



Informationssicherheit

Wenn es um Unternehmenssicherheit geht, denkt der Normalbürger automatisch an Internet-Sicherheit, an den Schutz des Unternehmens gegen Angriffe von außen aus dem Internet. In der Tat beschäftigt sich die überwältigende Mehrheit aller einschlägigen Veröffentlichungen mit dieser Online-Problematik. Dabei wird aber seit geraumer Zeit immer dringlicher auf die „Bedrohung von innen“ eingegangen. Gemeint ist damit der Risikofaktor Mensch – diejenigen Sicherheitsrisiken, denen ein Unternehmen ausgesetzt ist, weil die Mitarbeiter an ihren PC-Arbeitsplätzen und mit ihren firmeneigenen Notebooks meist fahrlässig oder aus Unkenntnis die notwendigen Sicherheitsmaßnahmen nicht beachten.

IT- Sicherheit ist mehr als Schutz gegen Internetgefahren

Aber Unternehmenssicherheit ist weit mehr als nur technologischer Schutz gegen die Online-Gefahren aus dem Internet. Die angemessene Zugangskontrolle zu sensiblen Räumlichkeiten gehört ebenso dazu wie Maßnahmen zur Datensicherheit (Backup-Konzepte), Schutz gegen Einbruch und Feuer, passwortgeschützte Zugangsberechtigungen zum IT- Netz und zur Workstation sowie die strikte Beachtung und Befolgung aller gesetzlichen und lizenzrechtlichen Datenschutz-Bestimmungen.

Dafür muss jedes Unternehmen seine eigene, maßgeschneiderte IT – Unternehmens-Sicherheits-Richtlinie definieren und im Unternehmen umsetzen. Das setzt natürlich die Dokumentation der IT-Sicherheitsrichtlinie und ihre Verankerung im Bewusstsein der Mitarbeiter voraus.

Auditierung und Zertifizierung nach BS 7799 / ISO 27001

Doch die Dinge sind inzwischen in Fluss gekommen: Zertifizierung nach BS 7799 / ISO 27001 verspricht die Lösung der Problematik rund um die Unternehmenssicherheit. Mit ISO 27001 wurde ein einheitliches internationales Fundament geschaffen der beide Teile des britischen Standards berücksichtigt.

Mit dieser international anerkannten Norm, auf der auch das Grundschutzhandbuch für IT - Sicherheit des deutschen Bundesinstituts für Sicherheit in der Informationstechnik (BSI) basiert, kann das Unternehmen das Zertifikat BS 7799 / ISO 27001 erhalten. Durch die Kumulation aller Aspekte für Informationssicherheit mit ISO 27001 und den internationalen Geltungsbereich verliert BS 7799 an Bedeutung und wird durch ISO ersetzt.

Dabei beschränkt sich ISO nicht auf die technische Betrachtungsweise der Informationssicherheit in Unternehmen, sondern hinterfragt alle Facetten der Informationssicherheit und die daraus resultierenden Bedrohungen die sich für Unternehmen ergeben. Ereignisse wie



Spionage, Terror, Naturkatastrophen, Fälschung und organisierte Kriminalität sorgen dafür dass sich das Bewusstsein von der IT - Sicherheit zur Informationssicherheit wandelt. Themen wie Einstellungsverfahren, Kontrolle von Benutzerrechten, Zugangberechtigung von Systemen, Risiko - Management, Schutz von Daten vor physischen Einflüssen wie Feuer oder Wasser, Wiederherstellungspläne und die Einbindung von Mitarbeitern sind Bestandteile der Informationssicherheit.

Das Menschen in vielen Fällen der größte Risikofaktor sind, ist den meisten Verantwortlichen bewusst. Mit ISO wird dieser Risikofaktor berücksichtigt und eingebunden.

Ein ISO- zertifiziertes Unternehmen hat Vorteile:

- Minimierung des Betriebsausfall-Risikos
- Günstigere Versicherungsprämien
- Vermeidung des privaten Haftungs-Risikos für GF/Vorstand
-> KonTraG
- Vermeidung strafrechtlicher Risiken
-> BDSchG / StGB / TDG
- Verbesserte Position bei arbeitsgerichtlichen Auseinandersetzungen
-> KSchG und Abfindung
- Verbesserte Bonität im Kredit - Rating der Banken
-> Basel II