

Auf Nummer sicher gehen

In deutschen Unternehmen besteht in puncto Compliance Nachholbedarf

Verstoßen US-Manager gegen den Sarbanes Oxley Act (SOX), müssen sie mit einer

Gefängnisstrafe von bis zu 20 Jahren rechnen. Ihre europäischen Kollegen lehnen sich noch gemächlich zurück – mit möglicherweise unangenehmen Folgen, denn auch in Europa wurden vergleichbare Vorgaben beschlossen. Pharma und Chemische Industrie sind durch eine Vielzahl spezifischer Regularien hier in besonderem Maße angesprochen. Mit Hilfe von „Compliance-Assessments“ können Verantwortliche jetzt prüfen, wo Handlungsbedarf besteht.

Unternehmen der Pharma-Industrie wissen, dass die Entscheidungen der Food and Drug Administration (FDA) bei Nicht-Einhaltung von Regularien drastische Folgen haben. Jetzt ist auch in Europa das Regelwerk enger geworden. Die so genannte Euro-SOX, 8. EU-Richtlinie und EU-Abschlussprüfer-Richtlinie, gilt seit Juli. Im Februar dieses Jahres wurde „Moreq2“, eine Spezifikation für elektronisches Dokumenten- und Records-Management, veröffentlicht. Für die Einhaltung dieser und vieler weiterer Einzelregelungen, etwa für den Finanzbereich oder zur Archivierung von E-Mails, sind Vorstände und Geschäftsführer

verantwortlich und persönlich, gesamtschuldnerisch haftbar. Sie sind verpflichtet, ein wirksames Risikosystem einzuführen, die Funktionsweise der IT nachvollziehbar zu dokumentieren und für eine angemessene Archivierung digitaler Dokumente zu sorgen.

Viele Unternehmen sind nicht „compliant“

Umfragen zeigen, dass die meisten Unternehmen derzeit nicht auf die Anforderungen der EU-Richtlinie vorbereitet sind. Das große Problem: Unternehmensverantwortliche können kaum noch beurteilen, welche Maßnahmen aus der Fülle der Regelungen zwingend umzusetzen sind und was wirtschaftlich angemessen ist: Welche Gesetze sind für unser Unternehmen relevant, welche erfüllen wir bereits (Rechtsfrage)? Welche Prozesse und Systeme sind betroffen, und wie setzen wir die Bestimmungen um? (Frage interner Prozesse und IT-Systeme)? Wie wahrscheinlich ist ein Schadenfall und mit welchen Auswirkungen ist zu rechnen? Lohnt es sich, dafür Vorkehrungen zu treffen (betriebswirtschaftliche Fragen)? Dr. Renate Mayer vom Enterprise-Contentmanagement-Spezialisten FME AG rät dringend dazu, die juristischen, betriebswirtschaftlichen und IT-technischen Fragen gleichrangig zu

behandeln und alle Experten in ein gemeinsames Team zu holen. Die fme-Experten lassen sich deshalb durch eine auf IT-Recht spezialisierte Rechtsanwaltskanzlei unterstützen. In einem „Compliance-Assessment“ soll Klarheit geschaffen werden, indem Schwachstellen im Unternehmen aufgezeigt, die notwendigen Änderungen definiert und betriebswirtschaftlich bewertet werden. Erst auf dieser Grundlage könne ein angemessener Maßnahmenplan erstellt und mögliche Anpassungen der IT-Systeme eingeleitet werden. Auf Unternehmensseite sollten neben der Unternehmensleitung auch das Rechnungswesen, die IT, der Datenschutzbeauftragte, die Revision und gegebenenfalls der Chief Compliance Officer mit im Team sein.

Betroffene Gesetze und Normen feststellen

Im ersten Schritt gilt es zu klären, welche Regularien für das Unternehmen aktuell und relevant sind und welche internen Regelungen und Arbeitsanweisungen bereits existieren. Dr. R. Mayer: „Wir stellen immer wieder fest, dass es angesichts der vielen neuen Regelungen einen erheblichen Nachholbedarf gibt. Zum Beispiel wird die Archivierung von E-Mails fälschlicherweise oft auf die Frage des geeigneten IT-Systems reduziert oder

es werden neue Entwicklungen, wie die Produkthaftung in der Fertigungsindustrie, nicht ernst genug genommen.“ Das „Compliance-Team“ erfasst außerdem, ob sich verschiedene Compliance-Felder überlappen, wie Anforderungen an das Risk-Management (ISO 9000), Corporate Governance (SOX), spezifische Regularien wie 21CFRPart11 (Pharma), Datenschutzgesetz, Telekommunikationsgesetz, Handelsgesetzbuch, Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU).

Handlungsbedarf definieren

Im zweiten Schritt werden die betroffenen Prozesse und Systeme identifiziert. Dazu gehört die installierte Hard- und Software, die Zugriffs- und Berechtigungsregelungen usw. Beispielsweise im Rechnungswesen gehören etwa die Prozesse des Rechnungseingangs und -ausgangs dazu, das ERP-System und schließlich alle Abläufe bis zum verwendeten Archivsystem. In Branchen wie der Pharmaindustrie sind für die Zulassung von Präparaten und Arzneimittel umfangreiche Auflagen zu erfüllen. Die Erfüllung dieser Auflagen muss gut dokumentiert werden. Eine Zulassung kann scheitern, wenn etwa nicht nachweisbar ist, dass die Mitarbeiter alle relevanten Arbeitsanweisungen kennen und

das per Unterschrift dokumentiert haben.

Durch den Abgleich der vorhandenen Systeme und Prozesse mit den geltenden Gesetzen und Regeln werden im dritten Schritt Lücken und Risiken in der Unternehmenspraxis identifiziert. Daraus wird ersichtlich, wo Handlungsbedarf besteht. Am Beispiel der E-Mail-Archivierung zeigt sich, dass dies recht komplex sein kann. Zum einen müssen die relevanten E-Mails z.B. gemäß Gewährleistungsrecht ordnungsgemäß archiviert werden, um Risiken aus der Produkthaftung gerecht zu werden. Zum anderen ist sicher zu stellen, dass bei der Archivierung keine Rechte aus dem Datenschutz verletzt werden, weil private E-Mails betroffen sind. Werden Regelverstöße festgestellt, müssen zunächst die Ursachen ermittelt werden, bevor an Maßnahmen zur Risikominimierung zu denken ist. Allerdings muss nicht jede Verletzung von Regeln und Normen zwangsläufig weitere Maßnahmen zur Folge haben. Ausgehende elektronische Rechnungen bedürfen beispielsweise einer qualifizierten elektronischen Signatur. Ein Unternehmen muss abwägen, wie schwerwiegend die Nachteile aus der Regelverletzung (Rechnungen ohne Signatur) im Vergleich zum notwendigen Aufwand sind, die Regel einzuhalten (Signaturen durchzuführen).

Erkenntnisse umsetzen

Sind die Mängel festgestellt und das Risiko bewertet, gilt es im nächsten Schritt, die geeigneten Maßnahmen auszuwählen. Das Team entwickelt auf der

Basis von Best-Practise-Erfahrungen Empfehlungen für organisatorische Maßnahmen und für die Verbesserung der eingesetzten IT-Systeme. Zu unterscheiden sind organisatorische und technische Maßnahmen. Reicht die Anpassung der Policy oder sind Änderungen bei der Technik notwendig? Typische Empfehlungen betreffen die Einrichtung von Frühwarnsystemen, Ausfallszenarien oder die Anpassung bestehender Arbeitsprozesse. Das Ziel ist möglichst eine integrierte Lösung über alle Compliance-Felder für Governance, Risk and Compliance (GRC). Dr. R. Mayer: „Wir können viel gewinnen, wenn wir das Notwendige mit dem Nützlichen verbinden. Wenn wir IT-Systeme oder organisatorische Abläufe ohnehin anpassen müssen, ist dies eine große Chance, auch gleichzeitig die Effizienz dieser Prozesse zu verbessern.“ Nach den Erfahrungen der fme AG sind erhebliche Einsparungen erzielbar, wenn über Jahre gewachsene Abläufe einfacher und schneller werden oder produktivere IT-Systeme eingesetzt werden.

Die Praxis zeigt: Handlungsbedarf besteht in vielen Unternehmen. Die meisten Bestimmungen der Euro-SOX gab es bereits vorher in ähnlicher Form. Die neue Richtlinie hat allerdings die Aufmerksamkeit auf seit Jahren bestehende Defizite in den Unternehmen gelenkt.

Kontakt:
FME AG, Braunschweig
Tel: 0531 2 38 54-0
Fax: 0531 2 38 54-70
info@fme.de
Internet: www.fme.de

