ziele, die mit der Integration von IT-Systemen zur Verarbeitung von Informationen in Liefernetze verfolgt werden sollen, sind unter anderem die Verminderung der laufenden Betriebskosten, die Verkürzung der Produkteinführungszyklen, gesteigerte Kundenzufriedenheit und die Erschließung neuer Geschäftsfelder. Auch der Austausch von Informationen über Bestellmengen, zusätzliche Serviceleistungen oder Preisabstimmungen zwischen in Geschäftsbeziehung stehenden Unternehmen ist erforderlich und kann zum Beispiel zu einer Optimierung der Kapazitätsauslastung im Lager eines Logistikunternehmens beitragen. Die Realisierung dieser Ziele erfordert einen medienbruchfreien und kontinuierlichen Informations-austausch über die Unternehmensgrenzen hinweg.

Vor dem Hintergrund der bereits genannten Schutzziele können sich beispielhaft die nachstehenden, ausgewählten Gefahren bzw. Störgrößen und Sicherheitsmaßnahmen in einer Wertschöpfungskette ergeben:

- *Vertraulichkeit:* Vertrauliche Informationen können bei der Kommunikation zwischen zwei in Geschäftsbeziehung stehenden Unternehmen innerhalb der Supply Chain von unbefugten Dritten mitgelesen werden. Hier bietet der Einsatz so genannter Verschlüsselungstechnologien einen Ansatz zur Gewährleistung der Vertraulichkeit.

- *Integrität:* Innerhalb des Unternehmens oder während der Übermittlung zu einem Supply Chain Geschäftspartner werden Informationen unbefugt modifiziert. Hier kann durch vorab bestimmte Zugriffsberechtigungen realisiert werden, dass nur berechtigte bzw. autorisierte Anwender Zugang zu den jeweiligen zu schützenden Informationen bekommen. Eine Modifizierung der Daten kann durch Security-Maßnahmen wie zum Beispiel mit der Streuwertfunktion bzw. der Einweg-Hash-Funktion identifiziert werden.
- *Verfügbarkeit:* Die Funktion eines Servers kann durch einen so genannten ‚Denial of Service' (DoS)-Angriff eingeschränkt bzw. bis zum Zusammenbruch führend gestört werden. Dabei werden Dienste auf etwa einem PC arbeitsunfähig. Dies geschieht in der Regel durch Überlastung. Bei DoS handelt es sich um Angriffe, die Schwachstellen in der Implementierung der Netzwerkfunktionalität verschiedener Betriebssysteme ausnutzen. Eine Möglichkeit zur Abwehr dieser Gefahr besteht in der Implementierung und Anwendung eines Sicherungssystems, etwa einer Firewall. Diese schützt vor externen Angriffen. Ferner kann durch die Bereitstellung von Ersatzsystemen und weiteren Kommunikationsmöglichkeiten den drohenden Angriffen auf das Schutzziel Verfügbarkeit entgegengetreten werden.

In der logistischen Praxis hat zusammenfassend jedes eingebundene Unternehmen sicherzustellen, dass keiner widerrechtlich in den Besitz der etwa zwischen Quelle und Senke kommunizierten Informationen gelangen kann. Ferner muss eine Manipulation ausgeschlossen werden können und zum Beispiel die den Transport begleitenden Informationsströme mittels IT-System geeignet sein und zügig zur Verfügung stehen. Auch ist aus Sicht des jeweiligen Logistikunternehmens zu gewährleisten, dass die Kooperationspartner nur auf die für sie bestimmten bzw. freigegebenen Informationen, nicht jedoch auf interne, vertrauliche Unternehmensdaten

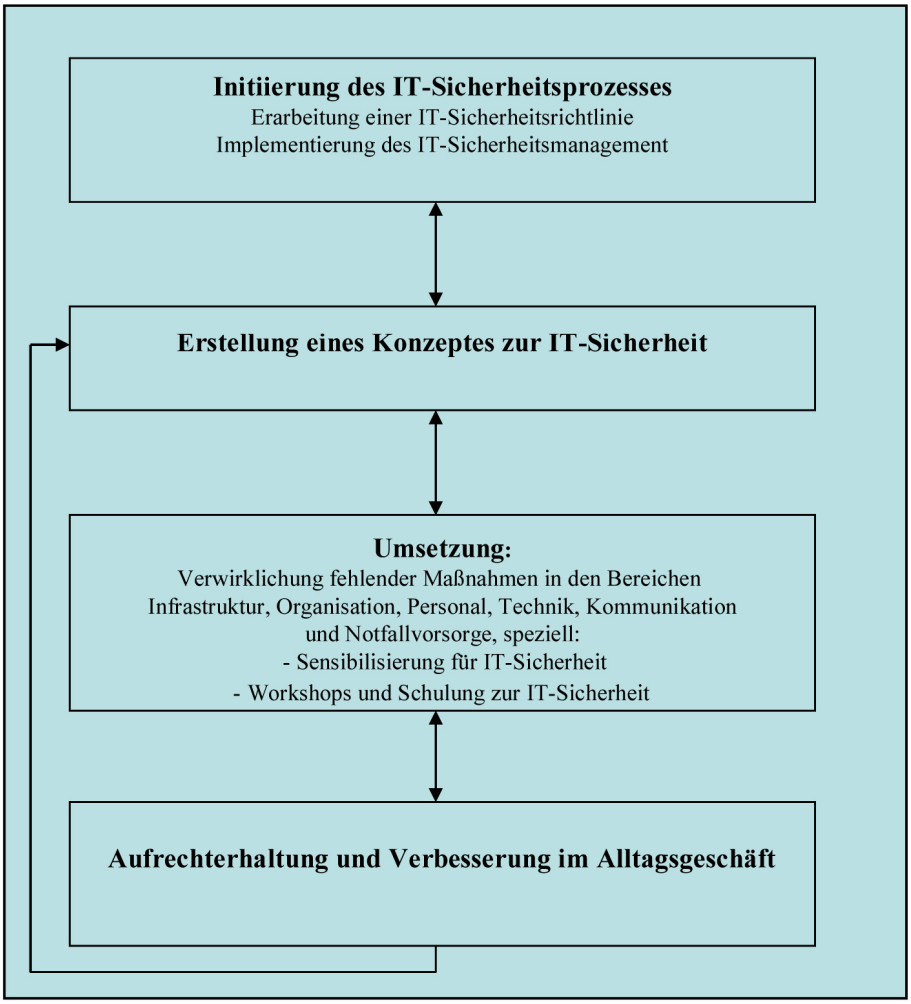
Zugriff erhalten. Mit einem adäquaten Rechtekonzept in Verbindung mit Authentifizierungs- und Autorisierungsmaßnahmen sind diese Aspekte zu realisieren. Beispielsweise bedeutet dies, dass ein Entwickler bei dem von ihm verfassten Dokument in einer Applikation festlegt, welche Rechte ein Geschäftspartner besitzen soll.

IT-Sicherheitsprozess und dessen betriebswirtschaftliche Relevanz

Zu Beginn eines IT-Sicherheitsprozesses steht die Erarbeitung einer IT-Sicherheitsrichtlinie und die Implementierung eines Sicherheits-managements, das in die bestehende Organisationsstruktur des Unternehmens zu integrieren ist. Die Aufgabe dieser Abteilung bzw. des IT-Mitarbeiters besteht darin, ein IT-Sicherheitskonzept zu erarbeiten, einzuführen und anzuwenden. Die Erstellung eines Sicherheitskonzepts ist notwendig, um konkrete Maßnahmen im Logistikunternehmen zu planen, umzusetzen und nach der Implementierung im Alltagsgeschäft zu aktualisieren.

Dabei gibt die so genannte IT-Sicherheitsrichtlinie die Zielsetzung vor und legt die organisatorischen Rahmenbedingungen fest, auf deren Basis ein IT-Sicherheitskonzept zu entwickeln ist. Nach diesen Vorgaben ist innerhalb des IT-Sicherheitskonzeptes der konkrete Schutzbedarf der IT-Anwendungen und IT-Systeme im Logistikunternehmen festzustellen, um in einem weiteren Schritt passende Sicherheitsmaßnahmen zu verwirklichen.

Die nachstehende Grafik zeigt den IT-Sicherheitsprozess im Überblick.



Kosten-Nutzen-Verhältnis

Wegen der problematischen Kostenermittlung eines in Zukunft eintretenden Schadens halten Experten die Behandlung des Sicherheitsniveaus als Variable für wenig praktikabel. Folglich empfiehlt es sich, das Sicherheitsniveau als Größe unabhängig von Kostenaspekten festzulegen und anschließend kostenoptimal umzusetzen. Auch in Logistikbetrieben sind IT-Sicherheitsanalysen meistens nicht realisierbar, da es kompliziert ist, den Nutzen einer Investitionen in die IT-Sicherheit vorab zu quantifizieren. Folglich sollte ein Budget für Sicherheitsmaßnahmen bereitgestellt und bestmöglich verwendet werden.

IT-Strukturanalyse

Die IT-Strukturanalyse dient der Vorerhebung von Informationen, die bei der Erarbeitung eines Konzeptes nach IT-Grundschutz erforderlich sind. Dabei ist die Struktur der in Logistikunternehmen vorhandenen Informationstechnik zu analysieren und zu dokumentieren. Diese Analyse lässt sich in folgende Schritte aufteilen:

- *Netzplanerhebung:*
  Erstellung eines Netzplans, in dem alle Verbindungen und Determinanten des betrachteten IT-Verbundes abgebildet werden. Dabei wird jede IT-Komponente eindeutig bezeichnet und in ihrer Funktion und Eigenschaft beschrieben.
- *Reduktion der Komplexität durch Bildung von Gruppen:*
  Zur Verbesserung der Übersichtlichkeit werden gleichartige Komponenten in Gruppen zusammengefasst. Als Voraussetzung dafür müssen die Komponenten vom gleichen Typ sein, gleich oder nahezu gleich konfiguriert sein, gleich oder nahezu gleich in das System integriert sein, den gleichen Rahmenbedingungen unterliegen und die gleichen Anwendungen bedienen.
- *Erhebung der IT-Systeme:*
  Auf Grund der zu einem späteren Zeitpunkt zu praktizierenden Modellierung erfolgt eine zusammenfassende Aufstellung der IT-Systeme in Form einer Tabelle.
- *Erfassung der IT-Anwendungen und der zugehörigen Informationen:*
  In diesem letzten Schritt der IT-Strukturanalyse werden die auf den betrachteten IT-Systemen laufenden Anwendungen erfasst und dokumentiert.

Schutzbedarfsfeststellung

Der Schutzbedarf der IT-Anwendungen, der IT-Systeme, der Netze und der Infrastruktur ist hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit kritisch zu analysieren. Das Logistikunternehmen muss sich dabei die Frage stellen, welcher Schutz für die Information und die eingesetzte Informationstechnik angemessen ist. Folglich ist abzuwägen, welcher Schaden durch eine Verletzung einer der drei genannten Grundwerte entstehen kann. Dabei ist auch die Beachtung möglicher Folgeschäden relevant.

Bewährt hat sich eine Kategorisierung in folgende Schutzbedarfskategorien:

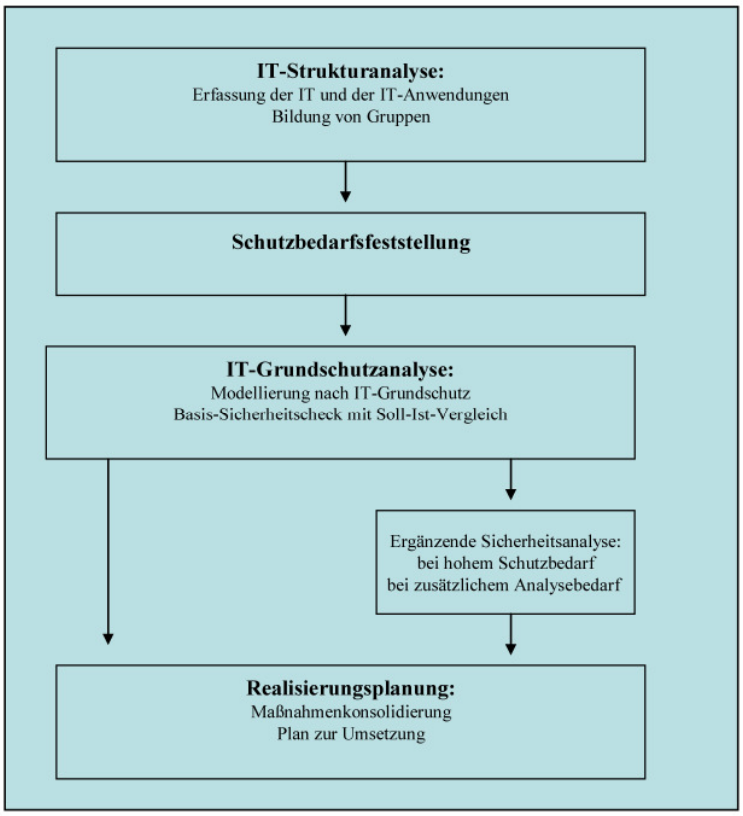
- *Niedrig bis mittel* (Auswirkungen sind begrenzt und überschaubar).
- *Hoch* (Potenzielle Schäden können beträchtliche Auswirkungen haben).
- *Sehr hoch* (Auswirkungen können existenzbedrohend sein bzw. eine katastrophales Ausmaß haben).

Bei der Feststellung des Schutzbedarfs ist darauf zu achten, dass dieser in enger Abstimmung mit den betroffenen Abteilungen erfolgt. Grund: Drohende Gefahren können nur von Mitarbeitern korrekt eingeschätzt werden, die täglich mit der speziellen Anwendungen zu tun haben.

IT-Grundschutzanalyse

Umseitige Abbildung stellt die Modellierung einer adäquaten IT-Grundschutzanalyse dar. Hierbei wird der betrachtete IT-Verbund mit den Bausteinen des Katalogs nachgebildet. Um der in einem Logistikunternehmen in der Regel heterogenen IT-Landschaft eine bessere Struktur auf Aufbereitung zu geben, verfolgt der Grundschutzkatalog ein fünfstufiges Baukastenprinzip. Durch diese sinnvolle Gliederung wird die Komplexität erheblich vermindert und übergreifende Aspekte und infrastrukturelle Fragestellungen getrennt von den IT-Systemen betrachtet.

Stufe 1 thematisiert Grundsatzfragen des IT-Einsatzes, Stufe 2 umfasst den Bereich Technik. Stufe 3 behandelt die administrative Ebene und die aller IT-Nutzer. In Stufe 4 folgende die Netz- und Systemadministratoren und 5 thematisiert schließlich die IT-Anwender.



Akzeptanzprobleme während der Umsetzung

Die Umsetzung neuer Sicherheitsmaßnahmen ist in der Praxis häufig problematisch. Durch die Implementierung neuer IT-Sicherheitsmaßnahmen können zum Beispiel Mitarbeiter ihren Informationsvorsprung gefährdet sehen. Die IT-Optimierung greift zwangsläufig auch in das bislang ausgewogene und traditionell gewachsene Machtgefüge der Abteilungen ein und stellt schnell bisherige Rechte und Kompetenzen in Frage. Das Erreichen einer persönlichen Akzeptanz bei allen Mitarbeitern muss jedoch ein zentrales Ziel eines jeden Logistikunternehmens sein. Erreicht werden kann dies durch Schulungen, Workshops, Testprojekte und Bereichsgespräche.