

Informationssicherheits-Management

Alles redet über Informationssicherheit. Was ist das überhaupt? Mit der weltweiten Vernetzung von Firmen, Standorten, Ländern und sogar Kontinenten steigen nicht nur Chancen, sondern auch Risiken. Zunehmende Komplexität und Unübersichtlichkeit der Strukturen sorgen dafür, dass die elektronische Geschäftswelt gegen Bedrohungen von außen aber auch von innen sehr anfällig geworden ist. Gegenmaßnahmen sind meist schlecht aufeinander abgestimmte Insellösungen, die zwar die Symptome bekämpfen, nicht aber deren Ursachen. Genau hier setzen wir an. Durch unsere ganzheitliche Betrachtungsweise schaffen wir einen deutlichen Mehrwert, gerade für kleinere und mittelständische Unternehmen. Unter "ganzheitlich" verstehen wir, dass nicht ausschließlich die Informationstechnologie eines Unternehmens betrachtet wird, sondern auch deren physikalisches Umfeld sowie die organisatorische Einbettung und die Dokumentation der Gesamtheit.

In unserer praxisorientierten Philosophie haben wir erkannt, dass ein gewinnorientiertes Unternehmen sich heutzutage nur noch ein sehr begrenztes Maß an Bürokratismus leisten kann. Daher stehen für uns Begriffe wie Kostenoptimierung, hohes Sicherheitsniveau, individuelle Sicherheitsbedürfnisse, einfache Bedienbarkeit, Flexibilität und Erweiterbarkeit im Vordergrund. Dies macht das Management von Informationssicherheit nicht nur schlank sondern auch lebbar - Klasse statt Masse!

Beispiele:

"Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden (§91 Abs. 2 AktG)."

Unternehmerisches Handeln ohne Risiken ist nicht möglich. Das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) hat durch die Änderung des §91 AktG (das übrigens auch auf GmbH's angewandt wird) die Verpflichtung des Vorstands, für ein angemessenes Risikomanagement und für angemessene interne Revision zu sorgen, explizit formuliert und damit auch zwei wichtige Attribute eines Information Security-Management-Systems beschrieben. In der Regel wird das Thema Information Security an qualifizierte Mitarbeiter delegiert. Die Verantwortung bleibt jedoch allein bei der Geschäftsleitung.



Ihr messbarer Erfolg

- ✓ Sensibilisierung für Sicherheitsdefizite
- ✓ Risikoanalyse der Geschäftsprozesse
- ✓ Erhöhung des Sicherheitsniveaus
- ✓ Kosteneinsparung durch Zentralisierung von Sicherungsmaßnahmen

Wege zur Informationssicherheit

Security Checks

Bei unseren „Security Checks“ werden sicherheitsrelevante Bereiche auf Schwachstellen analysiert und gegebenenfalls Lösungsmöglichkeiten erarbeitet. Da wir Informationssicherheit ganzheitlich betrachten, werden hierbei auch Themen berücksichtigt, die nur indirekt mit der Informationstechnologie zusammenhängen, beispielsweise bauphysikalische und organisatorische Belange. Somit könnten relevante Themen nicht nur Computer und Netzwerke sondern auch bauliche Absicherung oder etwa Notfallpläne sein.

Security Zertifizierung

Im Qualitätsmanagement ist es heutzutage üblich, dass Unternehmen ihre Prozesse nach ISO-Standard zertifizieren lassen. So gibt es auch im Sicherheitmanagement standardisierte Zertifizierungsmöglichkeiten. Z.B. die ISO Norm 27001 mit der Einführung eines systematischen Managements der Informationssicherheit in Unternehmen. Bei der Implementierung helfen unsere Einführungsseminare, in denen Strukturen und Verfahren der ISO Norm 27001 erläutert werden. Dies ist insbesondere für Unternehmen ratsam, die eine Zertifizierung nach ISO Norm 27001 anstreben.

Security Training

Im „Security Training“ bieten wir Aus- und Weiterbildung auf dem Gebiet der Informationssicherheit. Zu den Teilnehmern gehören Sicherheitsbeauftragte und Sicherheitsmanager oder auch interessierte Neueinsteiger. Verständlicherweise ist die Herstellung und Aufrechterhaltung einer umfassenden Informationssicherheit ein unternehmensweiter Prozess.

Auf Wunsch werden zum besseren Verständnis auch allgemeine Sicherheitsthemen behandelt. Im Anschluss an diese Seminare verfügen die Teilnehmer über die Fähigkeit, ein Informationssicherheits-Managementsystem aufzubauen, auf eine eventuelle Zertifizierung vorzubereiten und anschließend aufrecht zu erhalten. Weitere Schwerpunkte des „Security Training“ sind Mitarbeiter-Coaching für Unternehmen, die dieses Sicherheits-Know-how nicht im eigenen Hause vorhalten wollen, bis hin zur Moderation von Security-Workshops, in denen Risikoanalysen oder Sicherheitskonzepte erarbeitet werden.

