TÜV Rheinland: Anforderungen der ISO 27001 mit der Realität im Unternehmen abgleichen

10.04.2019 | Köln

Die Einführung eines Informationssicherheits-Managementsystems (ISMS) nach ISO 27001 ermöglicht es, Informationssicherheit im Unternehmen dauerhaft zu steuern und zu verbessern. Die Norm stellt verschiedene Anforderungen an Design und Dokumentation von Prozessen und Verantwortlichkeiten, die es gilt, möglichst lückenlos zu erfüllen. „Die Praxis zeigt allerdings, dass es immer wieder unbemerkte offene Flanken gibt, die eine Zertifizierung vereiteln können“, so Ralph Freude, Experte für Managementsysteme zur Informationssicherheit bei TÜV Rheinland.

Beispielsweise haben die Unternehmen zwar die Sicherheit der IT-Infrastruktur im Fokus, aber nicht die physische Sicherheit im Blick. Ungesicherte Seiteneingänge am Gebäude sind eine ungewollte Einladung an Cyberkriminelle. Sie eröffnen unbefugten Dritten

ungehinderten Zugang zum Unternehmen, zu Mitarbeiter-Arbeitsplätzen oder sogar zum Serverraum und damit zu Daten und digitalen Werten der Organisation.

Was ebenfalls immer wieder geschieht: Aufgaben innerhalb der Organisation sind nicht sauber voneinander getrennt, eine Kontrolle durch Dritte – etwa bei der Ausgabe von IT-Geräten – findet nicht statt. Oder: Unternehmenswerte werden nicht inventarisiert. Beim Ausscheiden des Mitarbeiters erfolgt keine geordnete Rückgabe der zuvor ausgehändigten Arbeitsmittel wie beispielsweise Laptops und Smartphones. Fast schon ein Klassiker stellt die unsachgemäße Entsorgung vertraulicher personenbezogener Daten dar. Gehaltsabrechnungen, Kundeninformationen, die unbefugten Dritten in die Hände fallen können – sind ein grober Verstoß gegen den Datenschutz und sind ein KO-Kriterium, die das Erfüllen der ISO 27001-Anforderungen vereiteln.

Anforderungen der Norm ISO 27001 mit der Realität im Unternehmen abgleichen

„Wer den Erfolg eines Prüfverfahrens und der Zertifizierung nicht gefährden will, sollte die Anforderungen der Norm ISO 27001 bei der Einführung des ISMS gewissenhaft mit der Realität im Unternehmen abgleichen“, erklärt Ralph Freude. Eine praktische Hilfe dazu ist der Leitfaden von TÜV Rheinland, der konkrete Sicherheitslücken aufzeigt, die bei der Implementierung eines ISMS oft unter den Tisch fallen. Der zwanzigseitige Leitfaden stellt eine ganze Reihe typischer Sicherheitslücken vor und liefert Hinweise, wie sich diese effektiv beheben lassen. Geschäftsführer, CISOs und

Informations-Sicherheitsbeauftragte, die bereits ein Informationssicherheits-Managementsystem implementiert haben, erhalten damit wichtige Ansatzpunkte, um bereits getroffene Sicherheitsmaßnahmen im eigenen Hause auf Konformität mit der ISO 27001 zu überprüfen. Mehr unter www.tuv.com/27001-Leitfaden

Kontakt für Journalisten: Antje Golbach
Telefon: +49 221 806-4465
E-Mail: antje.golbach@de.tuv.com

****

TÜV Rheinland ist ein weltweit führender unabhängiger Prüfdienstleister mit fast 150 Jahren Tradition. Im Konzern arbeiten über 20.000 Menschen rund um den Globus. Sie erwirtschaften einen Jahresumsatz von 2 Milliarden Euro. Die unabhängigen Fachleute stehen für Qualität und Sicherheit von Mensch, Technik und Umwelt in fast allen Wirtschafts- und Lebensbereichen. TÜV Rheinland prüft technische Anlagen, Produkte und Dienstleistungen, begleitet Projekte, Prozesse und Informationssicherheit für Unternehmen. Die Experten trainieren Menschen in zahlreichen Berufen und Branchen. Dazu verfügt TÜV Rheinland über ein globales Netz anerkannter Labore, Prüfstellen und Ausbildungszentren. Seit 2006 ist TÜV Rheinland Mitglied im Global Compact der Vereinten Nationen für mehr Nachhaltigkeit und gegen Korruption.

Website www.tuv.com