Empfehlungen und Normen im Bereich der IT-Sicherheit

Die IT-Sicherheit ist zu einem ständigen Thema geworden. Die Meinungen, wie etwas umzusetzen ist, gehen jedoch weit auseinander. Normen und Empfehlungen sollen helfen, im Dschungel der Möglichkeiten einen Wegweiser zu geben. Doch welche Norm ist denn nun die richtige? Dieser Artikel soll aufzeigen, welche Normen existieren und wie diese anzuwenden sind.

Andreas Wisler

Als wichtigste Norm in Europa für das Management von Informationssicherheit ist die ISO Norm 27001, welche aus dem Code of Practice (COP) hervorgegangen ist. Der Grundschutz in der IT wird oft auf Basis der BSI-IT-Grundschutz-Kataloge erstellt. Sobald eine Firma Waren in die USA liefert, werden Zertifikate nach Common Criteria gefordert. Gleichzeitig gilt natürlich immer auch das Datenschutzgesetz, sobald personenbezogene Daten bearbeitet werden.

InfoSurance: 10-Punkte-Programm

Im schweizerischen Verein InfoSurance arbeiten Experten aus verschiedenen Branchen zusammen, um die KMU mit einfachen Verfahren und Werkzeugen zur Steigerung der Informationssicherheit zu unterstützen. Eines der Produkte ist das 10-Punkte-Programm. Dieses ist mit folgendem Link herunter zu laden: www.infosurance.ch Button Dienstleistungen.

Grundschutz nach BSI

Das Deutsche Bundesamt für Sicherheit in der Informationstechnik stellt umfangreiche Informationen kostenlos zur Verfügung. Die IT-Grundschutz-Kataloge hiessen früher Grundschutzhandbuch. Darin ist definiert, welche Schutzmassnahmen für ein entsprechendes System zu treffen sind. Zusätzlich gibt es BSI-Standards zur IT-Sicherheit, mit dem Untertitel «Bereich IT-Sicherheitsmanagement». Dieser Teil deckt nun auch den Managementteil und das Erstellen von Risikoanalysen ab. Mit diesen Anpassungen sind die Unterlagen von BSI kompatibel zur ISO 27001 Zertifizierung. Infos sind unter www.bsi.de/gshb/ zu finden.

Dipl.-Ing. FH, CISSP, Andreas Wisler, Geschäftsführer, GO OUT Production GmbH, Schulstrasse 11, CH-8542 Wiesendangen, Telefon +41 (0)52 320 91 20, info@goout.ch, www.goout.ch

ISO 17799/ISO 27001

Aus dem ehemaligen British Standard 7799-2:1998, auch Standard für «Anforderungen an ein Informations-Sicherheits-Managementsystem», wurde der Standard ISO 27001:2005. Danach können sich Betriebe heute zertifizieren lassen. Aus dem ehemaligen «Code of Practice for Information Security Management« wurde im April 2007 «ISO/IEC 27002». Darin sind über 100 übergeordnete Sicherheitsanforderungen enthalten, plus 600 bis 800 Massnahmenpakete zu deren Umsetzung. Für KMU wird hieraus vor allem der Standard ISO/IEC 27005 von Interesse sein, weil dieser hilft, ein effektives Risk-Management zu realisieren. Weitere Infos sind zu finden: www.27000.org

ITIL

ITIL ist eine herstellerunabhängige Sammlung von Best Practices, mit denen es IT-Organisationen über einen prozessorientierten, skalierbaren Ansatz ermöglicht wird, Effizienzsteigerungen innerhalb ihrer IT-Prozesse zu erzielen. ITIL steht als Abkürzung für «Information Technology Infrastructure Library».

ITIL bietet die Grundlage zur Verbesserung von Einsatz und Wirkung einer operationell eingesetzten IT-Infrastruktur. Folgende Seiten bieten weitere Details zu diesem beliebten Standard: www.itil.org/de oder www.itil.org.uk

CObIT

Das CObIT-Modell (Control Objectives for Information and related Technology) wurde von Revisoren aus der Industrie und dem Berufsstand (ISACA – Information Systems and Control Association) auf Basis von bestehenden Revisionsrichtlinien, Kontrollmodellen und branchenspezifischen Regularien und Richtlinien entwickelt. Bei der Entwicklung von CObIT galt es, dem Anspruch eines IT-spezifischen Kontrollsystems gerecht zu werden, welches in optimaler Weise die bestehenden wie auch die zukünftigen Geschäftsprozesse unterstützt. Details: www.isaca.org/cobit

PRINCE2

PRINCE steht für PRojects IN Controlled Environments und wurde 1989 erstmals der CCTA – Central Computer and Telecommunications Agency – als der Standard der britischen Regierung für IT-Projektmanagement ins Leben gerufen. Durch ständige Weiterentwicklung wurde daraus ein generischer Ansatz zur Steuerung, Organisation und zum Management von Projekten jeglicher Art und Grösse. Mehr dazu unter: www.prince2.ch oder www.prince2.com

Literatur-Tipp
Anhand von Beispielen und Checklisten zeigen die Autoren die Eckpunkte für ein modernes Sicherheitskonzept, Schritt für Schritt, einfach auf den Punkt gebracht. Übersichten, Checklisten und Praxistipps machen aus diesem Booklet eine wertvolle Informationsquelle und ein übersichtliches Nachschlagewerk.
Informationssicherheit für KMU. Fredy Schwyter und Andreas Wisler, BPX-Edition 2007. ISBN 978-3-905413-72-4
CHF 30.–/Euro 20,–, www.bpx.ch

BSI 15000/ISO 20000

BSI 15000 wurde vom British Standard Institute (BSI) entwickelt und ist der erste weltweite Standard für IT-Service-Management. Dieser Standard beschreibt einen integrierten Satz von Management-Prozessen für die Lieferung von Dienstleistungen zwischen internen und externen Organisationen im Rahmen des IT-Service-Managements. BSI 15000 ist ausgerichtet auf die Prozessbeschreibungen von ITIL und ergänzt diese komplementär. Der britische Standard wird derzeit in die ISO 20000 eingearbeitet. Bei Interesse besuchen Sie die folgenden Seiten: www.iso20000.ch/ oder www.bs15000.org.uk/

Welche Norm für welches Unternehmen nun die richtige ist, kann nicht ohne weiteres und abschliessend beantwortet werden, zu verschieden sind die Anforderungen und Umsetzungsmöglichkeiten. Die IT-Grundschutz-Kataloge des BSI bieten jedoch einen guten Startpunkt, um die technischen Anforderungen anzupacken. Für eine umfassende Beschreibung von IT-Prozesse eignet sich ITIL sehr gut. Der Umgang mit Risiken kann optimal nach dem ISO 27005 Standard angepackt werden.

Hinweis: Kein Übereifer!

Stürzen Sie sich nicht auf alle Standards. Gehen Sie diese Schrittweise an. Planen Sie für die Vorbereitungen, die Konzeptphase, wie auch für die Umsetzung genügend Zeit ein. Oft lohnt es sich auch, einen externen Partner bei zu ziehen, welcher bereits Erfahrungen mit diesen Normen hat.

Dies kann Geld, Zeit und Nerven sparen und hilft, von Beginn weg einen optimalen Weg einzuschlagen.