Für Aufsichtsräte, Beiräte & Verwaltungsräte

Der Aufsichtsrat

Haftung von Aufsichtsräten und Beiräten

Haftungsfallen für den Aufsichtsrat
Höhere Anforderungen, aber kein Automatismus

D&O-Versicherung
Anreizwirkung des Selbstbehalts

D&O-Versicherung
Ein Blick in das Jahr 2010

Dokumentensicherheit
IT-Haftungsrisiken für Aufsichtsräte

Beratungsverträge mit Aufsichtsratsmitgliedern
Entwicklung der Rechtsprechung und offene Fragen

Ergänzungsmitglied im Aufsichtsrat
Voraussetzungen und Rechtstellung

„Safe harbor" für Aufsichtsräte
Strategien zur Haftungsvermeidung

FACHVERLAG
Verlagsgruppe Handelsblatt

Dokumentensicherheit: IT-Haftungsrisiko für Vorstände und Aufsichtsräte

Das Haftungsrisiko für Vorstände und Aufsichtsräte hat in den letzten Jahren deutlich zugenommen. Hierbei spielen vor allem zwei Entwicklungen eine Rolle: Zum einen sind durch strengere Regelungen die Anforderungen der Stakeholder an die Qualität der Unternehmensführung und -überwachung merklich gestiegen. Zum anderen hat durch den Fortschritt in der IT und die zunehmende Vernetzung der globalen Wirtschaft das technische Bedrohungspotenzial signifikant zugenommen. Diesem Haftungsrisiko kann nur durch den Aufbau eines adäquaten IT-Risikomanagement-Systems begegnet werden.

von Dirk Bode und Dr. Jochen Haller*)

I. Grundzüge der Managerhaftung

Grundsätzlich gilt, dass die Unternehmensführung (Vorstand bzw. Geschäftsführer) Schaden vom Unternehmen soweit wie möglich abzuwenden hat. Zudem müssen für das Unternehmen existenzbedrohende Entwicklungen frühzeitig erkannt werden. Daneben hat die Unternehmensführung für das Unternehmen eine Versicherungspflicht wahrzunehmen. Hiernach hat der Urheber einer potenziellen Gefahrenquelle (hier: die IT-Abteilung eines Unternehmens) alle zumutbaren Maßnahmen durchzuführen, um die von dieser Quelle ausgehenden Gefahren zu minimieren.

Diese Grundprinzipien werden durch mehrere Vorschriften konkretisiert. Am bedeutendsten sind in diesem Zusammenhang die aktienrechtlichen Änderungen durch das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG 1998), der Deutsche Corporate Governance Kodex (DCGK), die Basel II-Richtlinie und der amerikanische Sarbanes-Oxley Act (SOX).

Daneben existiert aber noch eine Reihe weiterer relevanter nationaler und internationaler Rechtsstandards. Hierzu zählen z.B. das Anlegerschutzverbesserungsgesetz (AnSVG) und die EU-Datenschutzrichtlinie. Daneben gibt es oft branchenspezifische Vorschriften, wie z.B. das Teledienstedatenschutzgesetz (TDDSG).

Diese o.g. Vorschriften weisen i.d.R. die folgenden Gemeinsamkeiten auf:

- Die Unternehmensführung ist für die IT-Sicherheit bzw. für ein adäquates IT-Risikomanagement-System verantwortlich.
- Es gilt die Verschuldensvermutung bei Schadenseintritt – einschließlich einer Beweislastumkehr (d.h. der Schädiger muss seine Unschuld beweisen).
- Vergehen werden mit empfindlichen Strafen (Geld- und teilweise auch Freiheitsstrafen) belegt.
- In vielen Fällen sind die Organe der Gesellschaft persönlich haftbar (einschließlich gegebenenfalls deren Privatvermögen).

*) Dirk Bode ist Vorstandsvorsitzender der fme-Gruppe, Braunschweig; Dr. Jochen Haller ist Geschäftsführer der certon systems GmbH, Heidelberg.

Insbesondere der letzte Punkt wird häufig übersehen. Folglich kann das Unternehmen im Innenverhältnis das Management für Fehler in Regress nehmen, falls es verklagt worden ist. Folglich sind Vorstandsmitglieder, die ihre Pflichten verletzen, der Gesellschaft zum Ersatz des hieraus entstehenden Schadens als Gesamtschuldner verpflichtet und haften persönlich mit ihrem gesamten Privatvermögen. Aber auch Aufsichtsratsmitglieder haften persönlich, wenn sie den Vorstand unzureichend überwachen oder klar erkennbare Missstände im Unternehmen nicht beseitigen lassen. Ein Aufsichtsrat haftet auch, wenn er den Vorstand nicht verklagt, obwohl ihm bekannt ist, dass Schadensersatzansprüche wegen Pflichtverletzungen gegen den Vorstand mit Erfolg eingeklagt werden könnten.

„IT-Haftungsrisiken für Vorstände und Aufsichtsräte werden häufig unterschätzt."

Zusammengefasst: Der Vorstand hat alle erforderlichen Maßnahmen im Rahmen des IT-Risikomanagements zu treffen und haftet dafür, falls er dies unterlässt. Der Aufsichtsrat hat dies zu überwachen. Vernachlässigt er diese Überwachungspflicht und treten hierdurch erhebliche Schäden (v.a. Insolvenz) ein, haftet auch jedes Aufsichtsratsmitglied ggf. persönlich.

Die Schäden, die durch ein unzureichendes IT-Risikomanagement für ein Unternehmen möglicherweise entstehen, können erheblich sein. Denkbare Folgen sind u.a.:

- Verluste durch den Ausfall von IT-Systemen, ggf. sogar Insolvenz,
- Verteuerung/Verweigerung von Krediten (Stichwort: Basel II),
- Verlust des Versicherungsschutzes,
- Imageschaden,
- Schadensersatzpflichten,
- Bußgelder,
- Verlust von Know-how,
- Verlust von Kunden und/oder Lieferanten,
- Verweigerung des Testats durch den Wirtschaftsprüfer.

Die Fülle der Anspruchsgrundlagen, die zahlreichen Folgen eines unzureichenden IT-Risikomanagements für das Unternehmen und das steigende Bedrohungspotenzial durch IT belegen, dass das IT-Haftungsrisiko für Vorstände und Aufsichtsräte in den letzten Jahren deutlich zugenommen hat. Dieses Risiko kann nur durch die Etablierung eines adäquaten IT-Risikomanagement-Systems minimiert werden.

II. IT-Risiko: Unzureichende Dokumentensicherheit

Aufgrund des großen Imageschadens, den die betroffenen Unternehmen befürchten, gelangen Fälle unzureichender Dokumentensicherheit bzw. des sorglosen Umgangs mit diesen zumeist nicht an die Öffentlichkeit. Dennoch sind bereits einige besonders schwerwiegende Fälle bekannt geworden.

Beispielsweise argumentierte ein Vertriebsmitarbeiter von Dell in einer E-Mail gegenüber einem Kunden, dass dieser sich bewusst sein müsse, dass er durch den Kauf von Hardware bei Dell's Konkurrenten Lenovo das chinesische Regime (der Staat China ist der Eigentümer von Lenovo) unterstütze. Diese E-Mail gelangte unbeabsichtigt an die Presse und wurde in den chinesischen Medien landesweit zitiert, woraufhin sich Dell öffentlich entschuldigen musste. Ein ähnlich „pikantes" Missgeschick unterlief dem ehemaligen CEO von Boeing. Kurz nachdem er eine private Affäre mit einer wesentlich jüngeren Managerin des Konzern begonnen hatte, zirkulierten im Unternehmen „anzügliche" private E-Mails von ihm. Da der Aufsichtsrat das moralische Fundament des Unternehmens gefährdet sah, legt er dem CEO umgehend den Rücktritt nahe. Ein ähnlich weitreichendes Versehen unterlief dem CEO des Musiksenders Viva, kurz nach der Übernahme von Viva durch den Medienkonzern Viacom. In einer internen E-Mail, die sich an sämtliche Mitarbeiter richtete, wollte er diese beruhigen und ihnen die Angst vor einem möglichen Arbeitsplatzverlust nehmen. Jedoch enthielt diese E-Mail versehentlich einen Anhang mit dem Titel „Ablauf Kommunikation Betriebsschließung". Der Inhalt war für die Mitarbeiter alles andere als erfreulich. Daneben ist ein Fall bekannt, in dem der Mitarbeiter einer angesehenen Consulting-Firma eine E-Mail mit beleidigendem Inhalt über einen Klienten aus Versehen direkt an diesen geschickt hatte. Dieser Fall eskalierte bis auf Vorstandsebene und hätte beinahe zum Abbruch eines großen Projekts geführt. Neben solchen Fällen, die reinen immateriellen Schaden verursachten, sind aber auch Fälle bekannt geworden, die zu nachhaltigen finanziellen Schäden geführt haben. So wurde das Schweizer Bankhaus UBS aufgrund des internen E-Mail-Verkehrs von einem Gericht zur Zahlung einer Geldstrafe von 29 Mio. USD verurteilt. Mithilfe von E-Mails ihres Vorgesetzten mit der Personalabteilung konnte eine Managerin nachweisen, dass ihr Vorgesetzter sie so schnell wie möglich loswerden wollte. Nicht immer sind die negativen Folgen derart offensichtlich. So wie in einem aktuellen Fall: Hier schickte der Vertriebsmitarbeiter eines Softwareherstellers eine E-Mail an 1.300 potenzielle Interessenten. Dabei nutzte er die CC-, anstatt wie gewünscht die BCC-Zeile seines E-Mail-Programms. Hierdurch gewann er wohl keine Kunden. Die Betroffenen nahmen die E-Mail-Flut vielmehr zum Anlass, eine Internet-Community zu gründen.

Die zitierten Fälle belegen die Brisanz der Thematik. Aufgrund des hohen Imageschadens für Unternehmen ist davon auszugehen, dass die bekannten Fälle nur einen kleinen Ausschnitt des tatsächlichen Gefahrenpotenzials darstellen. Dies gilt insbesondere für das äußerst heikle Thema der Wirtschaftsspionage. Hiervon sind vor allem Firmen betroffen, die in Ländern aktiv sind, in denen der Schutz von Urheber- und Patentrechten keinen hohen Stellenwert genießt. Wie konkret diese Gefahr ist, belegt die Tatsache, dass der weltweite Schaden durch Wirtschaftsspionage nach Schätzungen bereits in die Billiarden USD geht.

III. Gegenmaßnahmen

Neben organisatorischen Maßnahmen – wie z.B. Betriebsvereinbarungen – sind insbesondere technische Maßnahmen geeignet, die Risiken der IT im Unternehmen zu minimieren. Insbesondere in Bezug auf Dokumentensicherheit existiert bereits eine Reihe von ausgereiften Produkten. Mit deren Hilfe ist es möglich, exakt zu bestimmen, welcher Nutzer welche Rechte an dem Dokument besitzt. So ist es beispielsweise möglich festzulegen, dass eine E-Mail nur von Nutzer X gelesen werden darf. Darüber hinaus kann sogar der Nutzungszeitraum eines Dokuments eingeschränkt werden. Schließlich kann mit einem solchen Produkt auch verhindert werden, dass Dokumente an unbekannte Empfänger versandt werden können.

Dies wird dadurch realisiert, dass die Dokumente in verschlüsselter Form vorliegen. Vor jeder Aktion eines Nutzers (z.B. Öffnen, Drucken, Kopieren etc.) wird ein zentraler Rechner (sog. Policy-Server) abgefragt, ob der entsprechende Nutzer die Rechte hierzu besitzt. Ist dies nicht der Fall, kann er die Aktion nicht ausführen. Steht dem Nutzer temporär kein Netzzugang zur Verfügung (z.B. im Flugzeug), so besteht die Möglichkeit, ihm das Recht einzuräumen, die Datei zeitlich begrenzt „offline" zu benutzen.

Neben einem Rechtekonzept bieten moderne Enterprise Content Management-Plattformen (ECM) noch weitere Funktionen, um die Sicherheit digitaler Dokumente zu erhöhen. So kann die Authentizität eines Dokuments durch Digitale Signaturen sichergestellt werden. Des Weiteren hilft eine Versionshistorie (auch „Audit Trail" genannt), Änderungen an Dokumenten nachvollziehbar zu machen. Hierdurch kann man nachvollziehen, welcher Nutzer wann welche Aktion (z.B. Lesen) an dem Dokument vorgenommen hat. Zudem werden von einem Dokument mehrere Versionen vorgehalten, sodass sichergestellt ist, dass stets mit der aktuellsten Version eines Dokuments gearbeitet wird.

IV. Fazit

Aufgrund steigender rechtlicher Anforderungen an die Unternehmensführung und -überwachung sowie zunehmender technischer Bedrohungspotenziale durch IT ist das Haftungsrisiko für Vorstände und Aufsichtsräte drastisch gestiegen. Dem kann nur durch ein adäquates IT-Risikomanagement begegnet werden. Dieses sollte neben organisatorischen und rechtlichen auch technische Schutzvorkehrungen umfassen. Aufgrund fortschreitender Digitalisierung im Geschäftsverkehr stellen elektronische Dokumente eines der größten Bedrohungspotenziale dar. Eine Sicherheitslösung für elektronische Dokumente ist demnach ein elementarer Bestandteil eines IT-Risikomanagement-Systems.

Literaturhinweise:

ComputerPartner (2006): Mangelnde IT-Sicherheit – Gefahren für das Management, http://www.computerpartner.de/index.cfm?pid=179&pk=225923.

derStandard.at (2008): Mehr freie Zeit – Herr T. meinte es gut und schickte ein Mail cc an 1300 Menschen, http://derstandard.at/?url=/?id=1216325529161.

Gajek, Elektronische Datenräume verbessern Risikomanagement, „Der Aufsichtsrat", Heft 07-08/2006, S. 9-10.

Hackenberg (2005): Haftung für Unternehmensdaten – Handlungsbedarf für Vorstände und Geschäftsführer, http://www.competence-site.de/itmanagement.nsf/0/559fce18e2d43debc12570760037ee42?OpenDocument.