LU05a - Einleitung

Ein Netzwerk-Sicherheitskonzept ist ein spezifisches Dokument, das sich auf die Sicherheit eines Unternehmensnetzwerks konzentriert. Dieses Konzept umfasst nicht nur technische Massnahmen, sondern auch Nutzungsrichtlinien und Verhaltensregeln für Mitarbeiter. Ohne ein solches schriftlich ausgearbeitetes Konzept ist die Gefahr gross, dass die Vorgaben zur Sicherheit nur unscharf in den Köpfen einiger Beteiligter formuliert sind.

Ein Netzwerk-Sicherheitskonzept dient dazu, die **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** der in einem Netzwerk gespeicherten Daten und Dienste zu gewährleisten. Es sollte regelmässig aktualisiert werden, um sich den sich wandelnden Bedrohungen und technologischen Entwicklungen anzupassen. Die Einhaltung der Nutzungsregeln durch die Mitarbeiter spielt eine entscheidende Rolle bei der Sicherung des Netzwerks.

Anforderungen an ein Sicherheitskonzept

Die Ausarbeitung eines Sicherheitskonzepts ist eine Arbeit, bei der viele Teilaspekte in Bezug auf IT Security zu berücksichtigen sind:

- Absichern der Kommunikationswege im Fest- und Mobilnetz
- Schutz des Netzwerks vor unerwünschten Eindringlingen
- Die Prüfung der Sicherheit von PCs und Servern
- Richtlinien für die Nutzer
- Schulung und Sensibilisierung der Nutzer
- Updateroutinen
- Sicherheit der Daten
- Festlegung, welche Daten als sensibel anzusehen sind

Bestandteile eines IT-Sicherheitskonzepts

Ein IT-Sicherheitskonzept besteht aus mehreren verschiedenen Teilen, die je nach Unternehmen individuell anzupassen sind:

- Als erstes wird die **Bestandsanalyse** durchgeführt. Hier werden Assets, wie beispielsweise Dokumente, Zugriffsrechte und andere Daten, die schützenswert sind, ermittelt. Schaffen Sie in diesem Zuge einen schriftlichen Überblick darüber.
- Danach erfolgt die **IT-Strukturanalyse**. Alle Assets werden nun strukturiert erfasst. Diese werden in Teilbereiche aufgeteilt, die wiederum einen gesamten Geschäftsprozess abbilden. Alle Komponenten aus den verschiedenen Prozessen und Abteilungen, von Sales bis hin zum HR-Bereich, werden erfasst und analysiert.
- Ergänzend dazu wird eine **Schutzbedarfserstellung** durchgeführt, bei der zu ermitteln ist, wie hoch der Schutzbedarf einzelner Objekte tatsächlich ist. So erhalten neuwertige Fertigungsverfahren und personenbezogene Daten beispielsweise eine höhere Schutzstufe als Kontaktdaten zu juristischen Personen, wie Unternehmensadressen. Die Modellierung erfolgt nach dem jeweiligen IT-Grundschutz und soll die vorherigen Schritte graphisch veranschaulichen.
- Zum Basis Sicherheitscheck kommt eine ergänze **Sicherheits- und Risikoanalyse** hinzu. Die

Ergebnisse der Risikoanalyse werden am Ende vollständig dokumentiert.

---

m117