

## Aufgaben des IT-Sicherheitsbeauftragten:

- Wissen, laufende eigene Fortbildung, Informationsbeschaffung (rechtl. Grundlagen, aktuelle Entwicklungen und Bedrohungen, ...)
- Erhebung firmeninterner Ist-Stand (technisch & organisatorisch)
- Information und Beratung der GF, Information und Schulung der Mitarbeiter, Abstimmung mit dem Datenschutzbeauftragten & dem Betriebsrat/Personalrat
- Entwurf und Aktualisierung von Dokumenten (bei Änderung der rechtl. Lage, der IT-Landschaft, der Sicherheits-Lage): IT-Sicherheitsleitlinie (strategische Ziele usw.), IT-Sicherheitskonzept (u.a. Risiko-Analysen), Notfallhandbuch, interne Richtlinien & Anweisungen, ...
- Kontrolle der Umsetzung (wurde umgesetzt?) und ihrer Effektivität (hatte es die beabsichtigte Wirkung?)
- Dokumentation der Maßnahmen
- Koordination bei Audits und Zertifizierungen
- Kommunikation, Koordination und Dokumentation bei akuten Vorfällen (auch nach außen, z.B. bei Meldepflicht)
- Ressourcen- und Investitionsplanung im IT-Sicherheits-Bereich
- Entwurf, Aufbau und Weiterentwicklung der IT-Sicherheits-Organisation
- Beratung bei der Einführung neuer IT-Systeme (HW / SW / Infrastruktur), bei IT-Projekten (von Anfang an sicher machen, nicht nachträglich!)  
=> Mitglied des IT-Lenkungsausschusses
- Einschulung einer Vertretung und Nachfolge

==> Primär Kommunikations- und Organisations-Job, kein technischer Job

==> Bei halben Stellen: Achtung auf Interessens- und Weisungskollisionen!