

Peter Weger/Dr. Stephanie Kaufmann\*)

# Wie sich Aufsichtsräte vor Informationsmissbrauch schützen können

In der modernen Gremienkommunikation greifen Aufsichtsräte weltweit via Internet auf sensible Unternehmensdaten zu. Um ihrer Überwachungsfunktion nachkommen zu können, sind sie auf die vollständige und rechtzeitige Bereitstellung der relevanten Informationen angewiesen. Auch nach Abberufung oder Ausscheiden aus dem Amt sind sie für fünf weitere Jahre zur Verschwiegenheit über Betriebsgeheimnisse und vertrauliche Angaben verpflichtet (§§ 116, 93 AktG). Die vertraulichen Dokumente können unveränderbar in einem web-basierten sicheren Datenraum hinterlegt werden, wo sie auch nach dem Ende der Amtszeit nur von Berechtigten eingesehen werden können. Sie sind vor dem Zugriff durch unbefugte Dritte bestmöglich geschützt.

„Informationen in einem elektronischen Datenraum sind vor unbefugtem Zugriff geschützt.“

## I. Einleitung

Um die Wettbewerbsposition eines Unternehmens zu sichern und den Auflagen der Börsenaufsicht zu genügen, genießt der Schutz vertraulicher Informationen höchste Priorität. Es muss eine Balance gefunden werden zwischen dem „Security Level“ und dem schnellen, flexiblen, weltweiten Zugriff auf Dokumente. Wie eine aktuelle Studie (Gefahrenbarometer 2010) zeigt, bestimmt die Einschätzung des Risikos durch ein Unternehmen letztlich den Grad des Dokumentenschutzes. Umfassende Sicherheit basiert auf geeigneten Verfahrensregeln für sensible und vertrauliche Daten. Außerdem verlangt die Klassifizierung von Informationen einen systematischen und fortlaufenden Prozess. Teil dieses Prozesses ist die Einführung allgemein gültiger Standards für die Vertraulichkeit von Unterlagen. Auch gesetzliche Vorgaben und vertragliche Verpflichtungen der Vorstände und Aufsichtsräte während und nach ihrer Amtszeit wirken sich hierauf aus. Um den Zielkonflikt zwischen der web-basierten, weltweiten Informationsbereitstellung und ihrem Schutz zu lösen, müssen Unternehmen eine „Document Compliance-Strategie“ definieren und Dokumente nach verschiedenen Kriterien wie Vertraulichkeitsgrad und unternehmerischer Relevanz klassifizieren. Sowohl technische als auch organisatorische Faktoren sowie rechtliche Haftungsfragen, z.B. nach dem Ausscheiden eines Aufsichtsrats, finden hierbei Berücksichtigung und beeinflussen den Gefahrengrad der Informationen.

## II. Kommunikation zwischen Vorstand und Aufsichtsrat

Der gesetzliche Auftrag an den Aufsichtsrat lautet: „Der Aufsichtsrat hat die Geschäftsführung zu überwachen“

(§ 111 Abs. 1 AktG). Aufsichtsratsmitglieder sind aber überwiegend nicht im Unternehmen anwesend, und ein persönlicher Kontakt zu den Vorständen findet nur in großen Abständen statt. Um dem Vorwurf mangelnder Überwachung und den damit verbundenen Haftungsrisiken zu entgehen, muss aber für kurze Informationswege und engen Kontakt gesorgt werden. Es ist Aufgabe des Aufsichtsrats, eine Informationsordnung zu erstellen, die dem Vorstand detailliert vorgibt, in welchen Abständen, zu welchen Themen und in welcher Form der Aufsichtsrat zu informieren ist (Tz. 3.4 Abs. 3 DCGK). An den Aufsichtsrat sind also regelmäßig Unterlagen wie Kennzahlen, Hinweise auf kritische Entwicklungen, anstehende Planungen usw. zu übersenden. Da es sich dabei in der Regel um sensible Daten handelt, muss der Aufsichtsrat dafür sorgen, dass diese Informationen schnellstmöglich und auf sicherem Weg zu ihm kommen. Das Internet darf bzw. soll hier genutzt werden: § 90 Abs. 4 AktG schreibt für die Informationen des Vorstands an den Aufsichtsrat nur die Textform vor, die bei einer schnellen, aktuellen und zielführenden elektronischen Übermittlung eingehalten wird.

## III. Gesetzliche Regelungen zur sicheren Kommunikation

Über vertrauliche Angaben und Geheimnisse der Gesellschaft, namentlich Betriebs- oder Geschäftsgeheimnisse, die ihnen durch ihre Tätigkeit im Aufsichtsrat bekannt geworden sind, haben Aufsichtsräte Stillschweigen zu bewahren (§ 93 Abs. 1 Satz 3 AktG). Insbesondere sind sie zur Verschwiegenheit über erhaltene vertrauliche Berichte und vertrauliche Beratungen verpflichtet (§ 116 Satz 2 AktG). Jedoch setzt gute Unternehmensführung eine offene Diskussion zwischen Vorstand und Auf-

\*) Peter Weger,  
CEO, Brainloop AG;  
RA Dr. Stephanie  
Kaufmann, Feldafing.

sichtsrat voraus. Die umfassende Wahrung der Vertraulichkeit innerhalb dieses Kreises ist dafür von entscheidender Bedeutung. Alle Organmitglieder stellen sicher, dass die von ihnen eingeschalteten Mitarbeiter die Verschwiegenheitspflicht in gleicher Weise einhalten (Tz. 3.5 DGCK). „Die Berichte haben den Grundsätzen einer gewissenhaften und getreuen Rechenschaft zu entsprechen. Sie sind möglichst rechtzeitig und ... in der Regel in Textform zu erstatten“ (§ 90 Abs. 4 AktG). „Mit Freiheitsstrafe bis zu einem Jahr, bei börsennotierten Gesellschaften bis zu zwei Jahren, oder mit Geldstrafe wird bestraft, wer ein Geheimnis der Gesellschaft, namentlich ein Betriebs- oder Geschäftsgeheimnis, das ihm in seiner Eigenschaft als Mitglied des Vorstands oder des Aufsichtsrats oder Abwickler ... bekannt geworden ist, unbefugt offenbart; ...“ (§ 404 Abs. 1 AktG).

#### IV. Kommunikation mit Dritten

Aufsichtsratsmitglieder dürfen ihre Aufgaben nicht durch andere wahrnehmen lassen (§ 111 Abs. 5 AktG). Aber: Die Rechtsprechung hat die Inanspruchnahme sachverständiger Hilfe durch Aufsichtsratsmitglieder nicht nur gestattet, sondern sogar als Teil einer pflichtbewussten Amtsausübung gesehen: „Ferner kann es zur sachgemäßen Ausübung des Mandats und damit wiederum zum Nutzen des Unternehmens angezeigt erscheinen, vor einer wichtigen Entscheidung fachkundigen Rat auch außerhalb des Aufsichtsrats einzuholen, wobei allerdings schon durch die Auswahl des Beraters einer Weitergabe oder einem sonstigen Missbrauch vertraulicher Mitteilungen vorzubeugen ist“ (BGHZ 64, S. 331 f.). Im DCGK heißt es: „Alle Organmitglieder stellen sicher, dass die von ihnen eingeschalteten Mitarbeiter die Verschwiegenheitspflicht in gleicher Weise einhalten“ (Tz. 3.5 DCGK). Zieht ein Aufsichtsratsmitglied einen Berater, Mitarbeiter oder Sachverständigen in einer bestimmten Sache hinzu und dieser lässt z.B. vertrauliche Unterlagen für Dritte einsehbar liegen, dann werden die Geheimhaltungs- und Verschwiegenheitspflichten verletzt. Entsteht dem Unternehmen durch ein solches Fehlverhalten ein Schaden, haftet das Aufsichtsratsmitglied auf Schadensersatz. Der Aufsichtsrat muss also vor allem auch in der Kommunikation mit Dritten für Sicherheit und Vertraulichkeit sorgen, um sich keinen Haftungsrisiken auszusetzen.

#### V. Risiken beim elektronischen Versand

E-Mails haben einen praktischen Vorteil gegenüber der Briefpost. Sie werden dem Empfänger innerhalb weniger Sekunden übermittelt und können von diesem sofort gelesen werden. Was jedoch gerne vergessen wird: E-Mails sind nicht sicher. Für den Geübten ist es sehr einfach, an die Inhalte ungeschützter E-Mails zu kommen. Ebenso birgt der Vorteil der einfachen Weiterleitung der E-Mail die große Gefahr der Fehlhantierung in sich, beispielsweise den Versand an den falschen Adressaten. Auch der Standort des Servers kann zu Sicherheitseinschränkungen führen. Sollte sich die Plattform beispielsweise in den USA befinden, erlauben weitreichende staatliche Regelungen, im Falle möglicher Gefahren Einsicht in E-Mail-Korrespondenz nehmen zu dürfen. Was als Gefahr eingestuft wird, ist eine Sache der Definition und entzieht sich

in aller Regel den Korrespondierenden, deren elektronische Briefinhalte demzufolge noch weniger geschützt sind.

#### VI. Aufbewahrung von Unterlagen

Jedes Aufsichtsratsmitglied ist zur Verschwiegenheit über Betriebsgeheimnisse und vertrauliche Angaben verpflichtet. Dazu gehört auch, dass die entsprechenden Unterlagen beim Aufsichtsratsmitglied vor dem Zugriff Dritter sicher sind. Abgesehen von der aufwändigen Informationsverwaltung droht dabei immer die Gefahr, gegen die Vertraulichkeit zu verstoßen. Um die sichere Aufbewahrung der Unterlagen zu gewährleisten, können seit einiger Zeit Dokumente eines jeden Aufsichtsratsmitglieds elektronisch abgelegt, verwaltet und zur Verfügung gestellt werden. Den gesetzlichen Anforderungen wird diese elektronische Verwahrung der Unterlagen gerecht, wenn sie sicher ist und die Vertraulichkeit der Inhalte gewahrt bleibt. In der Praxis kann diese vom Gesetzgeber geforderte Sicherheit nur von einem ganzheitlichen „Document Compliance Management-System“ geleistet werden. Dieses verfügt über eine durchgängige Verschlüsselung, einen starken Authentifizierungsmechanismus sowie individuelle Benutzerrechte und die verschlüsselte Archivierung in einem hochsicheren Umfeld.

#### VII. Haftungssituation nach dem Ende der Amtszeit

Wird ein Aufsichtsratsmitglied abberufen (§ 103 AktG) oder wird es nicht wiedergewählt, dann endet seine Amtszeit. Die Haftung kann das einzelne Aufsichtsratsmitglied aber noch über das Ende der Amtszeit hinaus treffen. Das ist dann der Fall, wenn die Gesellschaft einen Schaden erlitten hat, der durch das rechtswidrige und schuldhaft Verhalten des Aufsichtsratsmitglieds verursacht wurde, und dieser Schaden erst nach dem Ausscheiden zutage tritt. Hierzu zählt auch die fahrlässige Weiterleitung und Preisgabe vertraulicher Inhalte aus im Datenraum hinterlegten Dokumenten. Will die Gesellschaft ein Aufsichtsratsmitglied auf Schadensersatz verklagen, verjähren diese Ansprüche in fünf Jahren. Nach den allgemeinen Regeln müsste in einem solchen Fall der Anspruchsteller – also die Gesellschaft – nachweisen, dass das Aufsichtsratsmitglied seine Sorgfaltspflicht verletzt hat. Der Gesetzgeber hat hier aber eine Beweislastumkehr festgelegt. Das Aufsichtsratsmitglied muss seinerseits beweisen, dass es sich sorgfältig verhalten hat bzw. nicht schuldhaft vorgegangen ist. Damit unterliegt das Aufsichtsratsmitglied in der Praxis einer Haftungsverschärfung. Um nicht in dieser Situation an der Beweisnot zu scheitern, muss ein Aufsichtsratsmitglied, das einem Aufsichtsrat nicht mehr angehört, folglich das Recht haben, zu seiner Verteidigung alle möglicherweise relevanten Akten des Aufsichtsrats und auch des Vorstands der Gesellschaft einzusehen. Idealerweise sind diese in einem Datenraum für Document Compliance hinterlegt und damit vor unbefugtem Zugriff wirkungsvoll geschützt. Bezogen auf den Umgang mit unternehmenskritischen Informationen bedeutet dies ebenfalls, dass anhand der im Datenraum automatisch protokollierten Zugriffe nachgewiesen werden kann, wer die Dokumente zu welchem Zeitpunkt bearbeitet, heruntergeladen, gedruckt und weitergeleitet hat.