

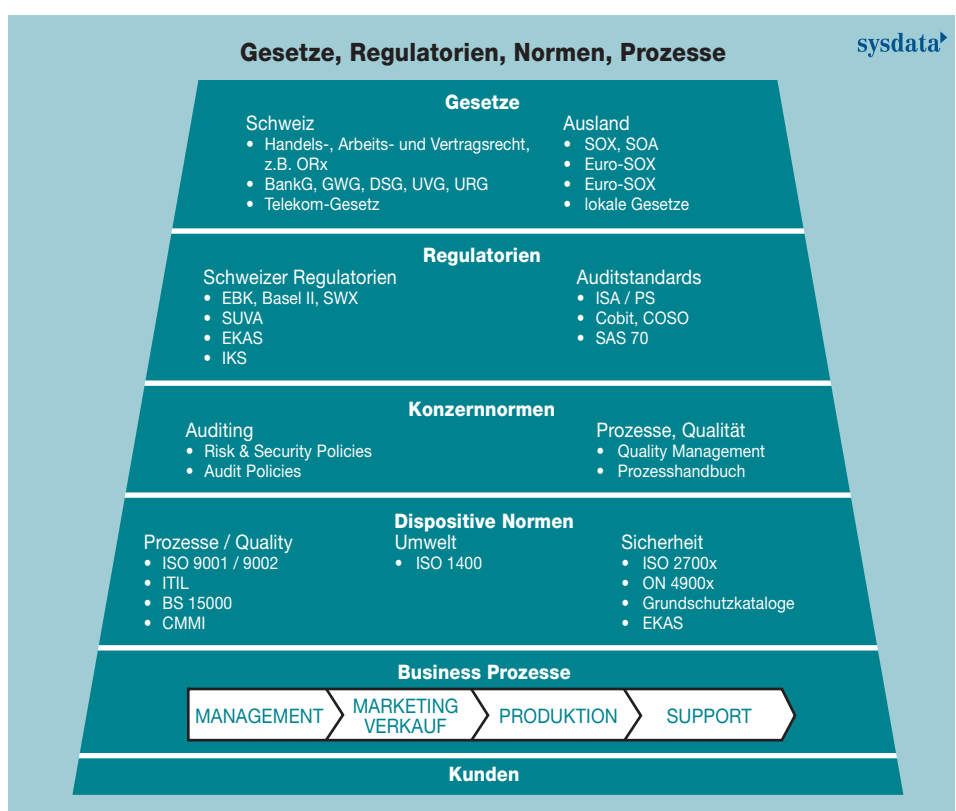
# Sicherheitsstrategie spart Geld

Eine Sicherheitsstrategie ist nur dann wirksam, wenn sie auch lebbar ist. Diese Idee fordert uns, im Spannungsfeld von Kostendruck und Image-Schaden nur praktische und machbare Sicherheit «zu bauen».

Marco Marchesi, CEO und Inhaber ISPIN AG

Die verschiedenen Unternehmensprozesse reichen tief in die Unternehmens-Substanz hinein. Deshalb **zielt die Informationssicherheit darauf ab, diese Prozesse sicher zu machen**. Die Strategie mit Sicherheitskonzept und Sicherheitsmassnahmen unterstützt die Unternehmensziele. Verknüpfungen zu Mensch und Umwelt sind dabei genauso wichtig wie das Einhalten der Gesetze und Vorschriften. Die Perspektiven einer Sicherheitsstrategie (bzw. eines Security-Frameworks) sind dann vielversprechend, wenn die Bereiche Mensch, Organisation, Technik und Gesetz gleichermaßen berücksichtigt sind. Die Frage ist, ob man in der Entwicklung eines Frameworks «from Scratch» oder nach Standard vorgeht.

Zunächst gilt es aber zu prüfen, welche Standards und Regulatorien für das Unternehmen von Bedeutung sind. Je mehr Regulatorien Firmen berücksichtigen müssen, umso höher die Komplexität und umso höher die Anforderung an das geplante Sicherheits-Management-System. Echt herausfordernd wird diese Aufgabe, wenn das Unternehmen europaweit oder gar weltweit verteilte Standorte zu betreuen hat. Das Management-System muss so aufgebaut sein, dass ein Zusammenführen der einzelnen Standorte als Divisionen, Geschäftsbereiche oder Kontinente einfach möglich ist. So fordert beispielsweise die Section 404 aus dem SOX (Bundsgesetz zur Veröffentlichung der Finanzdaten) vom Management, ein anerkanntes und etabliertes Framework für



Unternehmen müssen hinsichtlich IT-Sicherheit diverse Gesetze, Regulatorien und Normen befolgen

interne Kontrollen einzusetzen. **Das Ziel ist mehr Transparenz.** Das Reporting muss zeigen, was effektiv vorhanden ist und was gelebt wird. So wird ein erster Sicherheitsfilter eingebaut.

Basel II (Eigenkapitalvorschriften) wiederum fokussiert auf der Erhöhung der Risikosensibilisierung und der Verbesserung des Risikomanagements. Für die Informationssicherheit ist dabei der Teil «Operational-Risk-Management» wesentlich. Auch hier ergeht die Forde-

rung, dass der Verwaltungsrat über die wichtigen operationellen Risiken des Unternehmens im Bild sein muss. Er soll zudem sicherstellen, dass ein effektives und umfassendes Framework für interne Audits vorhanden ist und dass diese kompetente Personen ausführen. Zum risikogerechten Managen der Sicherheitsmassnahmen wird ein prozessorientiertes Informations-Management-System (ISMS) nach ISO 27001 eingesetzt. Es stellt die Steuermethodik zum

Framework dar. Ein prozessorientierter Ansatz ermutigt die User, die Wichtigkeit folgender Faktoren zu betonen:

- Verständnis der geschäftlichen Anforderungen an IT-Sicherheit schaffen
- Ziele für IT-Sicherheit etablieren
- Kontrollen im Kontext des übergeordneten geschäftlichen Risikomanagements implementieren und betreiben
- Leistung und Effektivität des ISMS überwachen
- Fortlaufende Verbesserung auf der Basis objektiver Messungen

Die Aufnahme eines ISMS in die Organisation muss eine strategische Entscheidung sein. **Geschäftliche Anforderungen und Ziele bestimmen das Design und die Implementierung** in die Organisation ebenso wie daraus resultierende Sicherheitsanforderungen. Eine Sicht



**Informationssicherheit bedarf der Beachtung aller Unternehmensstufen**

aufs Ganze aus verschiedenen Perspektiven der Informations- und Informatik-sicherheit ist also angebracht. Die Komplexität des Unternehmens wird so automatisch im ISMS gespiegelt. Die Norm unterstützt die Verwendung eines prozessorientierten Ansatzes für Einführung, Implementierung, Betrieb, Überwachung, Wartung und Verbesserung der Effektivität des ISMS.

Die Strategie, die aus der Umsetzung nach ISO 27001 resultiert, muss in der Informations- und IT-Sicherheitspolitik (dem «Warum») und den Functional Policies (dem «Was») klar ersichtlich sein. Die Integration ins bestehende Prozessmodell ist durch Zuweisung klarer Aktivitäten bzw. Prozessschritte («Wie») zu gewährleisten. Mit der Strukturierung des ISMS nach Themen und Prozessen, welche die Abhängigkeit, aber auch Synergien aufzeigen, wird das ISMS nachhaltig lebbar.

Ein ISMS ist nach solchen Themen strukturiert und bildet im Schichtenmodell die Informations- und IT-Sicherheitspolitik bis hin zu BCM und Compliance ab. **Der Vorteil dieser Strukturierung ist** die Eliminierung von Redundanzen und Inkonsistenzen, die zwischen mehreren Dokumenten auf Detailebenen auftreten können. Der Anwender findet sich mit dieser Angleichung der sicherheitsrelevanten Themen (Disziplinen) an die Prozessstruktur des Security-Managements wesentlich einfacher zurecht, womit die Grundlage für die effiziente Entwicklung und

Umsetzung von Informationssicherheit für alle Betroffenen gesetzt wird.

Wer auch die Unternehmensprozesse ausführt, die Firewall administriert und Träger von Unternehmensinformationen ist: Erst der Mensch schafft die Informationssicherheit. Denn die Menschen sind es, die die Informationssicherheit in ihre tägliche Arbeit einbauen und umsetzen. Umgekehrt muss das Management alles daran setzen, dass die Informationssicherheit auch

tatsächlich in die tägliche Arbeit einfließen kann. **Eine weitere Schlussfolgerung daraus:** Die Verknüpfung von Kontrollen und täglich umgesetzten

Prozessen muss gewährleistet sein. Damit erhöht sich auch die Sicherheitskultur. Eine Sicherheit, die konzeptionell das gesamte Unternehmen durchdringt und strategisch vom Management abgestützt wird. Und dies auch im Zeitgeist und Spannungsfeld von Kostendruck und Image-Schaden.

#### SECURITYCONFERENCE'09:

**Referenten:** Ulrich Tilgner, Gerold Bühler, Horst Teltschik, Thomas Lüscher, Peter Fischer, Hanspeter Thür, Heinrich Müller, Dieter Meier

**Moderator:** Stephan Klapproth

**Zielpublikum:** Verwaltungsräte, Geschäftsführer, Inhaber, CEO, CIO, CSO, CTO sowie Sicherheitsbeauftragte, Security-Architekten, Riskmanager und Security-Experts

**Organisation:** Die SecurityConference'09 wird von Ispin, dem Bassersdorfer Unternehmen für Informationssicherheit organisiert

**Technologie-Partner:** IBM, Swisscom, Phion, Blue Coat, Kaspersky, Secude, Norman, E-Sec, Sonicwall, Safenet, CA, Totemo, Fortinet

**Wann:** 10. September 2009, 8 bis 18 Uhr

**Wo:** X-TRA, Limmatstrasse 118, 8031 Zürich, www.x-tra.ch

**Teilnahmegebühr:** 680 Franken exkl. MwSt.; Mitglieder von Verbänden erhalten 10 Prozent Rabatt

**Info, Programm, Anmeldung:**

www.securityconference.ch

**Security Conference**

### Perspektiven der Sicherheit spiegeln das Unternehmen

#### KONTAKT:

SecurityConference'09  
Grindelstrasse 15  
8303 Bassersdorf  
Tel. 044 838 31 11  
Fax 044 838 31 12  
markus.kaegi@  
securityconference.ch  
www.securityconference.ch