Pressemitteilung

Wer hat Angst vorm Auditor?

Wie ein mittelständisches Unternehmen die ISO 27001-Zertifizierung erlebte

Stuttgart, 19.04.2018: Sie ist in aller Munde, die Norm ISO/IEC 27001, kurz ISO 27001 genannt. Betreiber kritischer Infrastrukturen lassen sich danach zertifizieren, um vor dem Gesetz ihre Compliance zu beweisen. Warum aber lässt sich ein kleines mittelständisches Unternehmen aus Stuttgart zertifizieren? Und welche Erfahrungen hat es dabei gemacht? Die ICS AG aus Stuttgart ist den Schritt gegangen. Drei beteiligte Mitarbeiter teilen ihre Erfahrungen.

Die ICS AG hat allen Grund zu feiern: Das Stuttgarter IT-Engineering und Consulting-Unternehmen hat die Zertifizierung nach dem international anerkannten Sicherheitsstandard ISO 27001 erhalten. Für das mittelständische Unternehmen, das selbst seit über 50 Jahren in der Sicherheitsberatung tätig ist, haben unternehmenspolitische Erwägungen zu der Entscheidung geführt.

Der Informationssicherheitsaspekt gewinnt durch das IT-Sicherheitsgesetz und verschärfte Vorschriften wie die Datenschutzgrundverordnung (DSGVO) zunehmend an Gewicht. Sie zwingen nicht nur global agierende Firmen und Betreiber kritischer Infrastrukturen zum Handeln sondern auch deren Zulieferer und Dienstleister. Rainer Gerhäuser, kaufmännischer Leiter und Beauftragter für das Qualitätsmanagement bei der ICS AG, sagt*: „Mit einer Zertifizierung nach der ISO 27001 beweisen wir unseren Geschäftspartnern gegenüber, dass wir mit dem, was wir innerhalb des Unternehmens tun, nachweislich sicher umgehen.*“

Für das ISMS werden die Kernkompetenzen in den Fokus gestellt

Die ISO 27001 stellt die Einführung eines Informationssicherheits-Managementsystems (ISMS) in den Mittelpunkt. Es definiert Regeln und Methoden, um die Informationssicherheit in einem Unternehmen zu gewährleisten. Um überhaupt definieren zu können, welche Maßnahmen im jeweiligen Unternehmen ergriffen werden müssen, wird zunächst der Geltungsbereich definiert. *„Das Unternehmen muss klar seine Kernkompetenzen in den Fokus stellen und nicht Prozesse, die notwendigerweise sowieso getan werden müssen, wie beispielsweise die Buchhaltung“,* rät Gerhäuser. *„Der Fokus muss sein: Womit agieren wir am Markt?“* Nach Meinung von Andrian Dürr, IT-Sicherheitsberater bei der ICS AG, schafft dies auch erst Glaubwürdigkeit. *„Der Geltungsbereich wird auf dem Zertifikat eingetragen. Und da das Zertifikat öffentlich einsehbar ist, stellt der Geltungsbereich nicht nur für die Zertifizierung einen wichtigen Teil dar. Er schafft auch Glaubwürdigkeit gegenüber unseren Geschäftspartnern.“*

Zieldefinitionen sichern die Qualität der Maßnahmen

Ein weiterer Schritt zur Vorbereitung auf die Zertifizierung ist die Bestimmung der Informationssicherheitsziele. Dabei geht es um die Qualität der Sicherheitsmaßnahmen sowie deren Anwendbarkeit und Wirkung. Dürr erläutert: *„Man definiert verschiedene Messgrößen*

anhand derer ich ablesen kann, ob das ISMS, das ich aufgesetzt habe, überhaupt funktioniert. Die Norm macht dazu zwar keine Vorgaben, sie stellt aber gewisse Qualitätsanforderungen an die KPIs (Key Performance Indicators). Wir können also relativ frei definieren, welche KPIs wir ansetzen wollen. Sie müssen für den Prüfer nur sinnvoll und nachvollziehbar sein."

Keine Angst vor Daumenschrauben: ISO 27001 berücksichtigt Individualität

Die ISO 27001 hat den großen Vorteil, dass sie sich an die Organisation und Struktur der einzelnen Unternehmen anpasst. Gerhäuser bemerkt: *„Es ist ganz wichtig zu verstehen, dass die Norm nicht etwas sein soll, was das Unternehmen in seinem Tun begrenzt. Man sollte immer erst analysieren, wie das Unternehmen agiert. Man muss sich fragen: Wie passt die Norm tatsächlich auf das Unternehmen? Was ist der Mehrwert davon?"* Für Michael Kirsch, Leiter der Geschäftsfeldentwicklung bei der ICS AG, ist die ISO 27001 wie ein Rezept zu verstehen: *„Die Norm bietet alle Zutaten, um die Informationssicherheit in einem Unternehmen zu überprüfen. Wenn alles stimmt, kann auch nichts mehr schief gehen",* weiß er.

Jede Firma kann Bereiche ausschließen, die für sie nicht von Belang sind. Das geht allerdings nur mit einer schlüssigen Begründung. Ursprünglich hatte die ICS AG das Sicherheitsmanagement der Lieferantenbeziehungen ausgeklammert, weil sie der Meinung war, dass dieser Bereich für eine Beratungsfirma nicht zutrifft. Doch als der Auditor vor Ort den Mitarbeiter eines Paketdienstes unbegleitet im Firmensitz antraf, war er wenig begeistert. Sein Einwurf war: Wie wird sichergestellt, dass der Lieferant nicht an Informationen kommt, an die er eigentlich nicht kommen darf? „*Da war für uns klar, dass wir diesen Bereich doch betrachten müssen"*, gesteht Gerhäuser.

Hauptabweichung, Nebenabweichung, Empfehlung? Nacharbeitung ist Pflicht

Der Prüfer stellte für den Lieferantenbereich eine so genannte Nebenabweichung fest. Dürr erläutert: *„Bei einer Nebenabweichung bekommt man das Zertifikat dennoch. Man muss aber im Überwachungsaudit nachweisen, dass man hier nachgearbeitet hat."*

Bei einer Hauptabweichung sind weder Prüfer noch die Norm kulant. Gerhäuser berichtet: *„Bei der Definition des Geltungsbereichs hatten wir nicht alle nötigen Punkte identifiziert. Das hat unser Auditor als harte Abweichung, also als Hauptabweichung eingestuft. Für die Nacharbeitung dieses Punktes mussten wir die Ziele definieren und die Erfüllung innerhalb von drei Monaten nachweisen."* Bei nicht rechtzeitiger Erfüllung einer Hauptabweichung verweigert der Prüfer das Zertifikat.

Zusätzlich kann der Prüfer Empfehlungen aussprechen. Sie haben die Funktion eines gut gemeinten Tipps, da sie nicht dokumentiert und nur verbal ausgesprochen werden. Sie stellen somit keine Abweichung dar. „Dennoch sollte man zeigen, dass man den Prüfer und seine Anmerkungen ernst nimmt", rät Michael Kirsch. *„Im jährlichen Überwachungsaudit muss dann auch der Fortschritt entsprechend nachgewiesen werden",* so Kirsch.

Und täglich grüßt das Murmeltier: jährliche Überwachungsaudits zur Qualitätskontrolle

Eine Zertifizierung nach ISO 27001 endet nicht mit dem Erhalt der Urkunde, da sie einen standardisierten Prozess zur ständigen Qualitätskontrolle vorsieht. Ein Jahr nach Erhalt der Zertifizierung gibt es ein Überwachungsaudit. Nach dem zweiten Jahr folgt ein weiteres Überwachungsaudit und nach dem dritten Jahr die Rezertifizierung. *„Das heißt, dass wir laufend kontrolliert werden. Somit wird gewährleistet, dass wir auch umsetzen, was wir definiert haben“,* erläutert Gerhäuser.

Der Kontakt mit dem Auditor (Prüfer) war entspannter, als Dürr und Gerhäuser erwartet hatten. *„Es ist wichtig, erst mal eine entspannte und vertrauensvolle Atmosphäre zu schaffen“*, rät Gerhäuser und fügt hinzu: *„Es ist ganz wichtig, dass man dem Auditor nichts vormacht, was man nicht nachweisen kann. Das kommt nicht gut an.“* Der Prüfer ist in erster Linie daran interessiert, das Unternehmen kennenzulernen. Nur so kann er schließlich einschätzen, ob es sich auf dem richtigen Weg befindet.

Die Prüfung der ICS AG unterlag allerdings einer besonderen Situation: Die Zertifizierungsstelle des Auditors wurde von der Deutsche Akkreditierungsstelle (DAkkS) geprüft, um seine Akkreditierung zu erhalten. *„Davor hatten wir ein wenig Angst und es war für uns auch mit erhöhtem Aufwand verbunden“,* gesteht Gerhäuser und fügt hinzu: *„Wenn einer von der DAkkS anwesend ist, gräbt der Prüfer natürlich in jedem Eckchen.“*

Augen auf bei der Beraterwahl: Falsche Prognosen führen zu Mehraufwand

Trotz guter Vorbereitung und entspannter Atmosphäre gab es für die Stuttgarter doch eine Überraschung. *„Wir hatten im Vorfeld drei Berater im Haus“,* berichtet Gerhäuser. Die Berater unterstützen das Unternehmen dabei, die Anforderungen der ISO 27001 individuell und korrekt zu interpretieren. Doch auch Berater sind nicht unfehlbar, darum sollte man bei der Wahl genau hinschauen. Gerhäuser erzählt: *„Die hatten uns attestiert, dass wir die Norm zu 95% erfüllen. Im Audit hat sich dann aber herausgestellt, dass wir bei Weitem nicht so weit sind, sondern dass wir nur zu 50% fertig sind. Das hat uns doch überrascht.“*

Der Aufwand, um die fehlenden Prozesse nachzuarbeiten, war dann auch entsprechend hoch. Dürr gesteht: *„Bei uns hat es hauptsächlich an der Dokumentation gelegen.“* Wenn die Dokumentation einmal vollständig und in einem vernünftigen Rahmen aufgesetzt ist, bleibt der Aufwand für die zukünftigen Überprüfungen und Anpassungen gering.

Sensibilisierung der Mitarbeiter ist der beste Hacker-Schutz

Bei den Vorbereitungen zum Audit waren ausgesuchte Personen der jeweiligen Business Units, aber auch das komplette Management und der IT-Service beteiligt. Die ISO 27001 deckt schließlich nicht nur die technische Seite ab, sondern befasst sich vor allem mit organisatorischen Maßnahmen zur Sicherstellung der Informationssicherheit.

Doch wie holt man die Mitarbeiter mit ins Boot, wenn es darum geht, möglicherweise unpopuläre Maßnahmen in den Arbeitsalltag zu integrieren? Gerhäuser rät: „*Zunächst einmal muss man*

gegenüber den Mitarbeitern kommunizieren, dass die ISO 27001 kein Hemmschuh für das Unternehmen ist, sondern eine Bereicherung zur weiteren Qualitätssicherung darstellt.“ Dürr ergänzt: *„Das erreicht man eigentlich ganz gut, indem man effiziente Prozesse organisiert, die keinen hohen Organisationsaufwand bedeuten, sondern die im täglichen Umgang gut handhabbar sind.“*

Wie von der Norm gefordert, legte die ICS AG ihren Mitarbeitern eine Informationssicherheitsleitlinie vor. *„Das Dokument sah auf den ersten Blick wohl etwas schwierig aus“,* weiß Dürr. *„Aber dann haben wir Awarenss-Schulungen durchgeführt und so das Dokument für die Mitarbeiter verständlich gemacht. Wir haben sie damit auf den neuesten Stand gebracht und auf tägliche Stolperfallen hingewiesen, wodurch die Informationssicherheit gefährdet werden könnte.“*

Zertifikat mit Außenwirkung liefert klare Wettbewerbsvorteile

Fühlt man sich denn sicherer, wenn man die Zertifizierung hat? Dürr sagt: *„Das Zertifikat selbst ist eher etwas für die Außenwirkung. Damit können wir zeigen, dass wir funktionierende Prozesse aufgesetzt haben, die unsere Informationssicherheit gewährleisten. Was uns aber Sicherheit gibt, ist, dass wir jetzt wissen, wie wir mit unseren Prozessen umgehen und wie sie gelebt werden. Man gewinnt auch grundsätzlich einen guten Blick für das Delta zwischen dem was man für die Sicherheit tun kann und was bisher getan worden ist.“*

Die mit dem ISMS nach ISO 27001 implementierten Sicherheitsstandards sind Teil der neuen europäischen Datenschutzgrundverordnung (EU-DSGVO). Für immer mehr Auftraggeber sind genau diese Sicherheitsstandards bei der Auftragsvergabe entscheidend. Diese Erfahrung haben auch die Sicherheitsexperten der ICS AG gemacht. Kurz nachdem die Zertifizierung abgeschlossen war, erhielten sie von zwei ihrer wichtigsten Kunden AV-Verträge (Auftragsverarbeitung) und Fragebögen zugeschickt, in denen Maßnahmen und Prozesse der Informationssicherheit abgefragt wurden. *„Da konnten wir mit ruhigem Gewissen auf die Inhalte der ISO 27001 verweisen und ziemlich schnell wieder zum Tagesgeschäft übergehen*“, freut sich Michael Kirsch. Der Aufwand hat sich also auf jeden Fall jetzt schon gelohnt.

Das Interview führte Julia Grewe.

(Autor: Julia Grewe)

Pressemitteilung

Über die ICS AG:

Die ICS AG ist seit mehr als 50 Jahren ein erfolgreiches, familiengeführtes IT-Beratungs- und Engineering-Unternehmen.

Die Spezialisierung liegt in den Geschäftsfeldern Industrial Engineering (Automation, Supply Chain, Logistic, Automotive), Transportation und den Bereichen Funktionale Sicherheit, Security & Safety sowie Informationssicherheit und DSGVO.

Weitere Informationen unter www.ics-ag.de.

https://www.einfach-sicher.info

Pressekontakt:	**Fachlicher Kontakt**
ICS AG Marketing & PR Stefanie Henzler Sonnenbergstraße 13 70184 Stuttgart Tel.: +49 711 21037 – 40 Web: www.ics-ag.de E-Mail: presse@ics-ag.de	ICS AG Informationssicherheit Martin Tege – Vertriebsleiter Sonnenbergstraße 13 70184 Stuttgart Tel.: +49 711 21037 – 00 Web: www.ics-ag.de E-Mail: einfachsicher@ics-ag.de