

Christopher Schrank/Martin Kollar

# Business Judgment Rule – der (neue) Sorgfaltsmaßstab auch für Aufsichtsratsmitglieder

*Ob das Management bei seinen Entscheidungen sorgfältig handelt, wird anhand der Business Judgment Rule geprüft, die seit 1. 1. 2016 ausdrücklich im AktG und im GmbHG verankert ist. Sie legt fest, wo der unternehmerische Ermessensspielraum aufhört und die Pflichtverletzung beginnt. Da für Aufsichtsratsmitglieder die Sorgfaltspflichten des Vorstands analog gelten, haben auch sie die Business Judgment Rule bei unternehmerischen Entscheidungen zu berücksichtigen. Dieser Beitrag zeigt auf, was die Business Judgment Rule für Entscheidungen im Unternehmen bedeutet und worauf Aufsichtsratsmitglieder in der Praxis achten müssen.*

## 1. DIE BUSINESS JUDGMENT RULE IN ÖSTERREICH

### 1.1. Ursprung

Die Business Judgment Rule hat ihre Wurzeln im US-amerikanischen Gesellschaftsrecht und wurde in den 1970er-Jahren von der Rechtsprechung im Bundesstaat Delaware entwickelt.<sup>(1)</sup> Ihr Grundgedanke ist, dass ein Manager nicht für Fehlentscheidungen haften soll, wenn er pflichtgemäß gehandelt hat. Das ist der Fall, wenn die Entscheidung

- in gutem Glauben,
- frei von Interessenkonflikten,
- auf Basis ausreichender Information und
- in der nachvollziehbaren Annahme, im besten Interesse des Unternehmens zu handeln, erfolgt. Maßgebend ist dabei die Sicht im Zeitpunkt der Entscheidung (Betrachtung *ex ante*). Sind diese Kriterien erfüllt, scheidet eine persönliche Haftung des Managers aus, auch wenn sich die unternehmerische Entscheidung im Nachhinein als falsch herausstellt.

### 1.2. Geltung

In Österreich wurde die Business Judgment Rule erst mit dem Strafrechtsänderungsgesetz 2015, BGBl I 2015/112, ausdrücklich im AktG

sowie im GmbHG verankert. Hintergrund dieses etwas ungewöhnlichen Ansatzes – nämlich eine gesellschaftsrechtliche Bestimmung im Zuge einer Strafrechtsreform anzupassen – war die Neuregelung der Untreue in § 153 StGB. Nach langen öffentlichen Diskussionen hat der Gesetzgeber beschlossen, den viel kritisierten Untreuetatbestand enger zu fassen.<sup>(2)</sup> Weil nun das Element der Pflichtwidrigkeit das zentrale Tatbestandselement der Untreue ist, sollte im Gesellschaftsrecht konkretisiert werden, wann ein pflichtwidriges Verhalten eines Entscheidungsträgers vorliegt.<sup>(3)</sup>

Der Gesetzgeber hat mit der Novelle freilich nur das im Gesetz ausdrücklich niedergeschrieben, was ohnedies bereits davor gegolten hat. Die herrschende Lehre ist schon vor Einfügung der Business Judgment Rule ins Gesetz davon ausgegangen, dass ihre inhaltlichen Kriterien als allgemeiner Rechtsgrundsatz anwendbar sind.<sup>(4)</sup> Was heute als Business Judgment Rule ausdrücklich im Gesetz steht, war in der Rechtsprechung schon davor als „*unternehmerisches Ermessen*“ anerkannt.<sup>(5)</sup>

Die Rechtsprechung geht dabei von einem sehr weiten Ermessensspielraum des Geschäftsleiters aus.<sup>(6)</sup> Eine Pflichtverletzung im gesellschaftsrechtlichen Sinn liegt nur bei einer eklatanten Überschreitung seines Ermessens und völlig unververtretbaren Entscheidung vor.<sup>(7)</sup>



- (1) *Gimbel v. Signal Companies, Inc.*, 316 A.2d 599 (Del.Ch. 1974), online abrufbar unter <https://casetext.com/case/gimbel-v-signal-companies-inc-2>.
- (2) Zur Kritik am alten Untreuetatbestand vgl etwa *Bollenberger/Wess*, Libro-Straferkenntnis: Untreue und Gesellschaftsrecht, RdW 2014, 247; *Kalss*, Gesellschaftsrechtliche Anmerkungen zur Libro-Entscheidung, *ecolex* 2014, 496.
- (3) Für einen Überblick über die Neuerungen des Untreuetatbestands siehe *Wess*, Entwicklung des Untreuestrafatbestands in Österreich, CFO aktuell 2015, 224.
- (4) *Ch. Nowotny in Doralt/Nowotny/Kalss*, AktG<sup>2</sup> (2012) § 84 Rz 8; *Strasser in Jabornegg/Strasser*, AktG<sup>5</sup> (2011) § 84 Rz 95a.
- (5) Vgl OGH 23. 2. 2016, 6 Ob 160/15w; *Ch. Schrank/Kollar*, Business Judgment Rule, CFO aktuell 2016, 117.
- (6) *Reich-Rohrwig in Straube/Ratka/Rauter*, GmbHG, § 25 Rz 33.
- (7) Vgl etwa OGH 22. 5. 2003, 8 Ob 262/02s; 11. 6. 2008, 7 Ob 58/08t.

MMag. Dr. Christopher Schrank ist Partner einer Rechtsanwalte-GmbH in Wien und auf Gesellschafts- und Wirtschaftsrecht spezialisiert.

MMag. Martin Kollar ist Rechtsanwaltsanwärter bei derselben Gesellschaft.

### 1.3. Umsetzung

Der Gesetzgeber hat die Business Judgment Rule dadurch umgesetzt, dass die Bestimmungen im AktG und im GmbHG über die Sorgfaltspflichten der Geschäftsleiter jeweils um einen neuen Absatz ergänzt worden sind (§ 84 Abs 1a AktG; § 25 Abs 1a GmbHG). Das Vorstandsmitglied oder der Geschäftsführer „handelt jedenfalls im Einklang mit der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters“, wenn es oder er folgende Kriterien einhält:<sup>(8)</sup>

- Die Entscheidung wird frei von sachfremden Interessen getroffen.
- Die Entscheidung wird auf Grundlage angemessener Information getroffen.
- Der Geschäftsleiter durfte in nachvollziehbarer Weise annehmen, zum Wohl der Gesellschaft zu handeln.

Trifft der Geschäftsleiter seine Entscheidung für das Unternehmen nach diesen Kriterien, handelt er sorgfaltskonform. Demzufolge kann er sich – auch wenn der erhoffte wirtschaftliche Erfolg der Maßnahme ausbleibt – dadurch nicht schadenersatzpflichtig oder strafbar machen. Den Geschäftsleiter trifft zivilrechtlich keine Erfolgshaftung für seine unternehmerischen Entscheidungen. Ebenso wenig kann eine sorgfaltskonform getroffene Entscheidung Gegenstand einer strafrechtlichen Untreue sein.

Festzuhalten ist aber, dass ein Nichteinhalten der Business Judgment Rule im Umkehrschluss nicht automatisch zur Folge hat, dass der Geschäftsleiter dann jedenfalls haftet.<sup>(9)</sup> Vielmehr wäre dann zu prüfen, ob im konkreten Fall eine Pflichtwidrigkeit und die allgemeinen Voraussetzungen einer Haftung vorliegen. Die Kriterien der Business Judgment Rule sind nur ein (wenngleich bedeutender) Teil der Sorgfaltspflichten des Geschäftsleiters. Sind die Vorgaben der Business Judgment Rule nicht erfüllt, wird das aber in aller Regel auf eine Pflichtverletzung hindeuten.<sup>(10)</sup>

(8) Die jeweilige Bestimmung im AktG bzw im GmbHG lautet: „Ein Vorstandsmitglied [Der Geschäftsführer] handelt jedenfalls im Einklang mit der Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters [eines ordentlichen Geschäftsmannes], wenn er sich bei einer unternehmerischen Entscheidung nicht von sachfremden Interessen leiten lässt und auf der Grundlage angemessener Information annehmen darf, zum Wohle der Gesellschaft zu handeln.“

(9) Vgl dazu auch IA 1110/A BlgNR 25. GP, 6.

(10) Vgl die Ausführungen zur Business Judgment Rule im deutschen AktG von *Spindler* in Münchener Kommentar zum AktG<sup>4</sup>, § 93 Rz 40.

(11) OGH 23. 2. 2016, 6 Ob 160/15w; vgl dazu auch *J. P. Gruber*, Haftung für unternehmerische Fehlentscheidungen (Business Judgment Role), Aufsichtsrat aktuell 5/2016, 33.

(12) Vgl dazu auch die Stellungnahme des OGH vom 12. 5. 2015 zum Initiativantrag zum Thema „Untreue und Business Judgement Rule“, 1 Präs. 1613-1748/15t, Punkt II., online abrufbar unter [http://www.ogh.gv.at/sites/www.ogh.gv.at/files/ogh/documents/Stellungnahmen/1praes.1613-1748.15t\\_stellungnahme.pdf](http://www.ogh.gv.at/sites/www.ogh.gv.at/files/ogh/documents/Stellungnahmen/1praes.1613-1748.15t_stellungnahme.pdf).

(13) *Kalss* in *Doralt/Nowotny/Kalss*, AktG<sup>2</sup>, § 99 Rz 5.

## 2. ERSTE ENTSCHEIDUNG DES OGH ZUR BUSINESS JUDGMENT RULE

Schon im Februar 2016, also unmittelbar nach der gesetzlichen Verankerung, hat sich der OGH zum ersten Mal mit den neuen gesetzlichen Bestimmungen zur Business Judgment Rule befasst.<sup>(11)</sup> Im konkreten Fall ging es um die Abberufung der Vorstandsmitglieder einer Privatstiftung. Der OGH hat in seiner Entscheidung erklärt, dass durch die Business Judgment Rule ein „rechtsformübergreifend anerkannter Rechtsgrundsatz“ gesetzlich festgelegt ist und diese somit auch für die Vorstandsmitglieder einer Privatstiftung gilt.<sup>(12)</sup> Die Tatsache, dass die Business Judgment Rule nur für die AG und die GmbH ausdrücklich im Gesetz verankert ist, bedeutet daher nicht, dass nur diese Rechtsformen von ihr erfasst sind. Vielmehr gilt die Business Judgment Rule als allgemeiner Sorgfaltsmaßstab für die Organe aller juristischen Personen.

Der OGH bestätigt mit seiner Entscheidung zudem, dass die Kriterien der Business Judgment Rule bereits vor der ausdrücklichen Verankerung im AktG und im GmbHG mit 1. 1. 2016 anwendbar waren. Ob die inhaltlichen Kriterien dabei als „unternehmerisches Ermessen“ bezeichnet werden oder jetzt der „Anglizismus der Business Judgement Rule“ verwendet wird, sei unbeachtlich. Im Kern – so der OGH – bedeutet beides dasselbe. Ob die gesetzliche Verankerung letztlich gar keine Veränderung, ein Herabsenken oder eine Erhöhung des Sorgfaltsmaßstabs bewirkt, wird davon abhängen, wie die Rechtsprechung die Kriterien der Business Judgment Rule in Zukunft auslegt und abgrenzt.

## 3. RELEVANZ FÜR AUFSICHTSRATSMITGLIEDER

Auch Aufsichtsratsmitglieder sind von der Business Judgment Rule erfasst. Sie sind nach dem Gesetz zur sorgfältigen Ausführung ihrer Tätigkeit verpflichtet.<sup>(13)</sup> Zu der von ihnen ein-

Der Gesetzgeber hat die Business Judgment Rule dadurch umgesetzt, dass die Bestimmungen im AktG und im GmbHG über die Sorgfaltspflichten der Geschäftsleiter jeweils um einen neuen Absatz ergänzt worden sind.

zuhaltenden Sorgfalt sieht § 99 AktG vor, dass der Maßstab für Vorstandsmitglieder sinngemäß gilt. Stehen somit unternehmerische Entscheidungen an, haben auch die Mitglieder des Aufsichtsrats die Business Judgment Rule einzuhalten. Hier ist vor allem an die beiden folgenden Fallgruppen zu denken:

- *Der Aufsichtsrat genehmigt Entscheidungen des Vorstands:* Sehen das Gesetz oder die Satzung eine Zustimmungspflicht des Aufsichtsrats vor, sind dessen Mitglieder unmittelbar an unternehmerischen Entscheidungen beteiligt. Ihre Aufgabe ist die sorgfältige Kontrolle der Entscheidung und ihrer Grundlage, bevor die Genehmigung erteilt wird. Wenngleich die Intensität der Kontrollpflicht vom Einzelfall abhängt, haben die Aufsichtsratsmitglieder regelmäßig nur die Plausibilität der konkreten Entscheidung und die Vollständigkeit der Informationsgrundlage zu prüfen. Ergeben sich in diesem Zusammenhang Anhaltspunkte für Zweifel, kann eine Detailprüfung erforderlich sein. Bei einer sorgfaltswidrigen Genehmigung können die Aufsichtsratsmitglieder zur Haftung herangezogen werden.<sup>(14)</sup> Wird etwa der Erwerb eines Konkurrenzunternehmens genehmigt, ohne dass der Vorstand dazu eine schlüssige Finanz- und Liquiditätsplanung vorlegt, wird eine Pflichtverletzung des Aufsichtsrats naheliegen.
- *Der Aufsichtsrat vertritt die Gesellschaft:* Das ist etwa der Fall, wenn der Aufsichtsrat den Vorstand bestellt oder dienstrechtliche Angelegenheiten mit den Vorstandsmitgliedern vereinbart werden. Handeln die Aufsichtsratsmitglieder dabei sorgfaltswidrig (zB weil einzelnen Vorstandsmitgliedern ein unangemessen hohes Entgelt gewährt wird), können ihnen Schadenersatzforderungen drohen.

Im folgenden Punkt 4. werden wir im Detail auf die Kriterien der Business Judgment Rule eingehen und dabei aufzeigen, was deren Anforderungen in Bezug auf die Arbeit im Aufsichtsrat konkret bedeuten. Dabei werden wir, weil dies in der Praxis der wichtigste Fall ist, vor allem auf die Genehmigung von Maßnahmen und Geschäften durch den Aufsichtsrat eingehen.

### 4. KRITERIEN

#### 4.1. Allgemeines

Die Business Judgment Rule ist nur anwendbar, wenn bei der unternehmerischen Entscheidung

ein Ermessensspielraum besteht. Das ist der Fall, wenn mehrere Handlungsalternativen vorliegen und die beste Option für die Gesellschaft ausgewählt werden soll. Ist das Handeln bereits zwingend vorgegeben (zB durch die Satzung oder eine ausdrückliche Weisung), bleibt bei der Entscheidung in der Regel kein Ermessensspielraum.

Der Aufsichtsrat übt bei seiner Entscheidung, einer Maßnahme oder einem Geschäft des Vorstands die Zustimmung zu erteilen oder diese zu verweigern, ein eigenes unternehmerisches Ermessen aus, das jenem des Vorstands vorgeht. Es steht dem Aufsichtsrat daher frei, eine Entscheidung des Vorstands etwa aus strategischen Gründen abzulehnen, auch wenn die Entscheidung sorgfältig vorbereitet und wirtschaftlich vertretbar ist.<sup>(15)</sup>

#### 4.2. Betrachtung *ex ante*

Ob ein Aufsichtsratsmitglied bei der Entscheidung über die Genehmigung eines Geschäfts sorgfaltskonform gehandelt hat, ist immer aus der Sicht im Zeitpunkt der Entscheidung zu beurteilen (*Betrachtung ex ante*). Das ist ein zentraler Punkt, weil es im Nachhinein – wie jeder weiß – leicht ist, zu sagen, welcher Weg eigentlich der Richtige gewesen wäre. Im Streitfall ist es daher wichtig, genau darzulegen, vor welcher Situation der Aufsichtsrat gestanden ist und welche Informationen ihm vorgelegen sind. Auf dieser Grundlage ist dann aufzuzeigen, welche Handlungsoptionen zur Verfügung gestanden sind und was – aus damaliger Sicht – deren Konsequenzen gewesen wären.

#### 4.3. Entscheidung frei von sachfremden Interessen

Das Aufsichtsratsmitglied ist in seiner Funktion verpflichtet, ausschließlich im Interesse der Gesellschaft zu handeln. Entscheidungen müssen daher frei von sachfremden Interessen getroffen werden. Der gesetzliche Begriff „*sachfremde Interessen*“ ist freilich unbestimmt. Erfasst sind davon jedenfalls Entscheidungen, bei denen ein Interessenkonflikt vorliegt. Das ist etwa der Fall, wenn ein Aufsichtsratsmitglied ein Geschäft genehmigt, von dem es selbst oder ein naher Angehöriger profitiert.

Fraglich ist, ob der Begriff „*sachfremde Interessen*“ über solche (eindeutigen) Interessenkonflikte hinausgeht und auch andere unsachliche Motive umfasst.<sup>(16)</sup> Hier könnten zB Prestige-

Auch Aufsichtsratsmitglieder sind von der Business Judgment Rule erfasst. Sie sind nach dem Gesetz zur sorgfältigen Ausführung ihrer Tätigkeit verpflichtet.

<sup>(14)</sup> Kalss in Doralt/Nowotny/Kalss, AktG<sup>2</sup>, § 95 Rz 106.

<sup>(15)</sup> G. Schima, Zustimmungsvorbehalte als Steuerungsmittel des Aufsichtsrates in der AG und im Konzern, GesRZ 2012, 35.

<sup>(16)</sup> Vgl dazu auch IA 1110/A BlgNR 25. GP, 6, wo von einer „*Freiheit von Interessenkollisionen*“ die Rede ist.

projekte, mit denen (auch) repräsentative Zwecke verfolgt werden, als sachfremde Interessen ausgelegt werden. Dieser Graubereich wird in den nächsten Jahren erst durch die Gerichte einzuschränken sein.

#### 4.4. Entscheidung auf Grundlage angemessener Information

Jede unternehmerische Entscheidung muss auf Basis angemessener Information getroffen werden. Wie fundiert eine Entscheidungsgrundlage tatsächlich sein muss, hängt in der Praxis von verschiedenen Faktoren ab:

- zur Verfügung stehende Zeit;
- wirtschaftliche Tragweite der Entscheidung;
- Anzahl der Handlungsalternativen;
- Komplexität des Sachverhalts;
- Höhe der Kosten (etwa durch externe Gutachten) für die Beschaffung der Information.

Diese Auflistung ist nicht abschließend und soll nur veranschaulichen, dass die Frage, welche Informationen aufbereitet werden müssen, bevor eine Entscheidung getroffen wird, immer im Einzelfall zu beurteilen ist. Es handelt sich dabei um ein bewegliches System: Je komplexer der Sachverhalt oder je wichtiger die Entscheidung für das Unternehmen ist, umso genauer ist auch die Entscheidung vorzubereiten. Hierbei ist natürlich auch zu berücksichtigen, dass der Maßstab der angemessenen Information in Bezug auf den Aufsichtsrat in der Regel niedriger als beim Vorstand sein wird.

Der Aufsichtsrat wird vom Vorstand regelmäßig mit komplexen Sachverhalten von hoher wirtschaftlicher Tragweite konfrontiert. Der Vorstand muss dem Aufsichtsrat eine Entscheidungsgrundlage vorlegen, die es dem Aufsichtsrat ermöglicht, eine Plausibilitätsprüfung durchzuführen. Zur Absicherung des eigenen Standpunktes kann es im Einzelfall aber auch für den Aufsichtsrat sinnvoll sein, externe Gutachten (etwa Rechtsgutachten oder *fairness opinions*) einzuholen. Diese werden in der Regel als angemessene Grundlage im Sinne der Business Judgment Rule gelten.

Ist die Informationsgrundlage ausreichend, prüfen die Aufsichtsratsmitglieder die Plausibilität der Entscheidung – zu mehr sind sie regelmäßig nicht verpflichtet – und erteilen oder verweigern auf dieser Basis ihre Zustimmung. Eine Entscheidung ohne ausreichende Informationsgrundlage ist hingegen sorgfaltswidrig.

#### 4.5. Annahme, zum Wohl der Gesellschaft zu handeln

Mit diesem Kriterium der Business Judgment Rule wird die Vertretbarkeit einer Entscheidung beurteilt. Bei der Genehmigung einer Maßnahme oder eines Geschäfts müssen Aufsichtsratsmitglieder vernünftigerweise annehmen dürfen, zum Wohl der Gesellschaft zu handeln. Das ist etwa der Fall, wenn eine Entscheidung der langfristigen Ertragsstärkung und Wettbewerbsfähigkeit des Unternehmens dient. Maßgebend ist die subjektive Sicht im Entscheidungszeitpunkt. Diese muss bei objektiver Betrachtung zwar nicht richtig, aber zumindest nachvollziehbar sein. Diese Grenze wird überschritten, wenn das mit der Entscheidung verbundene Risiko in völlig unverantwortlicher Weise falsch beurteilt wird.<sup>(17)</sup>

Festzuhalten ist, dass es bei unternehmerischen Entscheidungen in der Regel mehr als eine zulässige Handlungsalternative gibt und auch inhaltlich zueinander konträre Handlungsalternativen bei einer Entscheidung zulässig sein können.<sup>(18)</sup> Hier ist auch der weite Ermessensspielraum, den die Rechtsprechung bei unternehmerischen Entscheidungen einräumt, zu berücksichtigen.

#### 4.6. Dokumentation

Neben der Einhaltung des Weges, den die Business Judgment Rule für die Entscheidungsfindung vorgibt, ist es in der Praxis genauso wichtig, diesen Prozess in den Aufsichtsratsprotokollen entsprechend zu dokumentieren. Ohne Zweifel ist jede Dokumentation mit zusätzlichem Aufwand verbunden. Es sollte aber bedacht werden, dass Gerichtsprozesse und Ermittlungsverfahren oft erst viele Jahre später schlagend werden. Es ist dann oft kaum mehr möglich, noch im Detail zu begründen, was die Hintergründe einer konkreten Entscheidung waren und warum nicht eine – im Nachhinein betrachtet vielleicht bessere – Alternative gewählt worden ist. Um einen solchen Beweisnotstand zu vermeiden, helfen Aufzeichnungen ungemein. Die praktische Erfahrung zeigt auch, dass Gerichte solchen Dokumenten, die im Zeitpunkt der Entscheidung erstellt worden sind, einen höheren Beweiswert zumessen als nachträglichen Erklärungen auf Basis der oft nur mehr ungenauen Erinnerung.

Aufsichtsratsmitglieder können sich gegen zivilrechtliche Haftungen und strafrechtliche Konsequenzen absichern, indem sie Entscheidungen nach dem Raster der Business Judgment Rule treffen und dabei den Prozess der Entscheidungsfindung auch entsprechend dokumentieren.

(17) Siehe Hüffer/Koch, AktG<sup>12</sup> (2016) § 93 Rz 23.

(18) Reich-Rohrwig in Straube/Ratka/Rauter, GmbHG, § 25 Rz 34.



### 5. ZUSAMMENFASSUNG

Der Gesetzgeber hat mit der Verankerung der Business Judgment Rule im AktG und im GmbHG nur das klargestellt, was nach der Rechtsprechung bereits davor gegolten hat. Auch der OGH betont in seiner ersten Entscheidung zur neuen Regelung, dass die Business Judgment Rule ein allgemeiner Rechtsgrundsatz ist und daher generell als Sorgfaltsmaßstab für unternehmerische Entscheidungen der Organe aller juristischen Per-

sonen gilt. Die Business Judgment Rule ist neben den Geschäftsleitern auch für Mitglieder des Aufsichtsrats anwendbar, soweit diese an unternehmerischen Entscheidungen beteiligt sind.

Aufsichtsratsmitglieder können sich gegen zivilrechtliche Haftungen und strafrechtliche Konsequenzen absichern, indem sie Entscheidungen nach dem Raster der Business Judgment Rule treffen und dabei den Prozess der Entscheidungsfindung auch entsprechend dokumentieren.

Rainer Baumgart

## Geheimhaltung und Datensicherheit für Aufsichtsräte

*Wenn Aufsichtsrat und Vorstand miteinander auf elektronischem Weg kommunizieren, handelt es sich praktisch ausnahmslos um vertrauliche Informationen. Seien es Kennzahlen, Daten zur aktuellen Geschäftsentwicklung, relevante Antworten zur Strategie oder Informationen zu M&A: Gelangen diese durch Verlust oder Datendiebstahl in falsche Hände, kann sich das rasch negativ auf das Unternehmen auswirken.*

### 1. ANALYSE DER GEFAHRENLAGE

Der gesetzliche Auftrag des Aufsichtsrats bringt es mit sich, dass er frühzeitig Zugang zu fast allen unternehmensrelevanten Informationen hat. Diese Informationen sollen auf dem schnellsten Weg – und das ist heutzutage der elektronische – zum Aufsichtsrat gelangen.

Was liegt für einen Wettbewerber, Kriminellen oder Wirtschaftsspion näher, als sich diesen Umstand zunutze zu machen und sich an dieser Stelle auf die Suche nach relevanten Informationen zu begeben? Der Aufwand, sich in die Systeme eines Unternehmens zu hacken und an verschiedenen Orten die Informationen zusammenzutragen, erfordert viel mehr Einsatz, als die aufbereiteten Informationen, die gesammelt an den Aufsichtsrat gegeben werden, abzufangen.

Ein weiterer Vorteil für die Angreifer ist die IT-Ausstattung der Aufsichtsratsmitglieder. Häufig nutzen sie ihre persönliche IT und greifen nicht auf die IT-Infrastruktur des Unternehmens zurück. Das Sicherheitsniveau dürfte bei den meisten Aufsichtsräten daher vergleichbar mit dem einer gewöhnlichen Privatperson sein – und das entspricht sicher nicht der hierbei erforderlichen Vertraulichkeitsstufe. Damit wird es für Datendiebe zum leichten Spiel. Gerade der Übertragungsweg der Information bietet

sich an: Sender und Empfänger der Kommunikationsvorgänge sind in der Regel bekannt und ihre E-Mail-Adressen sind sehr leicht zu ermitteln. Mithilfe der feststehenden und ebenfalls bekannten Veröffentlichungstermine kann der Hacker leicht einen zeitlichen Korridor antizipieren, in dem die Wahrscheinlichkeit sehr hoch ist, dass vertrauliche Informationen elektronisch übermittelt werden.

### 2. MÖGLICHE SCHUTZMASSNAHMEN SEITENS DER AUFSICHTSRÄTE

Was können Aufsichtsräte tun, um die Hürde für die Angreifer möglichst hoch anzusetzen? Welche Schutzmaßnahmen sollten ergriffen werden, damit die Informationen an der Schnittstelle zwischen Unternehmen und Aufsichtsrat nicht abfließen können?

#### 2.1. Verschlüsselung

Eine hochwertige Verschlüsselung der gespeicherten Informationen ist – genauso wie die Verschlüsselung der gesamten Kommunikation – die Basis für einen sicheren Informationsaustausch zwischen Aufsichtsrat und dem Unternehmen. Nur so kann verhindert werden, dass Informationen im Klartext über das Internet ausgetauscht oder sie bei Verlust und Diebstahl



Dr. Rainer Baumgart ist Vorstandsvorsitzender eines führenden deutschen Anbieters für anspruchsvolle IT-Sicherheit. Er zeichnet sich verantwortlich für die Geschäftsbereiche Public und Business, die Unternehmensentwicklung/-strategie, Compliance/Revision und Kommunikation/Marketing.