

Bei jeder Institution, die für ihre Aufgabenerledigung Informationstechnik einsetzt, sollte ein IT Sicherheitsbeauftragter ernannt werden.

Die Hauptaufgabe der IT-Sicherheitsbeauftragten besteht darin die Unternehmensleitung bei der Wahrnehmung deren Aufgaben bezüglich der IT-Sicherheit zu beraten und bei deren Umsetzung zu unterstützen. Der IT-Sicherheitsbeauftragte muss bei allen Projekten mit IT-Bezug beteiligt werden, damit sichergestellt ist, dass sicherheitsrelevante Aspekte ausreichend beachtet werden. Dazu gehören z. B. die Beschaffung von IT-Systemen oder die Gestaltung von IT-gestützten Geschäftsprozessen.

In unserem Seminar lernen Sie die Rahmenbedingungen und Aufgaben der IT-Sicherheitsbeauftragten kennen.

Inhalte des Seminars:

- **Nationale und internationale IT Sicherheitsstandards**

- BSI IT-Grundschutz
- ISO 17799
- ISO 27001
- NIST Standards
- Prüfungsstandard der Wirtschaftsprüfer IDW PS 330
- ITIL

- **Gesetzliche Vorgaben zur IT-Sicherheit**

- Risikofrüherkennung nach dem KontraG
- Anforderungen des Bundesdatenschutzgesetzes
  - Grundlagen betrieblicher Datenschutz
  - Technisch-organisatorische Maßnahmen gem. Bundesdatenschutzgesetz
- Anforderungen an die IT gem. Abgabenordnung
  - eMail Archivierung
  - GoBS (Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme)
  - Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen (GDPdU)
- Unternehmen als unfreiwillige Telekommunikationsanbieter IT-Sicherheit und das TKG
  - SPAM Filterung
  - Private Internet- und eMail Nutzung
- Internationale rechtliche Vorgaben
  - Sarbanes-Oxley Act
  - Die 8. EU-Richtlinie EuroSOX?
- Typische Haftungsrisiken im Unternehmen
  - Strafrechtliche Haftungsrisiken
    - z.B. strafbare Handlungen durch Mitarbeiter
  - Zivilrechtliche Haftungsrisiken
    - z.B. Urheberrechtsverletzungen durch Mitarbeiter
- Markenrecht
  - Domainnamen und Webadressen

- **Aufgaben der IT-Sicherheitsbeauftragten**

- Festlegung der IT-Sicherheitsziele und -strategie
- Erstellung einer IT-Sicherheitsleitlinie
- Erstellung von zielgruppengerechten IT-Sicherheitsrichtlinien
- Aufbau einer geeigneten Organisationsstruktur für IT-Sicherheit
- Integration der Mitarbeiter in den Sicherheitsprozess
- Integration der IT-Sicherheit in organisationsweite Abläufe
- Wirtschaftlicher Einsatz von Ressourcen für IT-Sicherheit
- Managementreporte und -bewertungen der IT-Sicherheit
- Aufrechterhaltung der IT-Sicherheit

**Referenten:**

Holger Filges

*TüV Rheinland geprüfte Qualifikation als Datenschutz-Auditor (TüV)*

*Lizenzierter Auditor für ISO 27001-Audits auf der Basis von IT-Grundschutz (BSI)*

Oliver Gönner

*Rechtsanwalt, Datenschutzbeauftragter gem. Ulmer Modell*

**Termin:**

08.09.2010 - 10.09.2010 (Findet garantiert statt.)

28.06.2011 - 30.06.2011

**Seminarort:**

Oberhausen (Ruhrgebiet)

**Seminarpreis:**

999,- p.P. zzgl. ges. MwSt.

**Leistungen:**

Zertifikat, Pausensnacks, Mittagessen, Getränke und Handout.

**Anmeldung:**

[➔ Online Anmeldung](#)

[⬇ Fax-Anmeldung \[pdf\]](#)