Knipp Fallstudie

DIN ISO/IEC 27001:2015-Zertifizierung

Die ISO 27001 ist der führende internationale Standard für die Informationssicherheit. Das ISO 27001-Team von Knipp arbeitet kontinuierlich an der Verbesserung unserer Sicherheitsmaßnahmen.

Wir haben den Geschäftsführer Elmar Knipp (links), die Informationssicherheitsbeauftragte Linda Müller (rechts) und den Datenschutzbeauftragten Damian Lusiewicz (2.v.r.) nach Motiven, Erfahrungen und Erfolgen bei der ISO 27001-Zertifizierung befragt. Unser Bild zeigt außerdem Erol Pektas, Geschäftsführer des IFAZ Institut für Auditierung und Zertifizierung GmbH, bei der Übergabe der Zertifizierungsurkunde an Knipp.

Warum hat Knipp ein ISMS eingeführt?

Elmar Knipp: Informationen sind bei uns *die* zentrale Ressource. Alle Dienstleistungen bauen im Kern auf den Daten unserer Kunden auf. Ein Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit dieser Informationen könnte daher schnell geschäftskritisch werden. Deshalb haben wir uns entschlossen, unsere umfangreichen aber teilweise heterogenen Sicherheitskonzepte in einem zentralen Managementsystem zu strukturieren und zu systematisieren. Oberstes Ziel war dabei natürlich eine nachhaltige Verbesserung des Gesamt-Sicherheitskonzeptes.

Und wieso nun die ISO-Zertifizierung?

Linda Müller: Die ISO 27001 ist ein anerkannter internationaler Standard und bietet uns die Möglichkeit, die Wirksamkeit der Sicherheitsmaßnahmen bei Knipp für unsere Kunden transparent zu machen. Auf diese Weise möchten wir uns natürlich auch von weniger professionell arbeitenden Wettbewerbern abheben.

Was war die größte Herausforderung bei der ISO-Zertifizierung?

Damian Lusiewicz: Aufgrund der schon erwähnten Bedeutung der Datenverarbeitung für sämtliche Tätigkeitsfelder von Knipp haben wir schon immer großen Wert auf Informationssicherheit gelegt. Daher waren für alle Geschäftsprozesse bereits spezielle Sicherheitskonzepte etabliert. In dieser Hinsicht war die Einführung des ISMS also in erster Linie eine Fleißarbeit.

In einem ersten Schritt wurde eine Risikoanalyse nach Maßgabe der ISO 27005 durchgeführt. In vielen Gesprächen mit Kollegen und der Geschäftsführung wurden als Grundlage zunächst unternehmensweit alle geschäftskritischen Prozesse erfasst. Die zugehörigen Assets wurden anschließend in ein dediziertes Softwaresystem aufgenommen und alle denkbaren Bedrohungen und Gegenmaßnahmen identifiziert und klassifiziert.

Gerade bei der Risikoanalyse und -bewertung gab es auch durchaus kontrovers geführte Diskussionen. Im Nachhinein sehen wir das aber als wichtigen Teil des Zertifizierungsprozesses an, da es geholfen hat, das Bewusstsein für Informationssicherheit bei allen Beteiligten zu stärken.

Das ISMS wurde durch ein externes Audit überprüft…

Linda Müller: Genau. Eine externe Prüfung ist sinnvoll, um die Korrektheit und Effektivität des ISMS von unabhängiger Seite bestätigen zu lassen. Zuerst wurde die Dokumentation der Sicherheitsmaßnahmen auf Vollständigkeit und Sinnhaftigkeit geprüft. Dann erfolgte ein Abgleich des ISMS mit den Vorgaben der ISO-Norm. Besonders spannend für uns war natürlich die abschließende »praktische Überprüfung« inklusive Ortsbegehung und Mitarbeiter-Interviews.

Welche Vorteile können Sie bisher sehen?

Elmar Knipp: Wir haben unsere Sicherheitskonzepte vereinheitlicht und in einem zentralen ISMS konsolidiert. Das macht viele Abläufe effizienter und erleichtert die notwendige permanente Weiterentwicklung der Maßnahmen und Prozesse.

Und wie geht es nun weiter?

Elmar Knipp: Die Selbstverpflichtung zur Aufrechterhaltung und kontinuierlichen Verbeserung der Informationssicherheit, zu der wir uns mit der ISO 27001-Zertifizierung bekannt haben, nehmen wir sehr ernst. Dazu ist es wichtig, alle Beteiligten mit ins Boot zu holen und das Bewusstsein für Sicherheitsverstöße, Risiken und natürlich auch Verbesserungspotenziale zu stärken. Die Einführung des ISMS war ein erster Schritt auf dem Weg, den wir nun mit weiteren Sensibilisierungsmaßnahmen und regelmäßigen internen und externen Audits weiter gehen.