



# Aufgepasst!

**Foren, Blogs und Wikis** verändern die Art, wie Mitarbeiter in Unternehmen sich informieren, kommunizieren und zusammenarbeiten. Den Vorteilen von Web-2.0-Anwendungen stehen allerdings zum Teil gravierende Risiken gegenüber. Vor allem die rechtlichen Aspekte sind nicht zu unterschätzen.

Stephan A. Klein

**D**as Schlagwort Compliance steht bei vielen Unternehmen im Fokus. Vor allem die gestiegene Komplexität von Geschäftsprozessen, die sich daraus ergebenden rechtlichen Risiken und die unmittelbar damit zusammenhängenden Dokumentationspflichten lassen es sinnvoll erscheinen, im Rahmen einer ganzheitlichen Betrachtung auch „Randbereiche“ wie Web 2.0 in die Compliance-Strategie einzubeziehen.

Viele Unternehmen haben erkannt, dass der so genannte User generated Content – Inhalte, die von Internet-Nutzern erstellt wurden – als Bereicherung ihrer Internet-Strategie dienen kann. Denn der kollaborative Charakter des Internets ermöglicht es jedem, Dienste und Content zusammenzustellen und zu veröffentlichen. Neben den Vorteilen – wie einer höheren Nutzerbindung und kostenlosem Content – sind aber auch die Risiken nicht zu vernachlässigen. Wie sichern sich insbesondere kleine und mittlere Unternehmen hier ab? Und welche Bereiche im Unternehmen sind unter den strengen Augen der Compliance besonders zu beachten?

Aus rechtlicher Sicht stellt Web 2.0 alle Beteiligten vor neue Herausforderungen. Das betrifft nicht nur Unternehmen, die mit Web 2.0 direkt in ihrem Kerngeschäft zu tun haben.

Der Umgang mit Nutzern unterliegt nationalen und internationalen Rechtsgrundlagen. So müssen im Zuge von Web-2.0-Anwendungen auch Unternehmen Lösungen für ein ganzheitliches und nachhaltiges Datenschutz- und Identitätsmanagement entwickeln und in ihre Compliance-Strategie einbinden.

## **Risikofaktor User generated Content**

Wenn man wesentliche Compliance-Aspekte auf das Web 2.0 herunterbricht, steht die Betrachtung des User generated Content im Vordergrund. Interaktionsformen wie Diskussionsforen oder Feedback-Plattformen stellen auf der einen Seite eine kostenneutrale Bereicherung für Unternehmen dar, auf der anderen Seite aber auch ein unmittelbares Risiko. Im schlimmsten Fall gelangen unerwünschte, auch rechtswidrige Inhalte in den Internet-Auftritt des Unternehmens.

## DER AUTOR



**Rechtsanwalt Stephan A. Klein** ■  
Leiter der Internal Services der Atrada AG  
in Nürnberg

Darüber hinaus können Spannungen zwischen dem Datenschutz – sprich der Notwendigkeit zur Erfassung von Daten des Content-Erstellers – und dem Wunsch nach Anonymität auftreten. Hier müssen alle Vorgänge aus Unternehmenssicht zur wirksamen Kontrolle und besonders hinsichtlich notwendiger Handlungsrichtlinien im Falle eines Verstoßes eindeutig nachvollziehbar sein. Daher kommt der Historisierung eine bedeutende Rolle zu: Der Veröffentlichungszeitpunkt sowie nachträgliche Veränderungen von User generated Content müssen sich eindeutig erkennen und chronologisch zuordnen lassen.

### Content Policy: Regeln für alle

Um Konflikten vorzubeugen, hat es sich in der Praxis bewährt, klare Regeln für User generated Content zu kommunizieren. Die meisten User verstoßen nicht vorsätzlich gegen Regeln, sondern aus Unkenntnis oder Unbedacht-

heit. Hier kann man mit Hilfe einer Art Content Policy die unerwünschten Verhaltensweisen oder Themen bereits im Vorfeld benennen und damit eine klare Orientierung schaffen.

Im Übrigen werden besonders in Diskussionen persönliche Meinungen häufig sehr emotional kommuniziert. Hier gilt es, moderierend einzugreifen und ein sachliches Niveau zu fordern bzw. dieses auch durchzusetzen. Konsequentes Handeln zahlt sich aus – schließlich wird der User generated Content auf der Unternehmens-Website publiziert, so dass das eigene Image unmittelbar betroffen ist.

### Selbstbestimmung und Aufklärung

Der kollaborative Charakter des Web 2.0 ermöglicht es jedem, Inhalte zu erstellen und zu veröffentlichen. So hinterlassen Nutzer im Laufe der Zeit unzählige Datenspuren – ein latenter Konflikt zwischen dem Recht auf informelle Selbstbestimmung des Users und den Anforderungen an die Nachvollziehbarkeit. Mit Hilfe technischer Restriktionen, einer wichtigen Säule im Datenschutz- und Sicherheitskonzept, sollten User selbst bestimmen können,

wer ihre Inhalte in welcher Form nutzen darf und wie viel über den Ersteller preisgegeben wird.

Bewährt hat sich hier eine offene Kommunikation über die Art und den Umfang der Datenspeicherung, etwa im Rahmen einer Datenschutz-Policy sowie über die Möglichkeiten, selbst auf den Umfang der Veröffentlichung Einfluss zu nehmen.

### Kein rechtsfreier Raum

Im Internet gelten grundsätzlich die gleichen gesetzlichen Rahmenbedingungen und Regelungen wie in der Offline-Welt. Demzufolge muss sich jeder, der fremdes Recht verletzt – etwa durch die Veröffentlichung fremder Fotografien – nach den allgemeinen Regelungen wie dem Urheberrechtsgesetz verantworten. Doch auch für Unternehmen entsteht ein Risiko: Verletzen sie Rechte im Rahmen ihres Internet-Auftritts, können sie vom Rechteinhaber nach der so genannten Mitstörerhaftung ebenfalls zur Verantwortung gezogen werden.

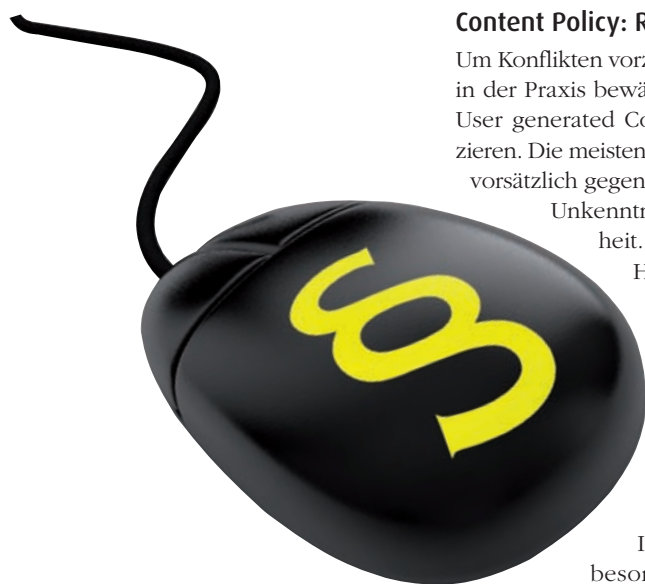
Viele Gerichtsentscheidungen beschäftigen sich bereits mit diesem Thema. Allerdings werden insbesondere die im Telemediengesetz statuierten Haftungsprivilegien sehr unterschiedlich ausgelegt und angewandt, so dass bis zu einer noch ausstehenden höchstrichterlichen Entscheidung Rechtsunsicherheit herrscht. Unabhängig von der juristischen Dimension liegt es jedoch für die Mehrzahl der Anbieter von Web-2.0-Portalen im eigenen Interesse, ihre Community zu schützen.

### Eskalationen verhindern

Um Konflikte zu vermeiden, sollten Web-2.0-Elemente von Anfang an in die Compliance-Strategie eines Unternehmens einbezogen werden. Dazu müssen zum einen Risikoszenarien identifiziert und zum anderen mögliche Reaktionen unter der Berücksichtigung von Eintrittswahrscheinlichkeit und Schadenspotenzial vorbereitet werden.

Bei der Umsetzung ist es ratsam, klare Verantwortlichkeiten festzulegen und kontinuierliche Prozesse zum Monitoring zu etablieren. Ebenfalls dazu gehört eine nachvollziehbare Dokumentation der erfolgten Präventivmaßnahmen.

Kommt es zu einer Rechtsverletzung, zählt in erster Linie eine schnelle Reaktion. Juristische Auseinandersetzungen strebt meist keiner der Beteiligten an.



Wenn Mitarbeiter im Web publizieren, kann das für die Firma unangenehme Folgen haben.

Vielmehr zählt das rasche und unbürokratische Beheben des Rechtsverstößes. Dabei kann der direkte Dialog zwischen Rechteinhaber und -verletzer helfen.

### **Betrugsprävention und Erkennung**

Grundsätzlich lässt sich der Missbrauch von Web-Angeboten in strafrechtlich relevantem Umfang nie ausschließen. Deshalb ist es wichtig, neben dem manuellen Screening bestimmte „gefährliche“ Muster möglichst automatisiert zu erkennen. Diese Muster sind individuell abhängig vom konkreten Geschäftsmodell des Internet-Angebotes und bilden sich im Laufe der Zeit heraus. Ein Beispiel ist die Einbindung externer Quellen in den User generated Content: Dabei wird Schad-Software auf den Rechner des häufig ahnungslosen Endnutzers transferiert; dieser nimmt wiederum an, die Software unmittelbar durch das Angebot des Unternehmens erlangt zu haben.

Der Reputationsschaden ist hierbei enorm – im einfachsten Fall hätte es geholfen, das Einstellen von externem Content zu unterbinden. In komplexeren Szenarien erfolgt auch eine automatisierte Kontrolle externer Quellen, die abhängig vom Ergebnis den Zugriff unterbindet oder zulässt. Je nach Schwere des Missbrauchs gibt es unterschiedliche Gegenmaßnahmen: vom Ausschluss des Users von der Nutzung des Online-Angebotes bis hin zur Einleitung rechtlicher Schritte.

### **Der Umgang mit Ermittlungsbehörden**

Nicht nur Anbieter überprüfen Unternehmen, auch Ermittlungsbehörden fragen regelmäßig Nutzerdaten ab – entweder in Eigeninitiative oder, was häufiger vorkommt, aufgrund von Hinweisen Dritter. Hierdurch geraten Unternehmen schnell in Konflikt mit datenschutzrechtlichen Bestimmungen, da die persönlichen Registrierungsdaten der Nutzer und möglicherweise sogar Daten zur Nutzungshistorie übermittelt werden sollen. Betreiber von Online-Angeboten stehen damit im Zwiespalt zwischen dem Schutz der Privatsphäre ihrer Nutzer auf der einen und der grundsätzlich gebotenen Unterstützung der Ermittlungsbehörden auf der anderen Seite.

In der Praxis zieht damit jede Anfrage einen manuellen Prüfungsprozess nach sich, dabei sollte man mit der Übermitt-

lung persönlicher Nutzerdaten zurückhaltend umgehen. Gegebenenfalls ist es empfehlenswert, einen Rechtsanwalt einzuschalten, der die Rechtsgrundlagen, nach denen sich möglicherweise eine Verpflichtung zur Herausgabe von Daten ergibt, kennt. In künftigen Fällen kann das Unternehmen auf dieser Basis selbst entscheiden.

### **Minenfeld E-Mail-Archivierung**

Das Thema Compliance beschränkt sich im Kontext von Web-2.0-Anwendungen jedoch nicht nur auf die Applikation als solche, sondern reicht auch in damit eng verbundene Bereiche im Unternehmen hinein. Besonders hervorzuheben ist hier das Thema E-Mail-Archivierung. Trotz ihrer herausragenden rechtlichen Bedeutung – insbesondere im Hinblick auf die Dokumentation von Geschäftsvorfällen – zeichnet sie sich durch allgemeine Unbeliebtheit und – daraus folgend – mangelhafte Umsetzung aus.

Dabei sind Unternehmen gemäß der GDPdU-Verordnung (Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen) vom 1. Januar 2002 verpflichtet, alle steuerrelevanten Daten in maschinell auswertbarer Form aufzubewahren. So müssen E-Mails mit samt ihren Anhängen genau wie Hardcopies, Fax- und Textdokumente zehn Jahre lang gespeichert werden (nach § 257 Abs. 4 des Handelsgesetzbuches und § 147 Abs. 3 der Abgabenordnung). Und dies in einer Form, die dem Inhalt, der Nutzung und dem Rechtscharakter entspricht. Aus diesem Grund ist beim elektronischen Archivieren der Kontext der Mail zu beachten. Darüber hinaus dürfen E-Mails weder inhaltlich verändert noch im Nachhinein ergänzt werden.

### **Die Infrastruktur sichern**

Im Bestreben, die Vorteile und enormen Potenziale digitaler Anwendungen optimal auszuschöpfen, bleiben die vom Internet ausgehenden Risiken in den Compliance-Überlegungen oft außen vor. Doch zunehmend sind auch die elektronischen Geschäftsprozesse kleiner und mittlerer Unternehmen das Ziel böswilliger Angreifer.

Ein Verlust von Kundendaten aufgrund einer unzureichend abgesicherten Plattform dürfte den betroffenen Kunden schwer vermittelbar sein und im Extremfall sogar Schadensersatzforderungen nach sich ziehen. Dies gilt

## **Compliance-Aspekte rund ums Web 2.0**

- > Automatisierte Filterung und manuelle Kontrolle (Stichproben)
- > Aufstellung einer Content-Policy
- > Anpassung des Datenschutzes und Identitätsmanagements an Web-2.0-Anforderungen
- > Implementierung von Eskalationsszenarien (Verantwortlichkeiten, Monitoring, Dokumentation).



## Wer haftet bei Rechtsverstößen? Der Autor oder das Unternehmen, für das er arbeitet?



umso mehr, wenn auch Zahlungsdaten, beispielsweise Kreditkartendaten, vom Datenleck betroffen sind. Insbesondere in diesem Fall droht auch von Seiten der Kreditkarten ausgebenden Banken Ärger.

Die Kosten des Austausches der betroffenen Karten trägt im Regelfall das Unternehmen, das für die Kompromittierung verantwortlich ist. Darüber hinaus kann auch die Berechtigung zur Kreditkarten-Akzeptanz entzogen werden. Um diesen Risiken effektiv zu begegnen, betrachten komplexe Konzepte Sicherheit als einen andauernden Prozess, der im Optimalfall bereits in der Planungsphase einer Plattform berücksichtigt wird. Er basiert, vereinfacht dargestellt, auf drei Säulen. Deren wesentliche Bestandteile sind

- die Sicherheit innerhalb der Serverplattform,
- die Absicherung der Web-Anwendungen selbst
- sowie der Umgang mit Daten innerhalb des Unternehmens.

Neben der Implementierung gängiger Sicherheitsstandards und einem gesunden Misstrauen ist die fortwährende Überwachung des IT-Systems wichtig. Um Risiken früh zu erkennen und mög-

liche bestehende Lücken zu schließen, bieten sich Intrusion-Detection-Systeme (IDS) sowie bei Bedarf ein regelmäßiger externer Sicherheits-Audit an.

### Fazit

Der Nutzen von Web-2.0-Anwendungen wie Bewertungssystemen, Foren, Blogs und Wikis als Mittel der Unternehmenskommunikation und Anreicherung von kommerziellen Angeboten ist vielfältig: So profitiert die gesamte Wirtschaft von den integralen und direkten Möglichkeiten der Kundenansprache und der User von einer „neutralen“ Perspektive anderer Nutzer.

Eng damit verbunden ist jedoch die Herausforderung, diese neuen Medien und ihre Besonderheiten in die Compliance-Strategie einzubinden. Nur die Beachtung und Einbeziehung von Regularien und die Sensibilisierung der User im Umgang mit digitalen Daten kann den Weg ebnen, um aus dem Web 2.0 wertvolle Erkenntnisse zu filtern und seine Elemente Gewinn bringend im Unternehmen einzusetzen. [rm]