Dirk Bode / Dr. Jochen Haller*)

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 wesentliche Rolle. Zum einen sind durch eine Fülle neuer Gesetze und Vorschriften die Anforderungen der Stakeholder an die Qualität der Unternehmensführung merklich gestiegen. Zum anderen haben der technische Fortschritt im Bereich der IT und die zunehmende Vernetzung der globalen Wirtschaft das technische Bedrohungspotenzial signifikant erhöht. Diesem Haftungsrisiko kann nur durch den Aufbau eines adäquaten IT-Risikomanagement-Systems begegnet werden.

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

I. Grundzüge der Managerhaftung

Grundsätzlich gilt, dass die Unternehmensführung (Vorstand bzw. Geschäftsführer) Schaden vom Unternehmen so weit 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-Infrastruktur 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 (wie das Anlegerschutzverbesserungsgesetz und die EU-Datenschutzrichtlinie), die oft durch branchenspezifische Vorschriften wie z.B. das Teledienstedatenschutzgesetz ergänzt werden.

Ohne auf diese Vorschriften detailliert einzugehen, kann festgehalten werden, dass sie in der Regel folgende Gemeinsamkeiten aufweisen:

- 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 (gegebenenfalls einschließlich ihres Privatvermögens).

Insbesondere der letzte Punkt wird häufig übersehen. So kann das Unternehmen im Innenverhältnis das Management für Fehler in Regress nehmen, falls es verklagt worden ist. Vorstandsmitglieder, die ihre Pflichten verletzen, sind der Gesellschaft zum Ersatz des daraus entstehenden Schadens als Gesamtschuldner verpflichtet. Folglich haften sie persönlich mit ihrem gesamten privaten Vermögen. 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 Schadenersatzansprüche wegen Pflichtverletzungen gegen den Vorstand mit Erfolg eingeklagt werden könnten.

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, insbesondere Insolvenz, ein, haftet auch jedes Aufsichtsratsmitglied gegebenenfalls persönlich.

Die Schäden, die durch ein unzureichendes IT-Risikomanagement für ein Unternehmen entstehen können, 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,

*) Dirk Bode, Vorstandsvorsitzender, Dr. Jochen Haller, Assistent bei der fme-Gruppe, Braunschweig.

- Imageschaden,
- Schadenersatzpflichten,
- 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 Konzerns begonnen hatte, zirkulierten im Unternehmen anzügliche private E-Mails von ihm. Da der Aufsichtsrat das moralische Fundament des Unternehmens gefährdet sah, legte er dem CEO umgehend den Rücktritt nahe. Ein ähnlich weit reichendes 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 versehentlich 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 zwischen ihrem Vorgesetzten und der Personalabteilung konnte eine Managerin nachweisen, dass ihr Vorgesetzter sie so schnell wie möglich loswerden wollte.

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 von IT im Unternehmen zu minimieren. Insbesondere in Bezug auf die 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.

IV. Fazit

Aufgrund steigender rechtlicher Anforderungen des Gesetzgebers an die Unternehmensführung und aufgrund 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 zunehmender 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, Mangelnde IT-Sicherheit – Gefahren für das Management, http://www.computerpartner.de/index.cfm?pid=179&pk=225923.
- Gajek, Elektronische Datenräume verbessern Risikomanagement, „Der Aufsichtsrat" 07-08/2006, S. 9-10.