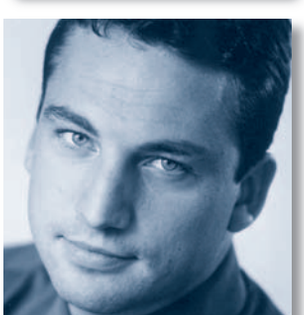
Compliance Management in der Praxis

Haftungsklagen und neue Gesetze haben Compliance Management zur Abwendung latenter Risiken unumgänglich werden lassen. Diese Aufgabe lässt einfach erledigen und generiert zusätzlichen unternehmerischen Nutzen *Martin Dietrich, Herbert Bischof, Wolfgang Gliebe*

Martin Dietrich
lic. oec. HSG, CISA, leitet die Entwicklung der BSG ITSEC Tool Box der BSG Unternehmensberatung, St. Gallen
martin.dietrich@bsg.ch



Herbert Bischof
Mag. rer. soc. oec, dipl. Wirtschaftsprüfer ist Geschäftsführer der CIS – Certification & Information Security Services AG, Vaduz
herbert.bischof@cis-cert.li

Die Einhaltung von Gesetzen und Richtlinien ist für viele eine Selbstverständlichkeit. In der Umgangssprache und in diesem Artikel wird der Begriff mit «korrektem Verhalten» umschrieben. Durch verschiedene Skandale und den damit einhergehenden Haftungsklagen – vor allem in den USA – ist Compliance Management aber zu einem Modewort geworden. Man könnte meinen, dass sich bisher niemand korrekt verhalten habe. Aus der Gerichtspraxis hat sich nun ein ganz neuer Aspekt entwickelt: Ein Unternehmen muss jederzeit und rückwirkend den Nachweis erbringen, sich korrekt verhalten zu haben. Das ist etwas, das wir aus unserem täglichen Leben nicht kennen, und das logisch zu Ende gedacht gar nicht möglich ist. Nämlich den Nachweis erbringen, etwas nicht getan zu haben. Es handelt sich hierbei um die Umkehr des fundamentalen Prinzips der Unschuldsvermutung: Galt bisher das Prinzip «Unschuldig, bis zum Beweis der Schuld» gilt neu: «Schuldig, bis zum Beweis der Unschuld.»

Dies führt dazu, dass eine ständige Überwachung und Dokumentation aller Tätigkeiten und Entscheidungen (und somit auch aller Nicht-Tätigkeiten und Nicht-Entscheidungen) notwendig wird, um im Schadensfall nicht nur das korrekte Verhalten, sondern auch das Unterlassen des nichtkorrekten Verhaltens beweisen zu können. Diese ständige Überwachung der Einhaltung aller Gesetze und Regeln wird auch mit dem Begriff Compliance Management beschrieben (Siehe dazu auch die Gedanken von Gunter Dueck; u.a. in «Panopticon» im Informatik-Spektrum_20_6_2006 Seiten 442ff.).

Gesetze ohne Handlungsanweisungen

Für die Beurteilung der Korrektheit des Verhaltens muss eine entsprechende Verhaltensvorschrift, also ein Massstab, explizit definiert sein. Aufgrund der Schnelllebigkeit der Informationstechnologie und des langwierigen Gesetzgebungsprozesses enthalten die Gesetze und Verordnungen keine klaren Handlungsanweisungen. Der Gesetzgeber verlangt, dass der «Stand der Technik» eingehalten werden muss. Im Bereich der Informationstechnologie beziehungsweise der Informatik-Sicherheit haben sich verschiedene Normen durchgesetzt, die als Stand der Technik betrachtet werden. So hat sich aus dem British Standard 7799 die ISO-Norm 17799 entwickelt, die in Zukunft Teil der ISO 2700x-Reihe sein soll. In den USA wurden Cobit von der ISACA (Information Systems Audit and Control Association) und SAS 70 von der AICPA (American Institute of Certified Public Accountants) entwickelt. Durch die Unterstellung aller in den USA tätigen Unternehmen unter den Patriot- und den Sarbanes-Oxley Act wurden diese Standards auch bei uns ein Begriff. Die Normen für IT Security sind umfassende Werke mit detaillierten Hinweisen, in welchen Bereichen Massnahmen getroffen werden müssen: ISO 17799:2005 umfasst 133 Controls auf 128 Seiten, Cobit 215 detaillierte Kontrollziele auf 207 Seiten.

Einhaltung von Regeln

Beim Studium der Normen fällt auf, dass nur generell beschrieben wird, in welchen Bereichen Massnahmen getroffen werden sollen, aber nicht, wie die Massnahmen konkret auszugestalten sind. So wird unter anderem ein Passwort-Konzept gefordert, ohne aber beispielsweise die Passwortlänge und -lebensdauer zu definieren. Compliance Management befasst sich also mit der Überwachung der Einhaltung von Regeln, über deren Interpretation zumindest diskutiert werden kann. Der Beweis der Einhaltung der geltenden Regeln beziehungsweise des Stands der Technik lässt sich auf verschiedene Arten erbringen. Es können zum Beispiel alle Arbeiten unter dem 4-Augen-Prinzip erledigt oder jede Tätigkeit, nicht nur diejenige am PC, laufend dokumentiert werden. Verschiedene grösse-

re Firmen setzen bereits heute einen Compliance Manager ein.

Compliance Management lässt sich in drei Schritten aufbauen:

1. Bestimmen der Norm, an die man sich halten will. Aufgrund der unsicheren Interpretation des «Stands der Technik» ist dies notwendig.
2. Dokumentieren der Einhaltung der gewählten Norm. Für die Beweisführung ist dies unumgänglich.
3. Zertifizierung durch eine unabhängige akkreditierte Stelle. Damit lässt sich die Ernsthaftigkeit des Compliance Managements unterstreichen. Zudem wird ein Angriffspunkt in einem möglichen Gerichtsverfahren entschärft.

Zusätzlicher Nutzen

Kurz- und mittelfristig können Unternehmen, die im öffentlichen Interesse stehen (etwa Kreditkartenunternehmen, Banken, Internet-Shops) mittels einer Zertifizierung Wettbewerbsvorteile erreichen. Langfristig wird eine Nicht-Zertifizierung in gewissen Branchen eine erfolgreiche Geschäftstätigkeit wesentlich erschweren.

Auf internationaler Ebene, aber vermehrt auch auf nationaler Ebene, wird die Frage nach der Haftung nach einem Schaden gestellt. Schadenersatzklagen können nicht nur gegen Unternehmen und deren Organe, sondern auch gegen Sicherheitsverantwortliche angestrengt werden. Die Einhaltung einer Norm schützt vor negativen Urteilen aufgrund von Fahrlässigkeit.

Da die Normen die konkreten Massnahmen offen lassen, können diese an die spezifischen Anforderungen des Unternehmens angepasst werden. Damit lassen sich die anfallenden Kosten reduzieren.

Informatik definiert IT-Sicherheit

Ausgangspunkt für die Identifikation des für ein Unternehmen anwendbaren «Stand der Technik» ist die Forderung, «es sei das Zumutbare zu unternehmen, um das Voraussehbare zu verhindern». Damit ist bereits gesagt, dass der «Stand der Technik» in der IT-Sicherheit nicht für alle Unternehmen gleich ist, sondern durch die Abhängigkeit der Geschäftsprozesse eines Unternehmens von der Informatik definiert wird. Wenn bereits ein kurzer Ausfall der Informatik oder ein Verlust von soeben erhaltenen Daten die Geschäftstätigkeit des Unternehmens in kritischer Art und Weise beeinflusst, sind weitergehende Massnahmen zur Verhinderung eines entsprechenden Zwischenfalles zumutbar, als wenn das Unternehmen davon nur beschränkt betroffen wäre.

Durch eine strukturierte, toolunterstützte Risikoanalyse mit den Geschäftsprozess-Verantwortlichen lassen sich die Abhängigkeiten der Geschäftsprozesse von der Informatik nachvollziehbar, strukturiert und wiederholbar aufzeigen. Eine Überprüfung des aktuellen Sicherheitszustandes ermöglicht den Vergleich mit den Soll-Anforderungen einerseits und ein Benchmarking mit vergleichbaren Unternehmen andererseits. Dies setzt aber voraus, dass für die Sicherheitsüberprüfung eine Methodik eingesetzt wird, die die Zumutbarkeit der möglichen Massnahmen entsprechend der spezifischen Situation des Unternehmens berücksichtigt, ohne dass für jedes Unternehmen eine eigene Klassifizierung der Massnahmen vorgenommen werden muss.

Der Zertifizierungsprozess

Die Zertifizierung nach ISO 27001 basiert auf den generellen Richtlinien und Grundsätzen der internationalen ISO Normenfamilie, deren populärste Vertreter hierzulande vermutlich die Qualitätsmanagementnorm ISO 9001 und die Umweltmanagementnorm ISO 14001 sind. Der Zertifizierungsprozess hat in erster Linie das Informations-Sicherheits-Management-System (ISMS) zum Gegenstand, das nach einem x-beliebigen Standard (international anerkannt oder individuell) aufgebaut sein kann. Entscheidend dabei ist nur, dass das ISMS alle wesentlichen Bereiche des Sicherheitsspektrums abdeckt.

Zu den internen Vorbereitungen auf eine bevorstehende Zertifizierung zählen die Erhebung des aktuellen Sicherheitszustands des Unternehmens sowie des zu erreichenden Sicherheitsniveaus der Geschäftsprozesse, um einen grundsätzlichen Soll-Ist-Vergleich anstellen zu können. Damit werden der Zeitaufwand, die Ressourcenbeanspruchung sowie alle mittel- und langfristigen Massnahmen transparent und planbar.

Für diese Schritte lohnt sich der Einsatz einer standardisierten Methode, die den «Stand der Technik», unter Berücksichtigung der Zumutbarkeit, beziehungsweise ausgerichtet auf die Anforderungen an die Informatiksicherheit, nachvollziehbar vordefiniert. Da diese Aufgabe für die meisten Unternehmen Neuland darstellt, ist es ratsam, erfahrene und spezialisierte Berater beizuziehen.

Wenn sich das Unternehmen reif für eine Zertifizierung fühlt und sich dazu entschliesst, so wird diese nach einem international einheitlichen Prüfstandard durchgeführt. Das drei Jahre gültige Zertifikat wird verliehen, wenn keine wesentlichen Mängel feststellbar sind. Auf dem Weg zu einem gewünschten Standard oder wenn auf ein Zertifikat weniger Wert gelegt wird, bietet sich ein «Stage Review» an. Dieses bietet als Feedback einen Auditbericht, ein Stärken-Schwächen Profil sowie konkrete Verbesserungspotentiale.

Die Rollen des Zertifizierers und des Beraters sind genau zu unterscheiden. Der Zertifizierer muss akkreditiert sein und unterliegt einer strengen Kontrolle durch die nationale Akkreditierungsstelle (in der Schweiz: METAS Bundesamt für Metrologie). Der Zertifizierer nimmt ausschliesslich Konformitäts-Beurteilungen vor, wohingegen der (externe) Berater viel umfassender in sämtliche Planungs- und Umsetzungsprozesse involviert ist und sein darf. Ohne dieses grundsätzliche Unabhängigkeitserfordernis zwischen Zertifizierer und Berater würden sowohl die fehlende Glaubwürdigkeit als auch Haftungsprobleme die Dienstleistung des Zertifizierers beziehungsweise sogar dessen Existenz in Frage stellen.