Zeitschrift: Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

Herausgeber: Swisscom

Band: 79 (2001)

Heft: 2

Artikel: Qualitätssicherung in der Internettechnologie

Autor: Altmeier, Jörg

DOI: https://doi.org/10.5169/seals-876518

Internettechnologie

Qualitätssicherung in der Internettechnologie

Nur wenn auch der Themenbereich IT-Sicherheit in das Konzept eines ganzheitlichen Qualitätsmanagements eingebunden wird, ist ein Unternehmen fähig, den Herausforderungen des Internetzeitalters zu begegnen. Dieser etwas provokative Gedanke soll aufzeigen, wie wesentlich die Qualitätssicherung der IT-Sicherheit in Zukunft für die Unternehmen sein wird.

JÖRG ALTMEIER

Wie soll diese Qualitätssicherung jedoch angegangen werden? Welche Voraussetzungen müssen geschaffen sein, damit die IT-Sicherheit den geforderten Qualitätssicherungs-Standards genügen kann? Was sind überhaupt gültige Standards? Der Beitrag soll aufzeigen, dass die zurzeit noch vorwiegend technisch orientierte IT-Sicherheit einiges von den Erfahrungen aus dem Bereich Qualitätsmanagement profitieren kann.

Sicherheitsforderungen

Bei der Beschäftigung mit dem Thema IT-Sicherheit tauchen immer wieder folgende Aussagen und Forderungen auf:

- Sicher ist, dass nichts sicher ist.
- Verantwortlichkeit liegt bei der Unternehmensführung.
- Funktionalität darf Sicherheit nicht kompromittieren.
- Das grösste Sicherheitsrisiko sind Mitarbeitende.
- Die Selbstverantwortlichkeit der Mitarbeitenden muss beachtet werden.
- Die Koordination der Verantwortlichen muss organisiert werden.
- Es muss eine Abschottung gegen Missbrauch durch Dritte erreicht werden.
- Die Diskrepanz zwischen potenzieller Gefahr und den eigentlichen Vorkommnissen muss überwunden werden.
- Die Verhältnismässigkeit der Massnahmen sind zu beachten.
- Transparente Sicherheitsregelungen können ohne die erfolgte Umsetzung missbraucht werden.
- Die Qualitätssicherung als begleitende Massnahme sollte eingerichtet werden.

Diese Aussagen legen nahe, dass sich das Management von IT-Sicherheit in seinen Inhalten und Zielen nicht wesentlich von Konzepten anderer Bereiche der Unternehmensführung unterscheidet und zudem Chefsache ist. Wenn aber IT-Sicherheit eine typische Organisationsaufgabe ist, dann ist die Beantwortung der folgenden Fragen wesentlich: Wer gibt den angestrebten Sicherheitslevel, das Ziel vor? Wer ist im Unternehmen für Sicherheit verantwortlich (Aufbauorganisation)? Welche Abläufe und Daten sind überhaupt betroffen? Welche Werkzeuge werden eingesetzt? Mit welcher Strategie werden die Anforderungen realisiert? Wie kann festgestellt werden, ob die Massnahmen wirken? Wichtig ist, dass vor der Einsatzdiskussion diese grundlegenden Fragen beantwortet sind.

Bestehende Qualitätsmanagement-Systeme

Vorgegebene Standards für die IT-Sicherheit sind zurzeit noch nicht vorhanden. Bestehende Zertifikate und Prüfungen behandeln noch ausschliesslich Produkte, beschäftigen sich aber nur unzulänglich mit den Ansprüchen von IT-Abteilungen oder IT-Service-Organisationen. Betrachtet man aber diverse bekannte und eingeführte Managementsysteme, lassen sich dennoch handlungsleitende Fragestellungen für den Nachweis von IT-Sicherheit ableiten.

ISO 9000:2000

Die revidierte Norm ISO/DIS 9000:2000 definiert neue QM-Prinzipien, die als umfassende und grundsätzliche Regeln für das Führen eines Unternehmens verstanden werden. Die Grundsätze zielen auf eine kontinuierliche Verbesserung der langfristigen Leistung mittels der Kundenfokussierung und einer gleichzeitigen Berücksichtigung der Bedürfnisse aller Interessenspartner. Eine direkte Empfehlung oder gar Anforderung für IT-rele-

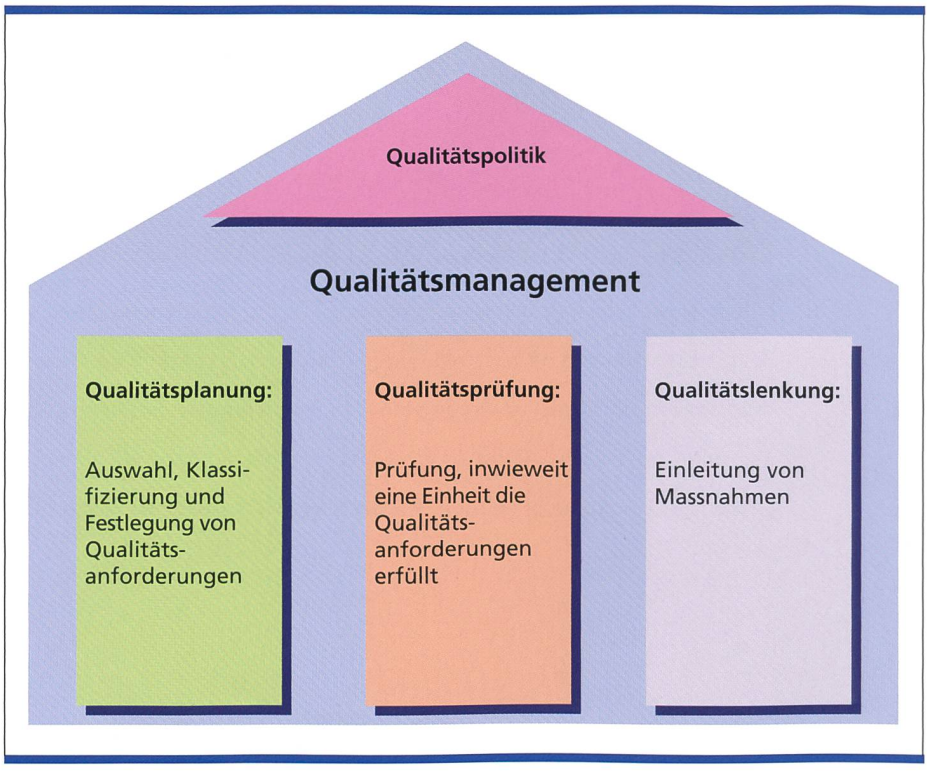

Bild 1. DIN EN ISO/DIS 9000:2000.

vante Sicherheitsmassnahmen ist in der Norm nicht zu finden. Dafür bietet uns die Norm Hilfestellungen zur Strategieformulierung und zur Aufbau- und Ablauforganisation, wie sie auch in IT-Organisationen umgesetzt werden können.

Das CobiT Framework

Control Objectives for Information and Related Technology (CobiT) stellt ein Modell von generell anwendbaren und international anerkannten Kontrollzielen bereit, die in einem Unternehmen implementiert werden sollten, um eine verlässliche Anwendung der Informationstechnologie zu gewährleisten. CobiT unterteilt die notwendigen Massnahmen in vier Gruppen:

Planung und Organisation
Diese umfasst die Strategie und Taktik und betrifft die Bestimmung der Art, wie die Informationstechnologie am besten zur Erreichung der Geschäftsziele beitragen kann. Im Weiteren muss die Realisierung der strategischen Vision für unterschiedliche Ausblicke geplant, kommuniziert und geleitet werden. Schliesslich muss eine geeignete Organisation wie auch eine technologische Infrastruktur bereitstehen.

Beschaffung und Implementation
Um die IT-Strategie zu erreichen, müssen IT-Lösungen identifiziert, entwickelt oder beschafft und implementiert sowie in den Geschäftsprozess integriert werden. Im Weiteren deckt dieser Bereich die Veränderungen und die Wartung von bestehenden Systemen ab.

Betrieb und Unterstützung
Das betrifft die effektive Bereitstellung der gewünschten Dienstleistungen, die bis zur Ausbildung reichen. Zum Betrieb von Dienstleistungen müssen die notwendigen Unterstützungsprozesse etabliert werden.

Überwachung
Alle IT-Prozesse müssen von Zeit zu Zeit auf ihre Qualität und die Erreichung der Kontrollziele überprüft werden.
CoBiT stellt in jedem der vorgestellten Bereiche sicherheitsrelevante Fragen, aus denen sich Anforderungen und Lösungsansätze, insbesondere zur Überprüfung der Massnahmen, lesen lassen.

Das EFQM-Modell

Das European Foundation for Quality Management (EFQM) stellt Kriterien für eine interne Selbstbewertung zur Verfügung und bietet dadurch Orientierungshilfe für die Ausrichtung des Qualitätsmanagements eines Unternehmens.
Dabei stellt das Modell die Führungsverantwortung der Unternehmensleitung und die Selbstverantwortung der Mitarbeitenden in den Vordergrund und fokussiert insbesondere auf die kontinuierliche Verbesserung des einmal Erreichten. Das EFQM-Modell bietet zwar keinen direkten Bezug zur Informationstechnologie, stellt aber deutlich die Selbstverantwortung und die Notwendigkeit der stetigen Verbesserung heraus. Diese beiden Aspekte werden in der momentanen Sicherheitsdiskussion nicht umsonst besonders genau betrachtet.

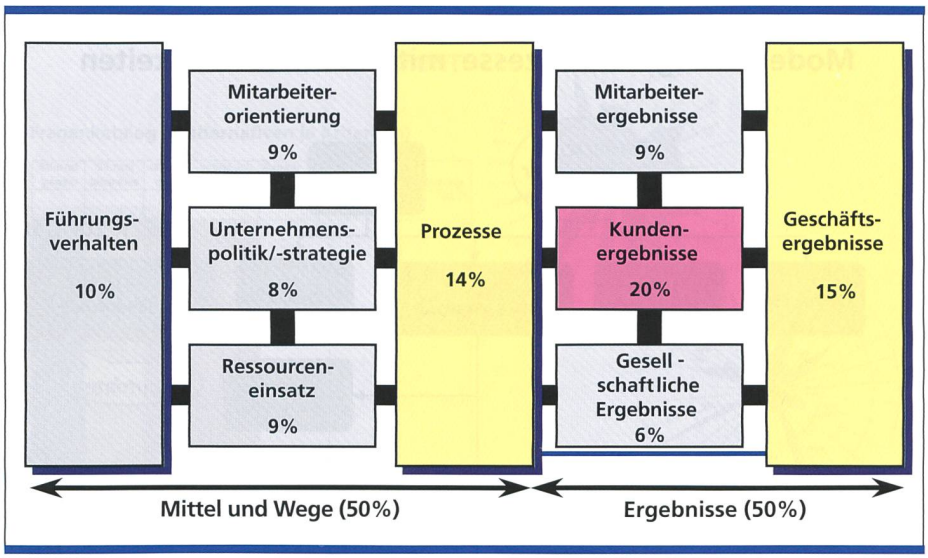

Bild 2. CorbiT Framework.

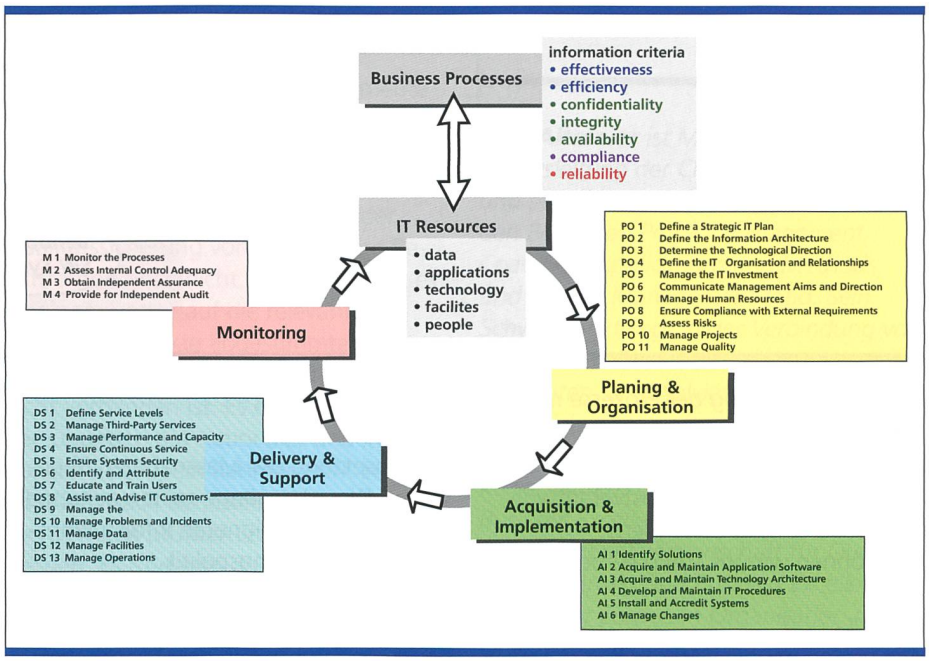

Bild 3. EFQM-Modell für Qualität.

Gemäss Studien geht die grösste Sicherheitsgefahr von internen Mitarbeitenden und der ungenügend aktiven Haltung des Managements aus.
Fasst man die aufgezeigten Hinweise zusammen, wird deutlich, dass die etablierten Qualitätsmanagementsysteme einen grossen Beitrag beim Management von IT-Sicherheit leisten können:

ISO
Wie formulieren wir unsere Sicherheitspolitik und -strategie?
Wie gestaltet sich der Realisierungsprozess?
Wie regeln wir die Verantwortlichkeiten?
Wie beschreiben wir die relevanten Abläufe?

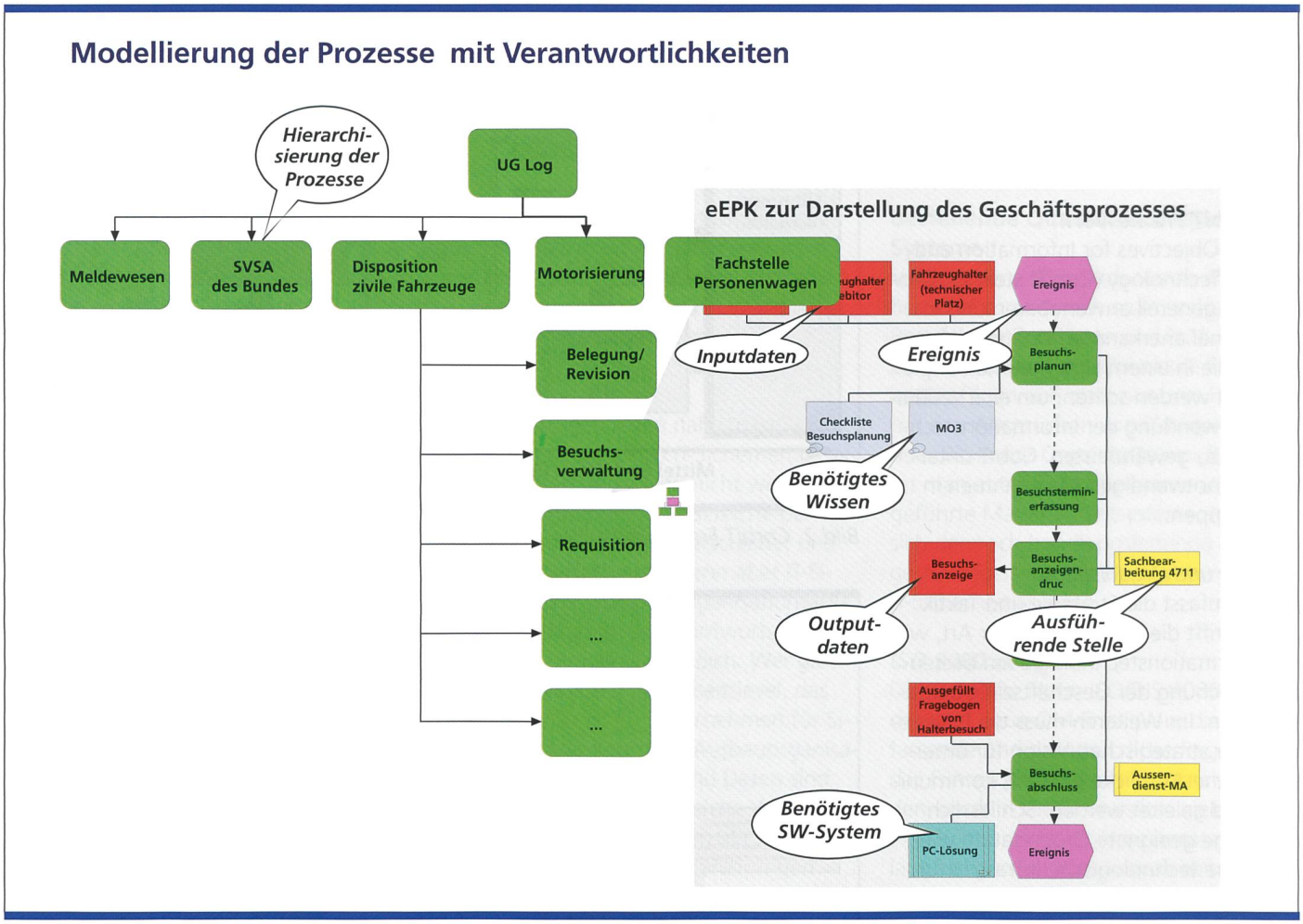

Bild 4. Modellierung der Prozesse mit Verantwortlichkeiten.

EFQM
Wie aktivieren wir die Selbstverantwortung unserer Mitarbeitenden?
Wie können wir uns stetig verbessern?

EFQM / CobiT
Wie prüfen wir die Wirksamkeit unserer Massnahmen?

Strategien zur Umsetzung der Anforderungen

Sicherheit und Datenschutz sind kein einmal erreichter Zustand, sondern müssen als stetiger Prozess im Unternehmen begriffen werden. Dieser Prozess umfasst Sicherheitsanalysen, die Erstellung von Sicherheitskonzepten, deren Umsetzung und die Kontrolle. Ziel ist die Erstellung eines Sicherheitskonzepts, das die unterschiedlichen Schutzbedürfnisse der einzelnen Systeme und Anwendungen berücksichtigt und die Erstellung eines Katalogs der durchzuführenden Sicherheitsmassnahmen. Als Nächstes sind die beschlossenen Sicherheitsmassnahmen zu realisieren. Dazu werden Prioritäten und Verantwortlichkeiten definiert und die Umsetzung der Massnahmen überwacht. Diese Vorgänge sollten gekoppelt sein mit einer geeigneten Informations- und Sensibilisierungspolitik.
Regelmässige Überprüfungen und Aktualisierungen des Sicherheitskonzepts bei Veränderungen in der IT-Landschaft schliessen den Kreis.

Auswirkungen auf die Organisation

Wichtig ist die Einbindung der Sicherheitspolitik in die Aufbauorganisation eines Unternehmens, da ihr nur so die Aufmerksamkeit zuteil wird, die sie benötigt. Das Sicherheitsteam kann dabei Teil des Qualitätsmanagementteams sein oder selbstständig, aber abgestimmt operieren. Das verantwortliche Team wird von der Unternehmensleitung bestellt und besteht aus Experten und Vertretern der Anwender der verschiedenen Unternehmensbereiche. Da alle Qualitätsmanagementsysteme die Transparenz und Beherrschung der Unternehmensprozesse in den Vordergrund stellen, ist die Ablauforganisation im Unternehmen entsprechend zu betrachten. Hier bestimmen altbekannte Konstrukte wie Prozessarchitektur, Kern-, Support- und Koordinationsprozesse das Vorgehen. Die Prozesse zur Unterstützung der IT-Sicherheit sind nach dem gleichen Muster aufgebaut.

Einsatz geeigneter Werkzeuge

Erprobte Werkzeuge und Vorgehensweisen des Qualitätsmanagements können beim Aufbau und der Realisierung von IT-Sicherheit unterstützen.
Das Prozessmanagement setzt die Erfordernisse der Prozessorientierung kundengerecht um. Die Abläufe eines Unternehmens werden nicht nur in ihrer Ablauflogik analysiert. Für jeden Prozessschritt wird ausserdem definiert, welcher Benutzer für den Zugriff auf Daten und Transaktionen berechtigt ist oder welche Bedeutung das zur Bearbeitung benötigte Wissen hat. Die auf strategischer Ebene festgelegte Sicherheitspolitik gibt vor, wie restriktiv oder passiv diese sicherheitsrelevanten Sachverhalte überprüft werden. Die Verantwortlichkeit der Mitarbeitenden tritt hier besonders zu Tage, werden doch alle relevanten Transaktio-

nen-Berechtigungsverbindungen transparent dargestellt.
People Empowerment führt diesen Verantwortungsgedanken weiter in die Selbstverantwortung. Nicht mehr Kontrolle durch Vorgesetzte steht im Vordergrund, sondern die Sensibilisierung und Involvierung der Mitglieder einer Organisation.
Selbstverantwortung muss aber erlernt und kann nicht von der Leitung befohlen werden. Als ein gutes Instrument zum Anstossen dieses Bewusstseinswandels hat sich das Self Assessment erwiesen. Alle Mitglieder einer Organisation unterziehen ihre Aktivitäten, Abläufe, Systeme und Dokumente selbstständig einem Review und leiten aus den Ergebnissen Ansatzpunkte für die kontinuierliche Verbesserung ab.

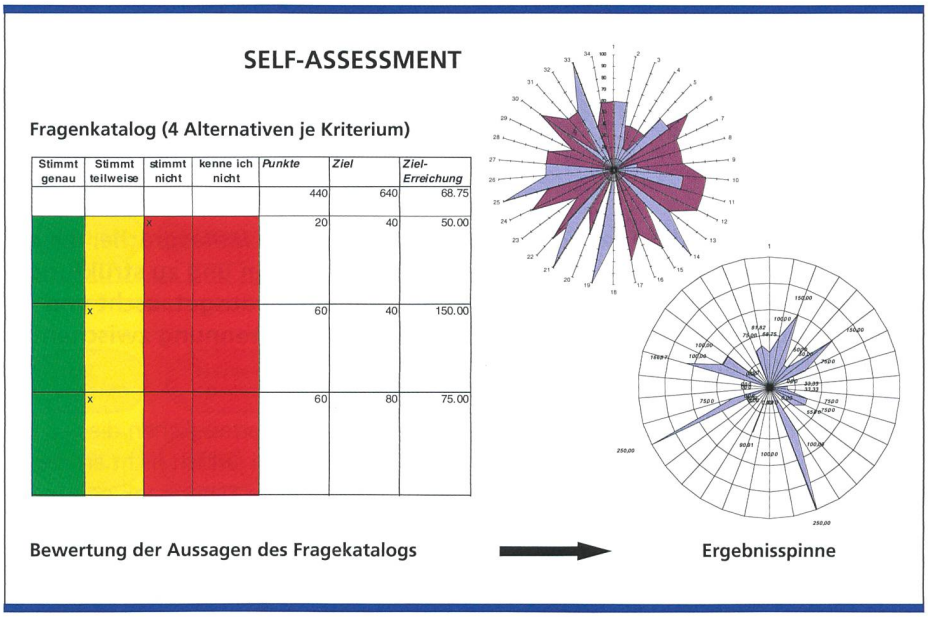

Bild 5. Self Assessment.

Auditierung und Zertifizierung

Zertifizierung ist die Beurteilung der Konformität eines Qualitätsmanagementsystems anhand vorgegebener Kriterien durch unabhängige Dritte. Im Rahmen eines Audits wird ermittelt, ob ein Unternehmen die Bedingungen zur Zertifikatserteilung erfüllt. Zu beachten ist allerdings, dass mit der Erteilung eines Zertifikats nicht die Qualität von Produkten, Dienstleistungen oder der Sicherheit eines Unternehmens bescheinigt wird, sondern die Übereinstimmung des Qualitätsmanagementsystems mit dem jeweils geforderten Regelwerk der Norm. Ein Unternehmen kann sich also nicht bescheinigen lassen, dass seine Politik und seine Massnahmen ausreichend sind, Sicherheit im Unternehmen in ausreichender Qualität zu gewährleisten. Es sollte vielmehr die Zertifizierungen und Wettbewerbe als Chance zur Verbesserung interner Prozesse und Strukturen verstehen, sowie als Impuls zur Veränderung von Verhalten und Einstellungen auch in Bezug auf das Thema IT-Sicherheit.

Ausblick

Was können Sicherheitsverantwortliche von klassischen Qualitätsmanagementsystemen lernen? Die folgende Liste stellt die wesentlichsten Erkenntnisse dieses Berichts zusammen:

- Bestehende Regelwerke können helfen, IT-Sicherheit auch für das Management greifbar zu machen.
- Ohne Sensibilisierung der "gefährlichen" Mitarbeitenden geht es nicht.
- Sicherheitswerkzeuge sind nur ein Rädchen im Uhrwerk IT-Sicherheit.
- Akzeptierte Managementinstrumente können unterstützend zum Aufbau von IT-Sicherheit übernommen werden.

Diese an sich trivialen Erkenntnisse befriedigen die Bedürfnisse der mit der Qualitätssicherung von IT-Sicherheit Beauftragten noch nicht. Ihnen mangelt es an einem besser auf die relevanten IT-Sicherheitsaspekte abgestimmten Vorgehens- und Prüfkatalog, der aber noch nicht vorhanden ist. Es existieren jedoch Bemühungen auf nationaler und internationaler Ebene, ein Rahmenwerk zu schaffen, nach dem sicherheitsrelevante Sachverhalte prüfbar und zertifizierbar werden. Es ist davon auszugehen – und erste Veröffentlichungen belegen diese Vermutung – dass diese neuen Rahmenwerke auf den Erfahrungen der etablierten Normen aufbauen werden. Was hält ein Unternehmen also davon ab, den gleichen Weg einzuschlagen und die bereits vorhandenen Hilfsmittel einzusetzen? 2

Jörg Altmeier *ist Mitglied der Geschäftsleitung der CIRRUS AG in Zürich und seit über sechs Jahren beratend in den Bereichen Project Management, Coaching, Applications and Methods und Quality Management tätig. Sein Schwerpunkt liegt in der Verbindung von SAP R/3 mit Qualitätsmanagementkonzepten. Er absolvierte seine Studien in Betriebswirtschaft und Total Quality Management in Saarbrücken und Kaiserslautern und ist zertifizierter Business Excellence Coach der Schweizerischen Arbeitsgemeinschaft für Qualitätsförderung und Business Excellence Leader der European Organisation for Quality (EOQ).*

Literatur

Scheibele, Campbell, "WEKA Praxis Handbuch Plus: Qualitätsmanagement nach der neuen ISO9000er-Serie"; Fachverlag für technische Führungskräfte, 2000.
Homburger, Schneider, "Sicherheit und Datenschutz mit SAP-Systemen"; SAP Press, 2000.
ISACA Spitzerland Charter, "Kontrollziele für Informationstechnologien"; ISACA, 1999.
Zink, "Prozessorientierung – ein Baustein umfassender Veränderungskonzepte", in Zülch, "Vereinfachen und Verkleinern – die neuen Strategien der Produktion"; Stuttgart, 1994.
Malorny, "TQM erfolgreich umsetzen", Schäffer-Poeschel, 1996.