

Compliance: Legal überwacht es sich nachhaltiger

Wissensmanagement-Anwendungen werden vermehrt mit Compliance-Lösungen verknüpft. So erleichtert die automatisierte Überwachung von E-Mails die Arbeit der Verantwortlichen. Eine segensreiche Entwicklung – wenn die Lösungen dem Datenschutz entsprechen. *Hans Fischer*



Hans Fischer

ist bei der Bieler Rolotec AG in den Bereichen Business Development, Marketing und Kommunikation mit Fokus auf Wissensmanagement, Beratung und Börseninformation tätig

Die Credit Suisse schreibt zum Thema Compliance: «Die Massnahmen zur Umsetzung beginnen mit der Personalauswahl und führen über Schulung, detaillierte Prozesse und Regeln bis hin zu wirkungsvollen Aufsichts- und Kontrollsystemen.» So und ähnlich klingt es bei den meisten Finanzdienstleistungsunternehmen. Die Einhaltung aller gesetzlichen, regulatorischen und bankinternen Vorschriften ist Pflicht. «Die Banken müssen über eine funktionierende Organisation verfügen», hält Tanja Kocher, Leiterin Kommunikation/Medien bei der Eidgenössischen Bankenkommision (EBK), auf Anfrage die Essenz fest.

Selbstredend, dass versucht wird, die genannten Aufsichts- und Kontrollaufgaben weitgehend zu automatisieren. Ein Beispiel: E-Mail oder Instant Messaging werden in Echtzeit überwacht. Die Alarmierung geschieht unmittelbar. So erhalten Mitarbeiter vor dem definitiven Versenden einer E-Mail eine Warnung, wenn Teile des Inhaltes gegen interne oder externe Verordnungen verstossen würden (oder könnten). Wahlweise könnten solcherlei Inhalte auch an Compliance-Verantwortliche weitergeleitet werden. Automatismen wie diese reduzieren die manuellen Tätigkeiten der Compliance-Abteilungen, sparen entsprechend Geld und erhöhen die Sicherheit.

Auf Kollisionskurs mit dem Datenschutz

In keiner anderen Branche scheinen solche Automatismen ähnlich notwendig oder sinnvoll wie in der Finanzbranche. Warum entsprechende Softwarelösungen noch nicht flächendeckend eingesetzt werden, hängt unter anderem mit der Rechtslage zusammen. Hanspeter Thür, Eidgenössischer Datenschutzbeauftragter, erklärt auf Anfrage, dass die Zunahme des Einsatzes von Überwachungssoftware feststellbar sei. «Erst jüngst habe ich einen Artikel gelesen, der die An-

wendung von automatisierter Compliance-Software als ganz selbstverständlich dargestellt hat», so Thür. Der Einsatz bedürfe demgegenüber aber sorgfältiger Planung und Einhaltung der Datenschutzrichtlinien. So sei E-Mail-Überwachung nicht ohne weiteres möglich, wenn die Unternehmen den Einsatz der geschäftlichen E-Mail-Adressen für private Inhalte und Zwecke erlauben.

Wenn im Unternehmen keine entsprechenden Bestimmungen erlassen würden – von Vorteil in Form schriftlicher Benutzerreglemente, die auch die Voraussetzungen möglicher Überwachung regeln – dürften die Mitarbeiter davon ausgehen, dass die private Nutzung der E-Mail-Accounts in vernünftigen Rahmen erlaubt sei. Entsprechend wären die Überwachungsmöglichkeiten stark eingeschränkt respektive in legalem Rahmen kaum möglich. Detaillierte Informationen sind auf der Site des Eidgenössischen Datenschutzbeauftragten (www.edoeb.admin.ch) zu finden.

Grundsätzlich gilt: Software, die nicht nur eine Filterung nach bestimmten Stichworten, sondern eine umfangreiche Analyse des E-Mail-Verkehrs ermöglicht (sog. Spionprogramme), ist illegal, weil sie gegen das arbeitsrechtliche Verhaltensüberwachungsverbot verstösst. Filterprogramme hingegen können aus der Sicht des Persönlichkeitsschutzes akzeptiert werden, wenn sie aus den E-Mail-Inhalten lediglich bestimmte Auffälligkeiten festhalten. Die in pseudonymer Art und Weise festgehaltenen Auffälligkeiten können dann personenbezogen ausgewertet werden. Grundlage der automatisierten Compliance ist folglich eine strikte Regelung der Verwendung von Kommunikationsmitteln durch die Mitarbeiter und deren Überwachung. «Werden dabei Straftatbestände festgestellt oder entstehen entsprechende konkrete Verdachtsmomente, ist ohnehin eine Strafverfolgung anzustrengen», hält der Datenschutzbeauftragte fest.

Anforderungen werden umfangreicher

Trotz des engen rechtlichen Korsetts bestätigt der freie Autor Thomas Schumacher im Artikel «Herausforderung Basel II und Sarbanes-Oxley – Compliance und Transparenz sind machbar» die zunehmende Bedeutung automatisierter Lösungen. Im Schlussabsatz hält er fest: «Egal ob es um Kreditvergabe an ein Unternehmen oder Bilanzierungsrichtlinien geht, die gesetzlichen Vorgaben und Rating-Anforderungen werden umfangreicher und immer strenger. Neben Basel II und Sarbanes Oxley müssen sich Unternehmen,

Wissensmanagement

Unternehmen, die Daten, Informationen und Wissen nicht bewirtschaften, verlieren täglich sehr viel Geld. Die Hauptübel sind lange Suchzeiten, Nicht-Finden und Dubletten-Produktion. Wer die Kosten hochrechnet, wenn betroffene Mitarbeiter täglich lediglich 30 Minuten wegen ineffizienter Suche oder Mehrfach-Produktion verlieren, kommt auf stolze Summen. In der Realität sind diese verschleuderten Gelder wahrscheinlich noch deutlich umfangreicher. KPMG hat analysiert, dass über 60 Prozent der Mitarbeiter eine Stunde pro Tag allein durch das Wiederholen längst getaner Arbeit ihrer Kollegen verschwenden. Dazu kommen noch lange Suchzeiten oder Wissensverlust durch Personalwechsel. Kurz: Den individuellen Gegebenheiten angepasste Such- und Wissensmanagement-Lösungen sind ein Muss.

Für jede Organisation und jedes Budget gibt es passende Lösungen. Reicht Suchen und Finden aus, werden Anwendungen für wenige tausend Franken angeboten. Bei mittleren und vor allem bei grösseren Organisationen kommt die Verknüpfung von Informationen mit sozialen Netzwerken dazu. Das Wissen soll zur richtigen Zeit, am richtigen Ort zur Verfügung gestellt werden. Je besser das Wissenskapital gepflegt wird, desto grösser sind die Wertschöpfung und die Unabhängigkeit gegenüber Know-how und Netzwerk von Einzelpersonen. Eine umfassende Wissensmanagement-Lösung betrifft in der Regel mehrere Managementbereiche und bedarf intensiver Abklärungen. Unternehmensstruktur und -kultur müssen für die Massschneidung der Lösung berücksichtigt werden.



Das Datenschutzgesetz ist eindeutig: Ohne entsprechende Bestimmungen dürfen Mitarbeiter davon ausgehen, dass die private Nutzung der dienstlichen E-Mail-Accounts in vernünftigem Rahmen erlaubt ist und unüberwacht bleibt.

je nach Branche, bereits heute mit Themen wie Solvency II, GAAP und IAS beschäftigen. Und eines ist bereits jetzt gewiss, die Anforderungen werden eher umfangreicher als geringer werden. Letztlich geht es bei Compliance darum, dass ein CFO auf Knopfdruck die aktuellen Daten auf seinem PC in ausgewerteter Form präsentiert bekommt und somit die Einhaltung aller Vorschriften nachweisen kann.»

Optimalen Return on Investment bringen Software-Installationen, die gleichzeitig Wissens- und Informationsmanagement sowie automatisierte Compliance-Überwachung ermöglichen – und Schnittstellen zu weiteren Business-Intelligence-Anwendungen bieten. Weltmarktführer sind das norwegische Unternehmen FAST und der englische Mitbewerber Autonomy. Auf Anfrage erklärt FAST-CEO John M. Lervik, dass sein Unternehmen eine breite Palette an Compliance Monitoring anbiete. Die Lösungen erlaubten die fallweise angepasste Rücksichtnahme auf betriebli-

che Vorgaben und auf gesetzliche Rahmenbedingungen verschiedenster Ausprägung. «Das ist absolut unabdingbar», hält Lervik fest. Entsprechende Referenzen wie von der Börse Oslo oder Goldman Sachs bestätigen dies. Mitbewerber Aungate, eine Tochtergesellschaft von Autonomy, führt auf der Webseite unter anderem Kunden wie die US-Börsenaufsicht SEC auf. Selbstredend, dass die Einhaltung gesetzlicher Bestimmungen eine Selbstverständlichkeit ist.

Klar ist: Mit illegalen Spionprogrammen haben solcherlei Lösungen nichts gemein. ■

Quellen

- Eidgenössischer Datenschutzbeauftragter: www.edoeb.admin.ch
- Thomas Schumacher: «Herausforderung Basel II und Sarbanes-Oxley – Compliance und Transparenz sind machbar»: www.competence-site.de