Sicherheitskonzept

Paul Kühn 11.09.2024



Sicherheitskonzept

# 3. Hauptziele:

### Vertraulichkeit:

Vertraulichkeit bedeutet, dass nur autorisierte Personen auf bestimmte Daten Zugriff haben. Man versucht unbefugten Zugriff auf sensible Informationen zu verhindern. Dies geschieht mithilfe von Passwörtern.

### Integrität:

Integrität bezieht sich auf die Vollständigkeit und Genauigkeit der Daten. Die Integrität stellt sicher das alle Informationen, die durch ein Netzwerk übertragen oder in einem Netzwerk gespeichert sind, korrekt sind. Dies wird mithilfe von Backups erreicht.

### Verfügbarkeit:

Verfügbarkeit stellt sicher, dass Daten und Dienste zu jeder Zeit verfügbar sind, wenn sie benötigt werden. Zum Beispiel kommt hier das Prinzip der Lastenverteilung zum Einsatz, um die Server nicht zu überlasten und damit die Verfügbarkeit sicherzustellen.

# Nutzen eines Sicherheitskonzepts:

Sicherheitskonzepte dienen als umfassende Strategie zum Schutz von IT-Systemen, Daten und Infrastrukturen in Organisationen. Ein durchdachtes Sicherheitskonzept identifiziert potenzielle Risiken und Bedrohungen, sodass geeignete Schutzmaßnahmen angewendet werden können. Dadurch wird das Risiko von Datenverlusten, Systemausfällen und Cyberangriffen minimiert. Sollte es dennoch zu einem Zwischenfall kommen, legt ein Sicherheitskonzept Notfallpläne fest, um schnell und effektiv zu reagieren. So können Schäden eingedämmt und die Zeit des Wiederherstellens der Systeme minimiert werden.

# Erstellen eines Sicherheitskonzept:

### Bestandsanalyse:

Der Erste Schritt des Erstellens eines Sicherheitskonzepts ist die Bestandsanalyse. Hierbei werden alle relevanten Assets eines Unternehmens erfasst. Die Identifikation wird schriftlich festgehalten. Sie stellt sicher, dass alle schützenswerten Informationen erfasst und dokumentiert werden.

### IT-Strukturanalyse:

Bei der IT-Strukturanalyse werden alle erfassten Assets aus der Bestandsanalyse strukturiert und in einer übersichtlichen Form dargestellt. Die IT-Infrastruktur wird in verschiedene Teilbereiche aufgeteilt. Dazu zählen Hardware, Software, Netzwerke und Sicherheitskomponenten. Das Ziel ist es hierbei, einen vollständigen Überblick über alle relevanten IT-Elemente zu erhalten.

### Schutzbedarfserstellung

Bei der Schutzbedarfserstellung wird ermittelt, welche Elemente einen besonderen Schutzbedarf haben. Nicht alle Assets sind gleichermassen schutzbedürftig und werden daher in verschiedene Kategorien anhand des IT-Grundschutz unterteilt. Dies dient der effizienten Aufteilung vorhandener Ressourcen.

### Sicherheits- und Risikoanalyse

Bei einer Sicherheits- und Risikoanalyse werden mögliche Bedrohungen sowie Schwachstellen identifiziert. Ziel ist es, die Wahrscheinlichkeit und den potenziellen Schaden dieser Risiken zu analysieren und entsprechende Gegenmassnahmen zu ergreifen.