

Umgang mit **vertraulichen** **Dokumenten**



Unternehmen werden mit immer mehr gesetzlichen Regelungen zu Datenschutz und Datenarchivierung konfrontiert. Mittelständische Unternehmen stehen zudem oft in einem besonders dynamischen Wettbewerb und haben – verglichen mit Großunternehmen – deutlich begrenztere Ressourcen, um die Governance-, Risk- und Compliance-Thematik in der Praxis zu beherrschen.



Nicht zuletzt sind die Daten, insbesondere der mittelständischen Unternehmen, als Unternehmenswert und -potenzial für den Marktausbau von existentiellem Wert. Die IT und das Informationsmanagement spielen hierbei eine entscheidende Rolle. Entsprechend ist nicht nur eine effiziente Infrastruktur und ein reibungsloser Betrieb erforderlich, sondern auch höchste Sicherheit beim Austausch vertraulicher Dokumente.

Risiken beherrschen

Wie werden Risiken transparent und beherrschbar gemacht? Wie kann in der Praxis die Einhaltung von Gesetzen und Richtlinien im Umgang mit zu schützenden Unterlagen ermöglicht werden? Zunächst ist „Compliance“ nichts anderes als die Einhaltung von Regeln, unabhängig davon, ob diese von externen Stellen oder von der Unternehmensführung selbst festgelegt werden. In der deutschen Sprache ist der Begriff Regelkonformität geläufig.

Während große Unternehmen die Führung und Kontrolle ihrer Unternehmen längst auf eine langfristige Wertschöpfung ausgerichtet haben und Compliance-Programme fester Bestandteil des Geschäftsalltags sind, tut sich der Mittelstand bei der Umsetzung noch schwer. Das hat eine Markterhebung des Kölner Prüfkonzerns TÜV Rheinland ergeben (siehe Kölner Nachrichten 8. 6. 2011). Zwar ist demnach für zwei Drittel der Unternehmen Compliance-Management ein wichtiges Thema. Allerdings hinkt die Umsetzung solcher Programme deutlich hinterher.

Trotz der verschärften Haftungssituation für Unternehmen und ihre Organe gibt es weiterhin große Vorbehalte gegen die Verwirklichung von Compliance. Das gängigste Argument dagegen ist die Befürchtung vieler Verantwortlicher vor einer allzu großen Bürokratisierung. Doch Compliance-Management kann gewinnbringend für die Unternehmen sein, die es richtig anzuwenden verstehen. „Gute Compliance“ machen vor allen Dingen die Spielregeln und Regularien aus, die sich ein Unternehmen intern gibt.

Gründe für Compliance-Systeme

Die Gefahr, Compliance-Verstöße zu begehen, oder Opfer von solchen zu werden, ist bei mittelständischen Unternehmen genauso groß wie bei den Großkonzernen. Als Konsequenz fehlender Präventionsmaßnahmen drohen Unternehmen und deren Leitungsorganen Geld- und Freiheitsstrafen, die gerade für mittelständische Unternehmen existenzbedrohend sein können. Neben dem Vermeiden von Compliance-Verstößen bietet ein wirksames Compliance Management auch gegenüber Auf-

bote gewährleisten sollen. Hinter dem Begriff Compliance steht aber mehr als nur Gesetzestreue, nämlich die Frage, wie die Einhaltung der gesetzlichen und innerbetrieblichen Vorgaben durch die Einführung entsprechender Maßnahmen innerhalb eines Unternehmens sichergestellt werden kann.

Mehr noch als für große Konzerne kann mangelhafte Compliance für mittelständische Unternehmen zum Existenzrisiko werden. Insbesondere in den Bereichen Korruption und Kartellverstöße, kann es zu erheblichen Bußgeldern und Gewinnabschöpfungen



Bild 1: An unternehmenskritischen Vorgängen beteiligte interne und externe Mitarbeiter brauchen ein Document Compliance Management.

traggebern, Lieferanten und Kunden einen Mehrwert. So legen insbesondere international aufgestellte Unternehmen aus Gründen des Selbstschutzes zunehmend Wert auf das Vorhandensein eines solchen Compliance-Systems bei ihren Geschäftspartnern. Verstärkt wird dieser Umstand durch neue Gesetze wie beispielsweise den UK Bribery Act.

Der Begriff „Compliance“ umfasst die Gesamtheit der Maßnahmen, die das rechtmäßige Verhalten eines Unternehmens, seiner Organe und Mitarbeiter im Hinblick auf alle gesetzlichen und unternehmenseigenen Gebote und Ver-

kommen. Werden Strafverfahren eingeleitet, so droht nicht nur die Einziehung der rechtswidrig erlangten Gewinne nach Abschluss des Strafverfahrens, oft droht auch die Verhängung eines Arrestes, wodurch dem betroffenen Unternehmen unmittelbar und massiv Vermögen entzogen werden kann. Daneben droht die persönliche Strafbarkeit von handelnden Mitarbeitern und der Geschäftsleitung.

Neben der Verhinderung von Korruption und kartellrechtlichen Verstößen sind zahlreiche andere – oft übersehene und unterschätzte Ge- und

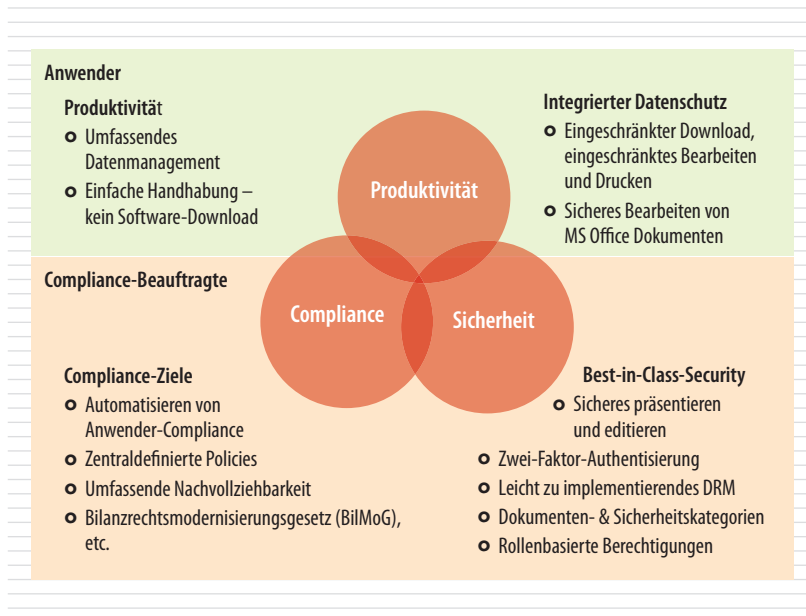


Bild 2: Der Compliance Officer steuert die Interessen und Ziele des Unternehmens und der Beteiligten.

Verbote zu beachten. Der aktuelle Beitrag fokussiert sich auf den Schutz von Dokumenten, hier insbesondere vertrauliches Wissen, das in der unternehmensübergreifenden Zusammenarbeit mit Mitarbeitern oder externen Spezialisten elektronisch ausgetauscht wird.

Je sensibler Informationen sind, umso stärker ist die Tendenz zu beobachten, dass sie die Unternehmensgrenzen verlassen. Dieses geschieht, weil gerade diese vertraulichen Informationen mit externen Beratern, Anwälten oder Partnern gemeinsam bearbeitet werden müssen. Folglich verlassen die Dokumente die schützende Firewall des Unternehmens und interne Schutzmaßnahmen greifen nicht mehr. Zu den Anwendungsfällen zählen beispielsweise die vertrauliche Weitergabe von Finanzdaten, die Kommunikation zwischen Vorstand und Aufsichtsrat oder die vertrauliche Weitergabe geistigen Eigentums. Solche Szenarien verlangen einen besonderen Schutz der Dokumente vor Missbrauch und Fehlhandlungen.

Unternehmen stehen damit in einem typischen Zielkonflikt zwischen der Sicherheit und Integrität der unternehmenskritischen Daten und deren schneller, reibungsloser Verteilung an alle, die innerhalb und außerhalb eines Unternehmens damit arbeiten sollen. Von der Lösung dieser widersprüchlichen Anforderungen hängt oft genug die Wett-

bewerbsfähigkeit eines Unternehmens ab. Denn je sicherer und effektiver die Bereitstellung und Bearbeitung von Dokumenten gelöst wird, desto schlagkräftiger kann das Unternehmen agieren beziehungsweise reagieren.

Anders formuliert bedeutet das: Sämtliche Sicherheitsmaßnahmen wie Zugriffskontrolle, Berechtigungen oder Verschlüsselung müssen für die gemeinsame Dokumentenbearbeitung im



„Je sensibler
Informationen sind,
umso stärker
ist die Tendenz
zu beobachten,
dass sie die
Unternehmensgrenzen
verlassen.“

Unternehmen und über seine Grenzen hinweg gemäß geltenden Compliance-Vorgaben organisiert und garantiert werden.

Hier gilt es, Anforderungen seitens der (technischen) Sicherheit, Compliance-Regularien sowie der Anwender zu berücksichtigen und bestmöglich zu integrieren.

Für den Umgang mit vertraulichen Dokumenten, in denen Wissen zu Papier gebracht wurde, das nicht für jedermann einsehbar sein darf, werden Lösungen erforderlich, die eine sichere Umgebung für die gemeinsame Bearbeitung und die regelkonforme Verwaltung sensibler Inhalte garantieren. Im Rahmen der Compliance werden Regeln für Vertraulichkeitsstufen festgelegt, die mit Lösungen für Document Compliance Management (DCM) auf das jeweilige Dokument angewandt und übertragen werden.

Durch eine hochsichere Verschlüsselung während der Datenübertragung und Ablage auf dem Server sowie die Abschirmung aller Dokumente vor unbefugtem Zugriff wird die Zusammenarbeit in ein hochsicheres Umfeld verlagert. Die Plattform für DCM bietet damit nur ausgewählten Adressaten über ein mehrstufiges Log-In-Verfahren den Zugang zu vertraulichen Dokumenten. Idealerweise stehen diese den Anwendern zu jeder Zeit und von jedem Ort aus webbasiert zur Verfügung. Gleichzeitig werden sämtliche Zugriffe und Veränderungen am Dokument revisionssicher protokolliert. Die Lösung erfordert keine Schulung der Mitarbeiter und gestaltet die Zusammenarbeit benutzerfreundlich, transparent und nachvollziehbar.

Der Protokollfunktion kommt dabei eine bedeutende Rolle zu, da im Falle der Aufarbeitung eines Geschäftsvorfalles durch die Staatsanwaltschaft oder bei Anfragen der Finanzkontrollbehörden lückenlose Abläufe, personalisierte Zugriffe, Änderungen et cetera oft sehr kurzfristig nachgewiesen werden müssen. Ebenfalls haften Aufsichtsräte auch nach dem Ausscheiden aus dem Amt noch weitere fünf Jahre für Beschlüsse ihrer Amtszeit. Insofern sollten auch sie die Möglichkeit bekommen, Dokumente nachträglich einsehen und Abläufe nachweisen zu können.

NICOLE DIETRICH

WEB-TIPP:

www.brainloop.de