Wie sich das Risiko IT-Sicherheit bewerten lässt

Die Unternehmensleitung ist für den Fortbestand eines Unternehmens verantwortlich. Sie muss deshalb die Risiken, denen das Unternehmen gegenübersteht, identifizieren und Massnahmen gegen die daraus absehbaren Gefahren ergreifen. Der vorliegende Artikel beschreibt die Aufgabe der Unternehmensleitung, stellt eine Methodik vor, mit der diese Aufgabe strukturiert erfüllt werden kann und stellt Tools vor, welche die Umsetzung der Methodik unterstützen.

VON MARTIN DIETRICH*

Die Geschäftsprozesse eines Unternehmens wurden in den vergangenen zwanzig Jahren immer stärker von der Informatik unterstützt. Dies bedeutet, dass die Informatik immer mehr in die Geschäftsprozesse einbezogen wurde, mit dem Ziel, diese schneller, effizienter, genauer oder einfacher organisieren zu können. In Informatikkreisen wird die Informatik deshalb auch gerne als *Enabler* der Geschäftsprozesse bezeichnet. Die (betriebswirtschaftliche) Unternehmensleitung hingegen konzentrierte sich lange auf die klassischen Bereiche wie Entwicklung, Finanzmanagement, Produktion oder Marketing und sah die Informatik gerne als rein unterstützenden Prozess, der hilft, die Geschäftsprozesse effizienter ablaufen zu lassen. In den letzten Jahren wurde aber auch diesen Führungskräften mehr und mehr bewusst, wie abhängig die Geschäftsprozesse von der Informatik sind.

Mit dieser Bewusstseinsänderung rückte die Informatik und damit auch die Informatiksicherheit vermehrt in das Betrachtungsfeld der Unternehmensleitung. Dieser Vorgang wird zurzeit beschleunigt durch verschiedene internationale Gremien, die auf die Bedeutung der Informatik und damit einhergehend auch auf die Bedeutung der Informatiksicherheit hinweisen und entsprechende Standards erlassen. ITIL beispielsweise definiert die Kernaufgabe der Unternehmensleitung wie folgt: «Abschliessende Beurteilung [der Informatiksicherheit] / Entscheidung [über die Priorisierung von Massnahmen im Bereich Informatiksicherheit] durch das Management unter Berücksichtigung der möglichen unternehmenskritischen Folgen.»

Methodisches Vorgehen: Management-Prozess

Um diese umfassende Kernaufgabe lösen und das Unternehmen vor existenziellen Gefahren schützen zu können, muss die Unternehmensführung folgende Informationen beschaffen:

► Schutzbedarf: Auswirkungen von Störungen (fehlerhafte Informatikunterstützung wie fehlende Verfügbarkeit der Informatikmittel, fehlende oder fehlerhafte Daten, fehlende Gewährleistung der Vertraulichkeit) auf die Geschäftsprozesse.

► Aktueller Sicherheitszustand der Informatik.

► Zusammenspiel der Geschäftsprozesse und der Informatik.

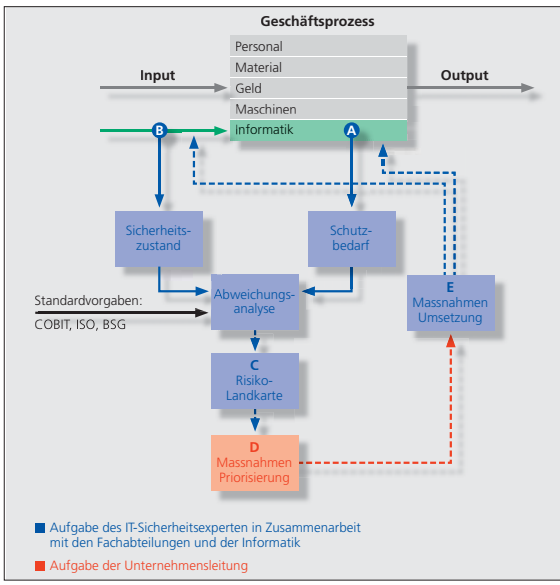
Um diese Informationen zu erhalten, muss die Unternehmensleitung einen Management-Prozess implementieren, in dem verschiedene Stellen (Fachabteilungen, Informatik, eventuell externe Spezialisten) zusammenarbeiten, die notwendigen Detaildaten erheben, aggregieren und für die Unternehmensleitung zusammenstellen.

Neben der Implementierung des Management-Prozesses und der damit einhergehenden strukturierten Informationsbeschaffung muss die Unternehmensleitung auch dessen Einhaltung (Compliance) nachweisen.

Auf den ersten Blick scheint die Erfüllung dieser Aufgaben einen übermässigen finanziellen und personellen Aufwand zu erfordern. Es ist allerdings nicht das erste Mal, dass solche Forderungen an die Unternehmensführung gestellt werden. Bereits bei der Einführung des Qualitätsmanagements wurden dieselben Forderungen gestellt. Mit der Implementierung eines strukturierten Qualitätsmanagements und einem entsprechenden Qualitätskontrollkreislauf (Qualitäts-Sicherung oder Quality Assurance) gehört die Erledigung dieser Aufgaben mittlerweile zur Routine. Sie haben die Qualität der Prozesse als auch der Endprodukte verbessert. Nun gilt es, in der Informatiksicherheit einen analogen Prozess aufzubauen. Der folgende Abschnitt zeigt, welche Arbeiten im Detail notwendig sind.

A: Auswirkungen auf die Geschäftsprozesse

Um die Auswirkungen auf die Geschäftsprozesse zu bestimmen, braucht es die Prozessverantwortlichen. Nur sie sind in der Lage, zwischen einem wirklich grossen Problem und einem Ärgernis unterscheiden zu können. Der Geschäftsprozessverantwortliche weiss, wie viele Mitarbeiter bei einem Informatikausfall nicht mehr arbeiten können und nach welcher Zeit seine Kunden davon direkt betroffen sind. Er weiss auch, ob Fehler in den Daten an weitere Abteilungen weitergegeben werden und dort für Fehler noch grösseren Ausmasses verantwortlich sein könnten oder ob ein Fehler in den Daten nur zu einem verfälschten Archiv führt.



Der IT-Security Management Prozess.

Es ist notwendig, dass mit den Spezialisten aus den Fachabteilungen ein strukturierter Risikodialog geführt wird. Dabei werden die wichtigsten Geschäftsprozesse bezüglich ihrer Anfälligkeit auf Störungen unter die Lupe genommen. In diesem Risikodialog leitet der IT-Sicherheitsexperte, mittels Szenario-Techniken, die Prozessverantwortlichen an, die Auswirkungen auf ihren Prozess und somit auf das Unternehmen identifizieren zu können. Das Basiswissen, welches der IT-Sicherheitsfachmann mitbringen muss, ist das Wissen, welche Informatikprobleme durch welche Bedrohungen eintreten können. Wenn also der Prozessverantwortliche feststellt, dass ein Informatikausfall von zwei Tagen ein Problem darstellt, welches sich auf die Kunden nieder-

schlägt und welches zur Folge hat, dass das Unternehmen wichtige Kunden verlieren könnte, dann liegt es am Informatiksicherheitsexperten, die möglichen Bedrohungen wie Hochwasser, Brand im Rechencenter, Stromausfall oder Viren als mögliche Ursache eines zweitägigen Ausfalls identifizieren zu können. Es liegt aber auch am IT-Sicherheitsfachmann, den Totalausfall eines einzelnen Arbeitsplatzrechners als nicht kritisch für das Unternehmen zu identifizieren, da dieser innert zwei Tagen ersetzt werden kann und im Unternehmen weitere Arbeitsplatzrechner vorhanden sind, die für den Prozess verwendet werden können. Anders würde es aussehen, wenn bereits ein fünfminütiger Computerausfall zu ernsthaften Problemen in der Kundenzufriedenheit führen würde. Dann wäre auch der Ausfall eines einzelnen Arbeitsplatzrechners kritisch.

B: IT-Sicherheitsaudit

Der IT-Sicherheitsaudit hat zum Ziel, den aktuellen Sicherheitszustand der Informatik zu überprüfen und zu dokumentieren. Um diese Überprüfung in einer praktikablen Art und Weise durchführen zu können, kann die Informatik in fünf Objektklassen unterteilt werden:

► Infrastruktur (Rechencenter und dazugehörige Infrastrukturkomponenten)
► Server (technische Serverinstallationen)
► Operating/Administratoren (Mitarbeitende der Informatik sowie deren Arbeitsplätze)
► Kommunikation (Übermittlungsnetze und Kommunikationseinrichtungen sowie die eng mit dem Netz verbundenen Dienste, insbesondere E-Mail-Dienste und Web-Services)
► Benutzer (Mitarbeitende sowie deren Arbeitsplätze)

Innerhalb dieser Objektklassen müssen nun die Informatikobjekte in der geeigneten Granularität definiert werden. Eine zu tiefe Detaillierung der Informatikobjekte bis auf die einzelnen Komponenten, wie sie in verschiedenen Unternehmen auf Grund des ITIL-Standards teilweise erfolgt, ist nicht zielführend. Als sinnvoll und praxistauglich hat es sich bewährt, die Informatikobjekte in Gruppen zusammenzufassen, die in sich gleich sind, zum Beispiel:

► Server: Microsoft, Unix, AS400.
► Benutzer: Backoffice, Management, Telearbeiter, Personal/HR, Marketing, Produktion.

Im IT-Sicherheitsaudit wird nun der aktuelle Sicherheitszustand jedes Informatikobjekts mittels Kontrollfragen ermittelt. Auf Grund der Antworten auf die einzelnen Kontrollfragen kann für jedes Informatikobjekt der aktuelle Sicherheitszustand bestimmt werden.

C: Risikolandkarte

Gemäss der ITIL-Methodik lassen sich die Geschäftsprozesse und die Informatikobjekte miteinander in Beziehung setzen. Dazu werden in der ITIL-Matrix für jeden Geschäftsprozess diejenigen Informatikobjekte identifiziert, die den entsprechenden Geschäftsprozess unterstützen.

So benutzt jeder Prozess einen oder mehrere Server (für die Applikationen) beziehungsweise Servergruppe, der oder die von der entsprechenden Administratorengruppe betreut wird und in einem Rechencenter steht. Dazu läuft der Prozess über eines oder mehrere Netzwerke. Der Prozess wird zusätzlich von einer oder mehreren Benutzergruppen bedient.

Nachdem nun die Geschäftsprozesse und die Informatikobjekte miteinander in Beziehung gesetzt wurden, kann die ITIL-Matrix mit weiteren Daten aus dem Management-Prozess gefüllt werden. Aus dem Risikodialog (Aufgabe A) ist bekannt, welche Geschäftsprozesse einen hohen Schutzbedarf haben, welche Geschäftsprozesse also sehr stark von einer funktionierenden Informatik abhängig sind, und welche Geschäftsprozesse weniger stark von einer funktionierenden Informatik abhängig sind. Aus dem IT-Sicherheitsaudit (Aufgabe B) ergibt sich der aktuelle Sicherheitszustand der Informatikobjekte. Der Informatiksicherheitsexperte kann auf Grund dieser Angaben, also aus dem Schutzbedarf des Geschäftsprozesses und dem Sicherheitszustand der für den Geschäftsprozess notwendigen Informatikobjekte, eine detaillierte und unternehmensspezifische Risikolandkarte der Informatiksicherheit erstellen. Da alle Daten strukturiert erhoben

Verknüpfung von Geschäftsprozessen und Informatikobjekten

Informatikobjekte (Sicherheitszustand) / Geschäftsprozesse (Schutzbedarf)	Server			Infrastruktur		Netz			Operating			Benutzer		
	Windows	AS/400	Unix	Werk A	Werk B	LAN Werk A	LAN Werk B	WAN	Windows	AS/400	Unix	Produktion	Entwicklung	Büro, Mgmt, Aussendienst
Logistik (Supply Chain Mgmt inkl. Business Warehouse)		×		×		×				×		×		
Produktentwicklung			×		×		×				×		×	
Büroautomation inkl. E-Mail	×			×	×	×	×	×	×					×
Complaint Management	×				×		×		×					×
Finanz- und Rechnungswesen		×		×		×				×				×
Personalabteilung (HR)		×		×		×				×				×

Verknüpfung von Geschäftsprozessen und Informatikobjekten: Die × werden dort gesetzt, wo ein Informatikobjekt einen Geschäftsprozess unterstützt.

und ausgewertet wurden, ist die Risikolandkarte jederzeit nachvollziehbar.

D: Risiken beurteilen und Prioritäten setzen

Mit der nun vorliegenden Risikolandkarte der Informatiksicherheit kann die Unternehmensleitung aktiv arbeiten. Sie kann entscheiden, in welchen Geschäftsprozessen der Schutzbedarf mit organisatorischen Massnahmen gesenkt und für welche Informatikobjekte der Sicherheitszustand erhöht werden muss. Die Unternehmensleitung muss die dazu notwendigen Entscheide fällen, möglicherweise Projekte starten und die erforderlichen finanziellen und personellen Ressourcen freigeben.

Die detaillierte Planung und Umsetzung der organisatorischen und technischen Massnahmen obliegt den internen und/oder externen Experten in den Fachabteilungen und der Informatikabteilung (Aufgabe E). Die Unternehmensleitung muss sich aber regelmässig über den Fortgang der Projekte orientieren und diese aktiv unterstützen.

Umsetzung in der Praxis

Um die im zweiten Teil vorgestellte Methodik mit vertretbarem Aufwand durchführen zu können und zu nachvollziehbaren Resultaten zu kommen, ist es unumgänglich, die Verantwortlichen mit Tools zu unterstützen. Die einzusetzenden Tools müssen die Routinearbeiten abnehmen und die Verantwortlichen in der strukturierten Arbeit unterstützen. Routinearbeiten sind beispielsweise:

- ► Auflistung aller möglichen Bedrohungen
- ► Bewertung möglicher Schäden
- ► Umgang mit Wahrscheinlichkeiten
- ► Definition der Kontrollfragen, Definition eines Grundschutzes
- ► Abgleich mit internationalen Standards
- ► Erstellung von Auswertungen, Soll-Ist-Vergleichen, Pendenzenlisten und Massnahmenvorschlägen
- ► Durchführen eines Benchmarkings
- ► Erstellung managementgerechter, grafischer Darstellungen.

Gute Tools zeichnen sich dadurch aus, dass unterschiedliche Anwender bei gleichen Situationen zu gleichen Resultaten kommen.

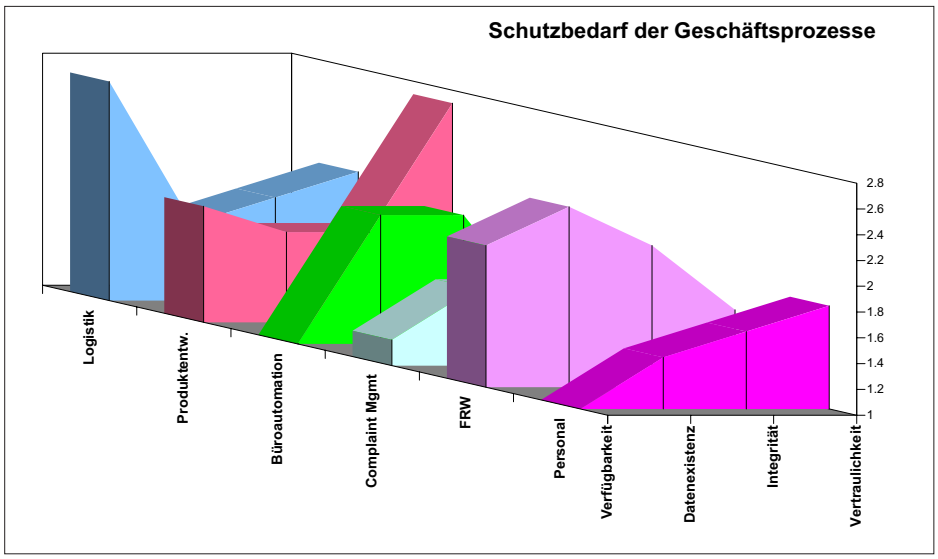
Der folgende Teil des Artikels zeigt, wie die Tools in der Praxis eingesetzt werden und wie die Resultate die Entscheidungsfindung der Unternehmensleitung vereinfachen.

Aus dem Risikodialog (Aufgabe A) lässt sich der Schutzbedarf («Wie viel Sicherheit braucht der Geschäftsprozess?») detailliert ableiten und der Unternehmensführung in einer geeigneten Form veranschaulichen.

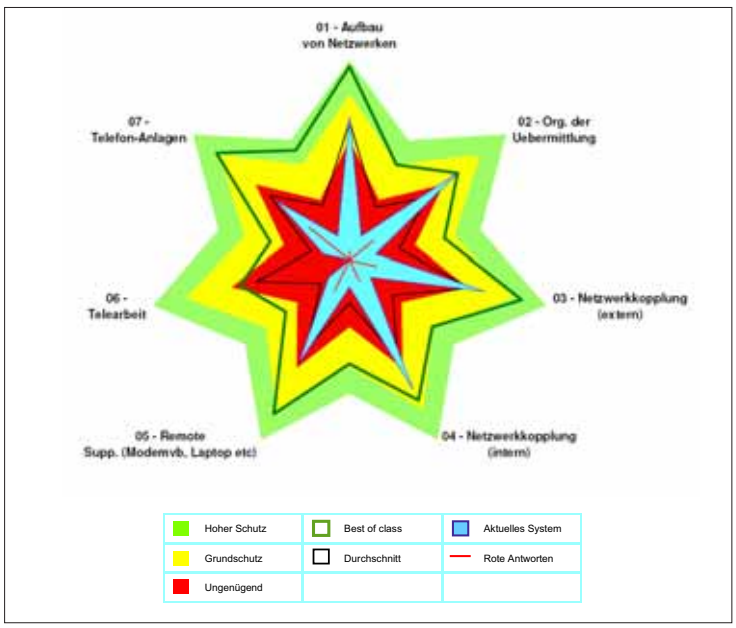
Im IT-Sicherheitsaudit wird der aktuelle Sicherheitszustand jedes Informatikobjekts mittels Kontrollfragen ermittelt. Im eingesetzten Tool sind jeder Kontrollfrage drei verschiedene mögliche Zustände (Antworten) zugeordnet:

- ► Grundschutz: Als Grundschutz akzeptierte Massnahmen sind implementiert.
- ► Hoher Schutz: Der Grundschutz wird übertroffen.
- ► Ungenügender Schutz: Der Grundschutz wird verfehlt.

Der Einfluss jeder Kontrollfrage auf die vier Dimensionen der Informatiksicherheit (Verfügbarkeit, Datenexistenz, Integrität, Vertraulichkeit) ist im eingesetzten Tool hinterlegt und wird dazu verwendet, einen aussagekräftigen Vergleich zwischen dem Sicherheits-Soll-Zustand



Schutzbedarf der Geschäftsprozesse: Übersicht



Beispiel eines Benchmarks einer Kommunikationseinrichtung.

(abgeleitet aus dem Schutzbedarf der Geschäftsprozesse) und dem Sicherheits-Ist-Zustand zu ziehen. Ebenso lassen sich die Sicherheits-Ist-Zustände der Informatikobjekte innerhalb einer Informatikobjektklasse unternehmensintern oder mit anderen Unternehmen vergleichen. Damit können die Forderungen der internationalen Standards wie Cobit oder ISO17799 erfüllt und ein Benchmarking durchgeführt werden.

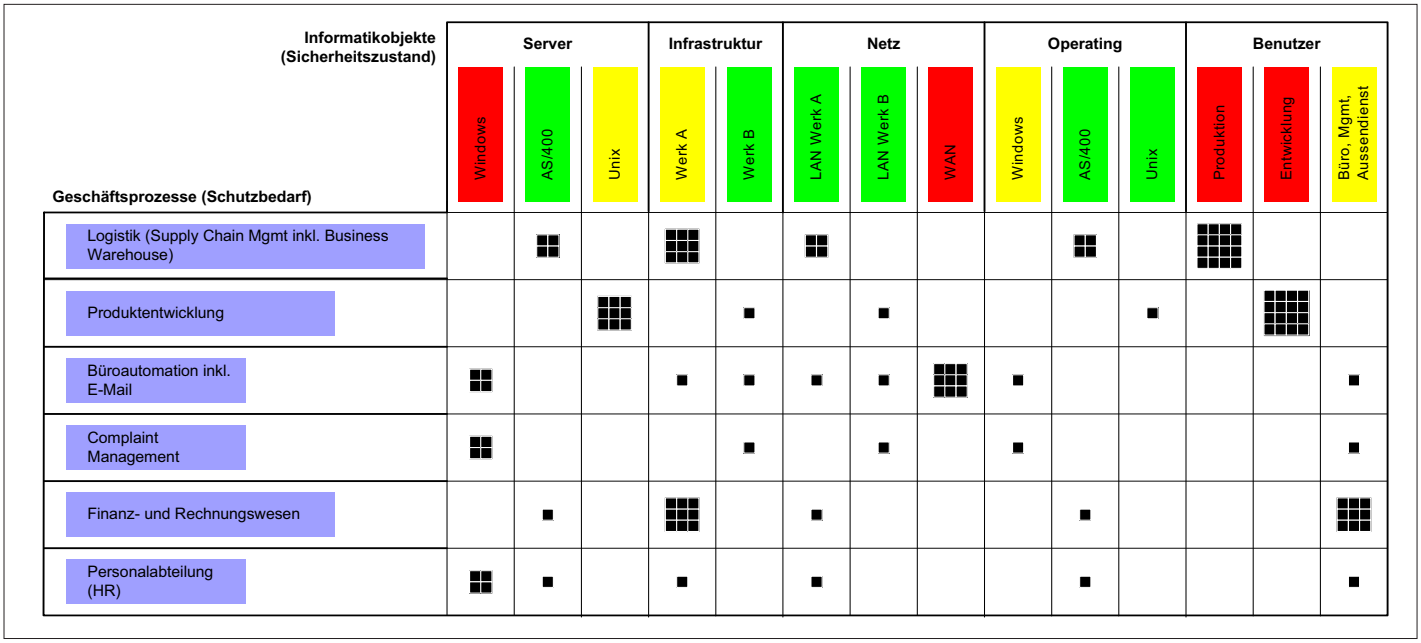
gend geschützt, der Grundschutz ist nicht eingehalten)

Auf Grund der Anforderungen der Geschäftsprozesse an die Informatiksicherheit (Schutzbedarf) und dem Wissen über den aktuellen Sicherheitszustand der Informatikobjekte lassen sich nun innerhalb der ITIL-Matrix die kritischen Bereiche identifizieren und von den unproblematischen Bereichen differenzieren. Dazu werden den Verknüpfungs-

(Rot), weshalb dieser Punkt *existenzbedrohend* ist und dringend genauer betrachtet werden muss.

Risiken beurteilen und Prioritäten setzen

Einerseits lassen sich aus der Risikolandkarte nun Sofortmassnahmen ableiten, und andererseits ist es für die Unternehmensleitung einfach ersichtlich, welche Bereiche prioritär diskutiert werden



Risikolandkarte der Informatiksicherheit.

Entwicklung der Risikolandkarte

Die ITIL-Matrix können wir nun mit den Resultaten aus der Schutzbedarfsanalyse und der Sicherheitszustandsanalyse füllen und so einfach interpretierbar machen.

Dazu hinterlegen wir die Geschäftsprozesse in der ITIL-Matrix mit einem Balken, dessen Länge den Schutzbedarf reflektiert:

► Balken kurz (tiefer Schutzbedarf; Grundschutz ist ausreichend)
► Balken mittel (mittlerer Schutzbedarf; Grundschutz reicht nicht mehr)
► Balken lang (hoher Schutzbedarf; eine funktionierende Informatik ist für das Unternehmen in diesem Bereich absolut kritisch).

Die Informatikobjekte hinterlegen wir auf Grund des aktuellen Sicherheitszustandes mit den drei Farben:

► Grün: Hoher Sicherheitszustand (das Informatikobjekt ist sehr gut geschützt, eine Störung der Informatikunterstützung ist nicht zu erwarten)
► Gelb: Grundschutz (der Grundschutz ist eingehalten)
► Rot: Ungenügender Sicherheitszustand (das Informatikobjekt ist ungenü-

punkten innerhalb der ITIL-Matrix vier Zustände zugeordnet:

▪ alles in Ordnung

▪ im Auge behalten

▪ Gefahr droht

▪ existenzbedrohend

Eine ausgefüllte Risikolandkarte der Informatiksicherheit liest sich wie folgt:

Der Geschäftsprozess *Produktentwicklung* hat einen mittleren Schutzbedarf (Balken mittel), der Grundschutz reicht also nicht mehr aus. Die Produktentwicklung benutzt *Unix-Server*, die einen Sicherheitszustand *Grundschutz (Gelb)* aufweisen: Hier droht Gefahr, da dieser Sicherheitszustand den Schutzbedarf nicht abdecken kann. Die Server für die Produktentwicklung befinden sich in Werk B, welches einen hohen Sicherheitszustand (Grün) aufweist. Hier ist alles in Ordnung. Auch das LAN im Werk B und die Unix-Operatoren haben einen hohen Sicherheitszustand (Grün). Hingegen gehen die Anwender in der Entwicklung fahrlässig mit ihren Informatikmitteln um

müssen und welche Bereiche zurzeit keine zusätzlichen Tätigkeiten erfordern. Organisatorische und technische Massnahmen müssen auf Grund der Risikolandkarte in Auftrag gegeben und die finanziellen und personellen Ressourcen freigegeben werden, um den Schutzbedarf der Geschäftsprozesse zu senken und/oder den Sicherheitszustand der Informatikobjekte zu erhöhen.

Mit der Implementierung des Management-Prozesses muss gewährleistet werden, dass sowohl die Schutzbedarfsanalysen als auch die Überprüfung des Sicherheitszustandes regelmässig durchgeführt werden. Damit ist die Risikolandkarte für die Informatiksicherheit immer auf einem aktuellen Stand und die Unternehmensleitung laufend über die aktuellen Risiken bezüglich Informatiksicherheit informiert. Sie kann damit die notwendigen Prioritäten setzen, die laufenden Projekte überwachen und die Ressourcen zielgerichtet einsetzen.

** Martin Dietrich, lic. oec. HSG, CISA, studierte Informationsmanagement. Er leitet die Entwicklung der BSGITSEC ToolBox der BSG Unternehmensberatung und führt IT-Sicherheitsaudits durch.* ■