Presse-Mitteilung

TÜV SÜD Checkliste 9. März 2015

Managementsystem für die Informationssicherheit

München. Das Thema Informationssicherheit sollte nicht unterschätzt werden, denn der Schutz von Daten und deren Verfügbarkeit sind essentiell für den Erfolg von Unternehmen. Ein Großteil der nötigen Maßnahmen und Zuständigkeiten entfällt dabei auf das Management und muss dementsprechend geplant und gesteuert werden. Die Experten von TÜV SÜD geben Tipps für die Umsetzung eines Informationssicherheits-Managementsystems und informieren über die kritischen Erfolgsfaktoren.

Die Umsetzung

- **Geltungsbereich:** Im ersten Schritt müssen der Geltungsbereich und die Grenzen des Informationssicherheits-Managementsystems definiert werden.
- **Informationssicherheitspolitik:** Anschließend braucht es eine vom Management bestätigte Informationssicherheitspolitik im Unternehmen, die die sicherheitsbezogenen Ziele, Strategien, Verantwortlichkeiten und Maßnahmen langfristig und verbindlich festlegt. Jedes Unternehmen sollte dabei für sich selbst definieren, welchen Grad an Sicherheit es benötigt.
- **Informationswerte:** Im dritten Schritt sind die wesentlichen Informationswerte zu definieren und zu kategorisieren. Darunter können technische Systeme, Informationen, Dokumente aber auch Personen fallen. Entsprechend der Kategorisierung als vertraulich, streng vertraulich etc. ergeben sich dann die zu treffenden Maßnahmen.
- **Risiken:** Je nach Rahmenbedingungen und Standort des Unternehmens gibt es unterschiedliche Risiken, die identifiziert werden müssen. Darunter können fallen: Überflutungen, Erdbeben, Brand, Cyberattacken oder der Ausfall von Kühlgeräten. Je nach Schwere der identifizierten Risiken ist abzuwägen, ob dieses Risiko tragbar ist oder ob entsprechende Maßnahmen notwendig sind.
- **Sicherheitsmaßnahmen:** Schlussendlich sollten die entsprechenden Sicherheitsmaßnahmen eingeleitet werden. Eine Orientierungshilfe mit passenden Maßnahmen bietet Anhang A der ISO 27001. Dazu zählen beispielsweise die Zugangskontrolle, der Schutz vor Malware, ein Backup für die Informationen oder die Zuteilung von Verantwortlichkeiten.

Kritische Erfolgsfaktoren

- **Geschäftsziele:** Alles rund um die Informationssicherheit – ob grundsätzliche Regelungen, Ziele oder Maßnahmen – muss einen Bezug zu den Geschäftszielen haben und auf diese abgestimmt sein – Informationssicherheit darf kein Selbstzweck sein, sondern muss den Geschäftszielen dienen.
- **Unternehmenskultur:** Vorgehen und Vorgehensmodell sollten mit der Unternehmenskultur übereinstimmen, um reibungslos zu funktionieren.
- **Management-Zustimmung:** Jegliche Maßnahmen und Regelungen der Informationssicherheit brauchen volle Zustimmung und Unterstützung durch das Management aller Hierarchieebenen.
- **Risikobewertung:** Alle Beteiligten brauchen ein gutes Verständnis von Risikobewertung und -management, weshalb umfangreiche Trainings sinnvoll sind. Zu Beginn kann eine nicht so detaillierte Risikobewertung, die nach und nach verfeinert wird, helfen um den Prozess überhaupt zu starten.
- **Informationssicherheitspolitik:** Die Kenntnis der Sicherheitspolitik ist essentiell, daher sollten sowohl Manager als auch Mitarbeiter sowie externe Beteiligte regelmäßig geschult werden.
- **Problem-Bewusstsein:** Durch Schulungen der Mitarbeiter sollte für ein vernünftiges Problem-Bewusstsein gesorgt werden.
- **Budget:** Damit immer ausreichend Budget für die Aktivitäten und Maßnahmen der Informationssicherheit bereit steht, muss ein realistischer Kostenplan erstellt werden.
- **Prozesse für kritische Vorfälle:** Tritt der Fall der Fälle ein, beispielsweise eine Cyberattacke oder ein Ausfall der Kühlgeräte, ist ein klar definierter Prozess notwendig, in dem auch die Verantwortlichkeiten und genaue Anforderungen festgehalten sind.
- **Kennzahlen-System:** Um die Effizienz und die kontinuierliche Verbesserung des Informationssicherheitsmanagements zu steuern, ist der Aufbau eines Kennzahlen-Systems sinnvoll.

Weitere Informationen zu den Themen Informationssicherheit, Datenschutz und IT-Security erhalten Interessenten unter http://www.tuev-sued.de/informationstechnologie-it oder unter der kostenlosen Rufnummer 0800/5791-5005. Seminare zur Informationssicherheit bietet die TÜV SÜD Akademie an www.tuev-sued.de/akademie/informationssicherheit.

Presse-Kontakt:

Carolin Eckert TÜV SÜD AG Unternehmenskommunikation Westendstr. 199, 80686 München	Tel. +49 (0) 89 / 57 91 – 15 92 Fax +49 (0) 89 / 57 91 – 22 69 E-Mail carolin.eckert@tuev-sued.de Internet www.tuev-sued.de

Als einer der führenden Dienstleister in den Bereichen Prüfung, Begutachtung, Auditierung, Zertifizierung, Schulung und Knowledge Services sorgt TÜV SÜD für Qualität, Sicherheit und Nachhaltigkeit. Seit 1866 schützt der technische Dienstleister gemäß seinem Gründungsauftrag Menschen, Umwelt und Sachgüter vor den nachteiligen Auswirkungen der Technik. Das Unternehmen mit Sitz in München ist inzwischen an über 800 Standorten weltweit vertreten. TÜV SÜD beschäftigt mehr als 20.000 Experten aus den verschiedensten Fachdisziplinen, die auf ihren Gebieten als Kapazitäten anerkannt sind. Der technische Dienstleister kombiniert unabhängige und neutrale Kompetenz und Fachkenntnis mit wertvollen Informationen und bietet Unternehmen, Verbrauchern und Umwelt damit echten Mehrwert. TÜV SÜD möchte seine Kunden auf der ganzen Welt mit einem umfassenden Leistungsspektrum unterstützen und so Effizienz steigern, Gemeinkosten senken und Risiken beherrschbar machen. www.tuev-sued.de