iX extra

Security

Compliance und Sicherheitsmanagement

Veranstaltungen

5. – 7. März 2013, Hannover
CeBIT
www.cebit.de

22. – 23. März 2013, Heidelberg
iX-Workshop: Metasploit – Das Penetration-Testing-Framework
www.ix-konferenz.de

23. – 25. April 2013, London
Infosecurity Europe
www.infosec.co.uk

14. – 16. Mai 2013, Bonn
BSI: 13. Deutscher IT-Sicherheitskongress
www.bsi.de

iX extra Security zum Nachschlagen:
www.heise.de/ix/extra/security.shtml

Security

Sich wappnen gegen Verstöße

Gesetzliche Vorgaben koordinieren

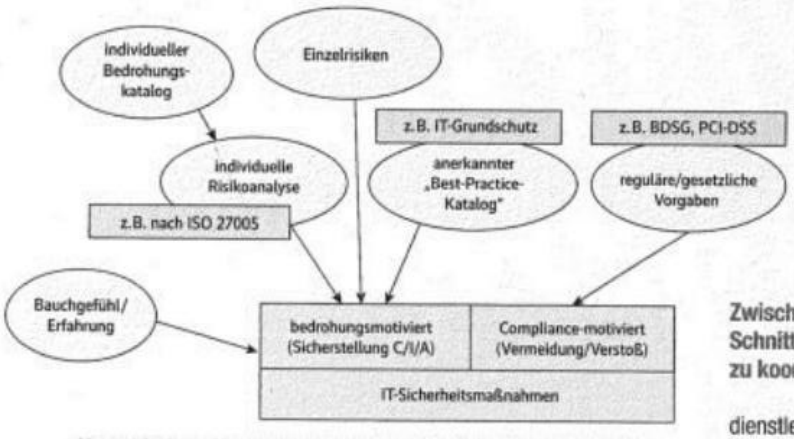
Compliance muss häufig als eines der wichtigsten Argumente für die Anschaffung eines Sicherheitsprodukts herhalten. Da in der Regel alle Bereiche eines Unternehmens von Vorgaben aus Gesetzen und sonstigen Quellen betroffen sind, wird das Compliance-Management meist als Querschnittdisziplin ausgelegt und muss sehr unterschiedliche Aspekte abdecken.

Compliance hat sich zu einem beliebten Marketingbegriff in der IT-Sicherheitsbranche entwickelt, lässt sich damit doch prima um Aufmerksamkeit buhlen. Im Unternehmensumfeld bezeichnet sie in erster Linie die Einhaltung der geltenden gesetzlichen, behördlichen, vertraglichen oder sonstigen relevanten externen Vorgaben. Ziel ist es, Verstöße und damit Strafen zu vermeiden. Im weiteren Sinne bedeutet Compliance aber auch die Einhaltung interner Richtlinien, die sich das Unternehmen selbst auferlegt.

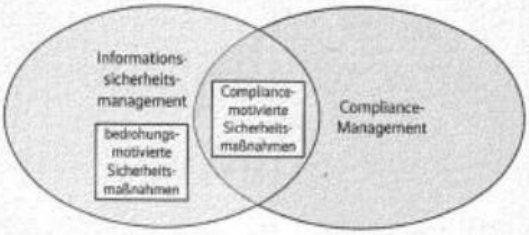
Mit einem strukturierten Compliance-Management möchte ein Unternehmen Verstöße vermeiden beziehungsweise sicherstellen, dass eingetretene Verstöße erkannt, geeignet behandelt und Wiederholungen künftig vermieden werden. Da in der Regel alle Bereiche eines Unternehmens von verschiedenen Vorgaben betroffen sind, legt man das Compliance-Management meist als Querschnittdisziplin aus. Das Identifizieren und Sicherstellen der Einhaltung von Anforderungen mit Bezug zur IT- und Informationssicherheit ist somit nur ein Teilaspekt des gesamten Compliance-Managements.

Betrachtet man den Aspekt Compliance aus dem Blickwinkel eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001, ist das Ermitteln und Berücksichtigen gesetzlicher und regulatorischer Anforderungen, die die Sicherheit von Informationen und der informationsverarbeitenden Systeme gewährleisten, explizit Bestandteil des Standards. Auch der BSI-Standard 100-2, der die IT-Grundschutzvorgehensweise beschreibt, sieht ausdrücklich die Ermittlung der gesetzlichen Rahmenbedingungen mit Auswirkung auf die Informationssicherheit vor und empfiehlt bei der Schutzbedarfsermittlung auch die Betrachtung von Schadensszenarien, die aus einem Verstoß gegen Gesetze et cetera resultieren können.

Für die innerhalb eines ISMS zu ermittelten Maßnahmen zur IT- und Informationssicherheit bedeutet dies in der Konsequenz, dass es nicht genügt, Sicherheitsmaßnahmen äusschließlich risikoorientiert herzuleiten aus „herkömmlichen" Bedrohungen, die die Verfügbarkeit, Vertraulichkeit und Integrität von Informationen beziehungsweise informationsverarbeitenden Systemen gefährden.



Verschiedene Vorgaben dienen als Auslöser für Sicherheitsmaßnahmen in Unternehmen (Abb. 1).



Zwischen Sicherheits- und Compliance-Management gibt es eine Schnittmenge. Die Kunst besteht darin, die Maßnahmen für beides zu koordinieren und das passende Werkzeug zu finden (Abb. 2).

Zusätzlich ist es eben auch erforderlich, die gesetzlichen, regulatorischen und sonstigen externen Anforderungen zu kennen und die daraus gegebenenfalls resultierenden Sicherheitsmaßnahmen einzuleiten, selbst wenn die herkömmliche Bedrohungs- und Risikoanalyse diese Maßnahme möglicherweise nicht naheliegend erscheinen lässt.

In der Praxis kommt der zuletzt genannte Bereich leider häufig zu kurz. Oft existiert innerhalb des ISMS nicht einmal die Möglichkeit, die relevanten gesetzlichen und regulatorischen Anforderungen mit Bezug zur Informationssicherheit nachvollziehbar zu ermitteln. Die Praxiserfahrung zeigt, dass hier in vielen Unternehmen Nachholbedarf vorhanden ist.

Relevante Regelwerke

Beispiele für gesetzliche, regulatorische oder sonstige externe Anforderungen mit unmittelbarem Bezug zur IT- und Informationssicherheit sind das Bundesdatenschutzgesetz (BDSG), die Mindestanforderungen an das Risikomanagement der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) für Unternehmen im Umfeld von Finanzdienstleistungen oder der Payment Card Industry Data Security Standard (PCI-DSS) für Unternehmen, die Kreditkartentransaktionen abwickeln. Letzterer fordert beispielsweise ganz konkret die Anwendung einer Zweifaktor-Authentifizierung bei Remote-Access-Zugriffen ins Unternehmensnetzwerk.

Die inhaltliche Überlappung des meist interdisziplinär ausgeprägten Compliance-Managementsystems im Unternehmen mit dem Informationssicherheits-Managementsystem muss sich zwangsläufig in der organisatorischen Ausprägung der Managementsysteme niederschlagen. Beispielsweise müssen die Schnittstellen zwischen dem ISMS und dem Compliance-Managementsystem klar definiert sein, und die Verantwortlichkeiten und Zuständigkeiten des Compliance Officers und des Information Security Officers müssen sauber abgegrenzt werden. Auch wenn es um die Auswahl eines unterstützenden Werkzeugs für das Compliance- und Sicherheitsmanagement geht, sollte man sich der Überlappungen bewusst sein. Das bedeutet, für beide Managementsysteme muss man ein gemeinsames Werkzeug auswählen und in den Auswahlprozess somit auch alle Seiten einbeziehen. (ur/sf)

Steffen Gundel ist Leitender Berater bei der cirosec GmbH.