

# Managementverantwortung für Informationssicherheit

Welche Auswirkungen haben der Sarbanes-Oxley Act und Basel II tatsächlich? Obwohl die Informationssicherheit in diesen Regelungen nicht explizit erwähnt wird, darf sie keinesfalls ausser Acht gelassen werden – Informationssicherheit ist Führungsaufgabe. Doch wie steht es wirklich damit? *Maria Winkler*

Spektakuläre Unternehmenszusammenbrüche im Ausland wie im Inland sowie die derzeitige Wirtschaftslage haben zu einer grösseren Sensibilisierung der Öffentlichkeit gegenüber Grossunternehmen geführt. Das Ausmass der Verantwortung der oberen Unternehmensführung für ihr Handeln und Unterlassen im Interesse des Gesamtunternehmens wird intensiv diskutiert. Neue Begriffe wie Corporate Governance und Risikomanagement als Hauptaufgaben des Verwaltungsrats wurden geprägt. Die persönliche Haftung der Mitglieder des Verwaltungsrats wird öffentlich thematisiert. Verwaltungsräte, die ihre Aufgabe bisher in erster Linie als eine ehrenvolle Aufsichtsfunktion gegenüber der Geschäftsleitung verstanden haben, stehen vor der Frage, welche Pflichten sie zu erfüllen haben, um ihren Aufgaben im Rahmen des Gesetzes nachzukommen.

## Corporate Governance

Unter Corporate Governance ist die verantwortliche Führung, Kontrolle und Überwachung von Unternehmen zu verstehen, um die Rechte und Interessen der Investoren und weiterer Anspruchsgruppen, wie zum Beispiel der Arbeitnehmer, wahrzunehmen. Es geht also um einen neuen Begriff, nicht jedoch um eine neue Aufgabe, denn die klare Verantwortung für die Oberleitung und Überwachung eines Unternehmens sind in der Schweiz bereits seit der Einführung des neuen Aktienrechts im Jahr 1992 klar dem Verwaltungsrat zugewiesen.

Obwohl das Gesetz somit die Pflichten von Verwaltungsrat und Geschäftsleitung konkretisiert und die Verantwortlichkeiten klar zugewiesen hat, ist die Umsetzung in der Praxis alles andere als einfach. Die Fragen, wie weit die Verantwortung tatsächlich reicht, welche Kontrollinstrumente zwingend eingesetzt werden müssen, ohne das Unternehmen einer Überreglementierung auszusetzen, müssen für jedes Unternehmen diskutiert und gelöst werden.



Vor allem international tätige Schweizer Unternehmen sind verpflichtet, neben nationalen auch internationale Normen zu beachten

## Risikomanagement

Zu den nicht delegierbaren Aufgaben des Verwaltungsrats gehören neben der Oberleitung der Gesellschaft und der Erteilung der nötigen Weisungen auch die Finanzplanung und -kontrolle sowie die Oberaufsicht über die mit der Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten und Weisungen.

Der «Swiss Code of Best Practice for Corporate Governance», der im Juli 2002 vom Verband der Schweizer Unternehmen *economiesuisse* veröffentlicht wurde, konkretisiert die gesetzlichen Vorschriften und verlangt, dass der Verwaltungsrat mittels auf die Bedürfnisse des Unternehmens abgestimmter interner Kontrollsysteme und eines Risikomanagements die finanziellen und operativen Risiken abdeckt.

## Die Verantwortung liegt bei der Unternehmensführung

Wurde bisher die Verantwortung für funktionierende IT-Infrastrukturen ausschliesslich dem IT-Verantwort-

lichen des Unternehmens zugewiesen, ist somit heute klar, dass diese, je nachdem, wie geschäftskritisch das Funktionieren der IT-Systeme für ein Unternehmen ist, von der Unternehmensführung als IT-Governance berücksichtigt werden muss. Dabei ist von einem weiten Begriff der Informationssicherheit auszugehen und diese ist nicht nur auf die technischen Aspekte zu reduzieren.

Konkret bedeutet das, dass der Verwaltungsrat und die Geschäftsleitung sicherzustellen haben, dass

- die Bedeutung der Informationssicherheit im Unternehmen in der Organisationsstruktur angemessen berücksichtigt wird, indem Verantwortlichkeiten und Kompetenzen klar zugewiesen werden;
- die mit dem Einsatz von Informationstechnologie im Unternehmen verbundenen Risiken identifiziert und Massnahmen zu deren Ausschaltung oder Reduzierung ergriffen werden;
- durch ein funktionierendes internes Kontrollsystem sichergestellt

wird, dass interne Weisungen, Regeln der Technik und nationale sowie relevante internationale Normen eingehalten werden (Compliance).

## Einfluss internationaler Normen auf Schweizer Unternehmen

Vor allem international tätige Schweizer Unternehmen sind verpflichtet, neben nationalen auch internationale Normen zu beachten. Die Frage, inwieweit sich etwa der Sarbanes-Oxley Act oder das Basel-II-Abkommen auch auf Fragen der Informationssicherheit auswirken, scheint aber bis heute weitgehend ungeklärt.

Beide Normen enthalten keine Bestimmungen, die die Informationssicherheit direkt ansprechen, dennoch sind sie auch in diesem Bereich zu beachten.

Der Sarbanes-Oxley Act verpflichtet unter anderem den CEO und den CFO, bei jedem Jahres- oder Zwischenabschluss eidestattlich zu bezeugen, dass sie die Berichterstattung kritisch durchgesehen haben, dass diese keine falschen oder miss-

► verständlichen Aussagen enthält und dass diese die finanzielle Verfassung sowie das Geschäftsergebnis zutreffend wiedergibt. CEO und CFO sind gemeinsam verantwortlich für das Funktionieren interner Kontrollen, die sicherstellen, dass die relevanten Informationen zum Unter-

nehmen auch richtig und rechtzeitig zur Verfügung stehen.

CEO und CFO müssen somit öffentlich bekunden, dass die bekannten Finanzdaten richtig sind und dass die entsprechenden internen Kontrollen funktionieren. Der Zusammenhang mit der Informati-

onsicherheit liegt hier auf der Hand – Finanzdaten werden elektronisch erstellt, bearbeitet und archiviert, ihre Integrität steht und fällt mit der Sicherheit der IT-Infrastrukturen, mit denen finanzrelevante Daten bearbeitet werden.

Diese Vorgaben betreffen alle Unternehmen, die an einer US-Börse kotiert sind, sowie deren Tochtergesellschaften und deren Wirtschaftsprüfer. Indirekt wird sich der Sarbanes-Oxley Act allerdings auch auf andere Unternehmen auswirken – indem an der US-Börse kotierte Unternehmen ihre Aufträge bevorzugt oder ausschliesslich an solche Unternehmen weitergeben, die sich ebenfalls wieder an die Vorschriften des Sarbanes-Oxley Act halten.

Mit dem Basel-II-Abkommen, der Eigenkapitalvereinbarung für Banken, werden sich ab 2006 die Voraussetzungen für die Vergabe von Unternehmenskrediten ändern, da die Banken neu mehr Eigenkapital für unsichere Kredite hinterlegen müssen. Bei der Risikobeurteilung, dem sogenannten Rating, müssen neben den Finanzdaten aus der Vergangenheit auch die operationellen Risiken des Kreditnehmers berücksichtigt werden. In Zukunft wird ein Unternehmen, das einen Kredit beantragt, der Bank auch darlegen müssen, wie zum Beispiel seine Unternehmensstrategie aussieht, ob es seine Risiken kennt und wie es diese kontrolliert etc. Das Rating wirkt sich auf die Kreditkosten aus – je schlechter das Rating, umso höher der risikospezifische Prozentsatz der Kreditsumme, den die Bank als Eigenkapital hinterlegen muss – und umso teurer der Kredit für das Unternehmen!

### Zusammenfassung

- Informationssicherheit als Teil der IT Governance ist integraler Bestandteil von Corporate Governance und somit eine Führungsaufgabe von Verwaltungsrat und Geschäftsleitung.
- Die Sicherheit der IT-Systeme eines Unternehmens wirkt sich unmittelbar auf die Integrität und Verfügbarkeit der geschäftsrelevanten Informationen und dadurch auf den Geschäftserfolg aus, sollte in einer gesamtheitlichen Risikobetrachtung Eingang finden und angemessen berücksichtigt werden.
- Der Sarbanes-Oxley Act und das Basel-II-Abkommen sanktionieren indirekt die Vernachlässigung der informationssicherheitskritischen Risiken. Sie bekräftigen die Bedeutung, welche dem umfassenden Risikomanagement als Ausdruck sorgfältiger Unternehmensführung bereits nach schweizerischem Recht zukommt.



Die Sicherheit der IT-Systeme eines Unternehmens wirkt sich unmittelbar auf den Geschäftserfolg aus

#### Autorin



Mag. iur. **Maria Winkler** ist geschäftsführende Partnerin der IT & Law Consulting GmbH in Zug und Luzern und Dozentin für

Informatikrecht sowie Recht im Internet an der Hochschule für Wirtschaft (HSW) Luzern. Sie ist schwerpunktmässig im Bereich Informatikrecht und Recht im Internet tätig.

Anzeige

# Sie organisieren Ihren Event.

# Mit uns erreichen Sie Ihre Teilnehmer.

**Die Netzagenda macht Ihre Veranstaltung bekannt!**

Tragen Sie Ihre eigenen Veranstaltungen unkompliziert online unter [www.netzagenda.ch](http://www.netzagenda.ch) ein; der Basiseintrag ist kostenlos. Mit einem «Netzagenda-Plus»-Eintrag kombinieren Sie online und print und werden nie mehr übersehen.

Weitere Informationen finden Sie auf [www.netzagenda.ch](http://www.netzagenda.ch)

netzagenda

Events, Kurse, Seminare, Workshops und andere Termine für die Web- und ICT-Branche.