Hinführung zur Umsetzung eines IT-Sicherheitskonzepts nach IT-Grundschutz Anforderungen zur Informationssicherheit

Unser IT-Sicherheitskonzept gibt eine Empfehlung zur Umsetzung der Vorgaben und Anforderungen zur IT- Sicherheit gemäß IT-Grundschutz des BSI (Bundesamts für Sicherheit in der Informationstechnik) als Basis für Informationssicherheit wieder.

Dies ermöglicht ein systematisches Vorgehen, um notwendige Sicherheitsmaßnahmen zu identifizieren und umzusetzen. Die BSI-Standards nach IT-Grundschutz liefern hierzu bewährte Vorgehensweisen, das IT-Grundschutz-Kompendium die konkreten Anforderungen.

Unser IT-Sicherheitskonzept ist konform zu den Vorgaben zur IT-Sicherheit und der Modellierung nach IT-Grundschutz des BSI. Dies bietet Einrichtungen und Institutionen ein systematisches und einheitliches Vorgehen bei der Identifizierung und Umsetzung von notwendigen Sicherheitsmaßnahmen zur Basisabsicherung nach den BSI-Standards oder den weit umfangreicheren Bausteinen des IT-Grundschutz-Kompendiums (frühere IT-Grundschutz-Kataloge).

Die IT-Sicherheitskonzept-Vorgehensweise besteht aus den folgenden Einzelschritten:

Definition des Informationsverbundes (IT-Verbund):

- Zu Beginn dieses IT-Sicherheitskonzepts wird festgelegt, welcher Bereich der Einrichtung abgedeckt wird (Geltungsbereich).

Strukturanalyse:

- Grundlage eines jeden IT-Sicherheitskonzepts ist die genaue Kenntnis der Informationen, Prozesse und unterstützenden technischen Systeme des betrachteten Informationsverbundes. Ziel der Strukturanalyse ist es, die hierfür erforderlichen Kenntnisse zusammenzustellen und aufzubereiten.

Schutzbedarfsfeststellung:

- Bei der Schutzbedarfsfeststellung wird ermittelt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.

Modellierung:

- Für den betrachteten Informationsverbund werden die relevanten Bausteine (Maßnahmensammlung) der IT-Grundschutz-Kataloge ausgewählt, auf deren Basis im weiteren Verlauf mögliche Sicherheitsmaßnahmen definiert werden.

Basis-Sicherheitscheck:

- Ein Überblick über das vorhandene Sicherheitsniveau wird erarbeitet. Mit Hilfe / im Rahmen eines Vor-Ort-Termins in der Einrichtung wird der Status quo des bestehenden Informationsverbunds in Bezug auf den Umsetzungsstatus für jede relevante Maßnahme bewertet.

Ergänzende Sicherheitsanalyse:

- Die ergänzende Sicherheitsanalyse stellt sicher, dass die nicht vollständig abgedeckten Risiken (z. B. bei höherem Schutzbedarf) ermittelt werden.

Risikoanalyse:

- Ziel der Risikoanalyse ist, die vorhandenen Risiken durch eine Risikobehandlung auf ein verträgliches bzw. akzeptables Maß (Restrisiko) zu reduzieren.
- Die Beispiele/exemplarische Einträge für die wesentlichen Abschnitte/Kapitel in unserem IT-Sicherheitskonzept geben einen Einblick, wie ein Sicherheitskonzept systematisches und einheitlich nach den Vorgaben des IT-Grundschutzes (BSI) zu erstellen ist. Das Sicherheitskonzept muss regelmäßig fortgeschrieben und mit der zuständigen GF / Leitung IT und dem IT-Sicherheitsbeauftragten abgestimmt werden.