# Inforeihe „Informationssicherheit“


Informationssicherheit ist eine existentielle Voraussetzung für jedes Unternehmen, der sich kein Verantwortlicher entziehen kann.
In dieser sechsteiligen Inforeihe zeigen wir die Zusammenhänge auf und geben eine Hilfestellung für  das eigene Vorgehen.

**Teil 5: Wie kann die Entwicklung der Informationssicherheit überwacht werden?**

Der aktuelle Status der Informationssicherheit spiegelt sich in verschiedenen Themenfeldern wieder:

- Konsequenz der Maßnahmenumsetzung
- Aktualität der Risikobeurteilungen
- Sicherheitsbewusstsein der Organisation
- Konsequenz der Aufzeichnung von Ereignissen und Veränderungen
- Regelmäßige Beurteilung der aktuellen Situation
- Gezielte Herbeiführung von Managemententscheidungen

Anhand dieser Auflistung sehen Sie, dass eine auf Langfristigkeit ausgelegte Informationssicherheit nicht durch einen punktuellen „Aktionismus“ zu erreichen ist. Sie ist eine permanente Aufgabe – deshalb fokussiert die ISO 27001 auch das Informationssicherheits-Managementsystem.

Dehalb hier ein paar Hinweise / Tipps aus der Praxis:

- Dokumentieren Sie alle administrativen Aktivitäten, die zentrale Komponenten oder Zugangsmodalitäten betreffen.
- Zeichnen sie alle Vorfälle der Informationssicherheit auf und analysieren Sie mehr- bzw. vielfaches Auftreten, um sie systematisch zu beseitigen.
- Berichten Sie den aktuellen Status regelmäßig dem Management und sorgen Sie für adäquate Entscheidungen.
- Kontrollieren Sie die Umsetzung der internen Richtlinien regelmäßig und effektiv (= unangekündigt).
- Bringen Sie Ihre Zulieferer bzw. Dienstleister dazu, denselben Sicherheitsstandard zu verfolgen – und überzeugen sich sich davon.

Diese Auflistung ist bei Weitem nicht vollständig. Letztlich geht es darum, dass die gesamte Organisation im Umgang mit Informationen zu jedem Zeitpunkt genau das tut, was beabsichtigt ist. Das bedeutet für die Mitarbeiter, dass sie die Richtlinien befolgen und deren Bedeutung kennen und verstehen. Das heiß aber auch, dass die Prozesse und die IT-Umgebung zu jedem Zeitpunkt so „funktionieren“, wie es beabsichtigt ist. Veränderungen an Prozessen oder deren Abbildung in Systemen müssen zwingend geplant und dokumentiert werden!

Das muss nicht zwangsläufig viel Aufwand bedeuten, sondern kann mit der entsprechenden Erfahrung recht effizient organisiert werden.

Lesen Sie in der nächsten Ausgabe:
**Warum sollte das Sicherheitsmanagement ständig verbessert werden?**

*Für Eilige haben wir zusätzliche Informationen unter:* www.teaming-IT.de/Vertrauen