

Der IT-Sicherheitsbeauftragte und seine Aufgaben

(Quelle: Bundesamt für Sicherheit in der Informationstechnik – BSI)

Bei jeder Institution, die für ihre Aufgabenerledigung Informationstechnik (IT) einsetzt, sollte ein IT- Sicherheitsbeauftragter ernannt werden. Ob diese Stelle von einer einzelnen Person, einer Personengruppe oder in Teilzeit wahrgenommen wird, hängt von der Größe des Unternehmens, der vorhandenen Ressourcen und dem angestrebten Sicherheitsniveau ab. Die Hauptaufgabe des IT-Sicherheitsbeauftragten besteht darin die Unternehmensleitung bei der Wahrnehmung deren Aufgaben bezüglich der IT-Sicherheit zu beraten und bei deren Umsetzung zu unterstützen.

Aufgabenbeschreibung

Allgemein lassen sich die Aufgaben des IT-Sicherheitsbeauftragten wie folgt zusammenfassen.

Der IT-Sicherheitsbeauftragte:

- bereitet die Auffassung der Unternehmensleitung über Stellenwert der IT, anzustrebendes IT- Sicherheitsniveau und die unternehmensweiten IT-Sicherheitsziele vor, formuliert sie aus und führt eine Entscheidung herbei.
- berichtet der Unternehmensleitung über den Status Quo zur IT-Sicherheit.
- berät die Unternehmensleitung zu Fragen der IT-Sicherheit.
- entwickelt und formuliert die IT-Sicherheitsleitlinie und holt danach die Zustimmung der Unternehmensleitung ein.
- gibt die abgestimmte IT-Sicherheitsleitlinie allen betroffenen Mitarbeitern des Unternehmens bekannt.
- erlässt Richtlinien und Regelungen, auf welche Weise IT-Sicherheit im Unternehmen erreicht werden soll.
- unterstützt die Anwendung des IT-Grundschutzes und die Durchführung von Risikoanalysen zur Erstellung des IT-Sicherheitskonzeptes.
- koordiniert die IT-Sicherheitsziele mit den Unternehmenszielen zum IT-Einsatz und stimmt sie mit den IT-Strategien der einzelnen Unternehmensbereiche ab.
- legt die Aufgaben für IT-Sicherheit für den nachgeordneten Bereich fest.
- überprüft die erstellten IT-Sicherheitskonzepte auf Korrektheit und Nachvollziehbarkeit.
- bereitet die Unternehmensentscheidung über zu treffende, kostenträchtige IT-Sicherheitsmaßnahmen vor und führt eine Entscheidung herbei.
- verwaltet die für IT-Sicherheit zur Verfügung stehenden Ressourcen an Geld und Arbeitszeit.
- kontrolliert den Fortschritt der Realisierung von IT-Sicherheitsmaßnahmen.
- koordiniert Kontrollen der Effektivität von IT-Sicherheitsmaßnahmen im laufenden Betrieb.
- koordiniert Sensibilisierungs- und Schulungsmaßnahmen zum Thema IT-Sicherheit.