ISO 27001 in mittelständischen Unternehmen

- **Starkes Signal für Vertrauen und ein Plus im Wettbewerb**
- **Synergien mit ITIL, ISO 20000 und ISO 9001**
- **Riskmanagement, Mitarbeiter-Awareness, Standardisierung**

Fotocredit: Anna Rauchenberger

„ISO 27001 ist größenunabhängig anwendbar. Mittels Risikoanalyse ergibt sich der individuelle Handlungsbedarf. So profitieren die Unternehmen von einem schlanken, effektiven System."

Erich Scheiber,
CIS-Geschäftsführung

Der Markt spricht eine klare Sprache: Nachweise für Informationssicherheit werden von immer mehr Kunden explizit gefordert. Wie sich der internationale Security-Standard ISO 27001 in mittelständischen Unternehmen effizient umsetzen lässt, zeigen drei Fallbeispiele: Danube IT Services, Fabasoft und POOL4TOOL wurden erfolgreich nach ISO 27001 zertifiziert und berichten über ihren Weg von der Implementierung zum Zertifikat. ISO 27001 ist größenunabhängig anwendbar: Mittels Risikoanalyse ergibt sich der individuelle Handlungsbedarf. So profitieren die Unternehmen von einem schlanken, effektiven System.

Informationssicherheit wird von immer mehr Kunden explizit gefordert

Fotocredit: istockphoto Photomorphic

Firmenprofil:
Die Danube IT Services GmbH in Wien beschäftigt 50 Mitarbeiter und bietet IT-Dienstleistungen mit den Schwerpunkten Rechenzentrum, Private Cloud und Managed Services an. Sicherheit und Vertraulichkeit haben höchste Priorität, denn ein strategischer Markt ist der Finanzsektor mit anspruchsvollen Kunden wie Banken, Versicherungen oder Leasing-Gesellschaften.

Fotocredit: beigestellt von Danube IT Services

Im Interview:
Geschäftsführer:
Johann Ehm

- **Herr Ehm, was waren Motive für die Einführung von Informationssicherheit nach dem internationalen Standard ISO 27001?**

  „Sicherheit steht für uns an erster Stelle, denn unsere Kunden vertrauen darauf, dass wir ein hochsicheres Rechenzentrum bertreiben. Die Zertifizierung nach ISO 27001 ist ein sichtbarer Nachweis dafür. Zudem verlangen einige Unternehmen das Zertifikat bei Ausschreibungen, insbesondere im Finanzdienstleistungsbereich."

- **Welchen internen Nutzen zieht das Unternehmen aus ISO 27001?**

  „Aus interner Sicht war unser Ziel, dass alle Prozesse dokumentiert sein müssen. Anhand der ISO 27001 konnten wir wichtige Prozesse wie das Change Management formalisieren, was zwar einen Mehraufwand für die Mitarbeiter bedeutet – weil jede Änderungen dokumentiert werden muss, aber was auch einen deutlichen Qualitätsgewinn für das Unternehmen bringt. Fehler, Sicherheitsvorfälle und **System-Ausfälle werden minimiert.** Alle Änderungen vom neuen User bis zur neuen Software sind nun verbindlich geregelt. Diese Nachvollziehbarkeit ist ein großer Vorteil hinsichtlich Einhaltung von Service-Verträgen und Haftung, denn Fahrlässigkeit ist damit praktisch ausgeschlossen."

- **Stichwort Scoping: Wurde nur die IT oder das ganze Unternehmen zertifiziert?**

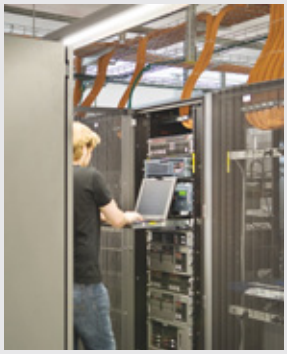
  „Zum zertifizierten Bereich zählt das gesamte Unternehmen einschließlich Rechnungswesen, **Marketing und Vertrieb.** Der sichere Umgang mit Daten ist für jede Abteilung wichtig, vor allem auch die Sensibilisierung aller Mitarbeiter bis hin zur Raumpflegerin. Die Wichtigkeit der Informationssicherheit im ganzen Unternehmen umfasst Aspekte wie Business Continuity, Legal Compliance oder die Nutzung von Mobile Devices, Email, Internet und Social Media."

- **Welche Strategie haben Sie für Implementierung und Zertifizierung verfolgt?**

  „Für die Implementierung wurde unser Chief Information Security Officer eingesetzt, der im Ausmaß einer Teilzeitbeschäftigung nur für die Informationssicherheit zuständig ist. Nach einer Gap-Analyse stellte er fest, dass wir bereits **80 Prozent der Security-Anforderungen** gemäß ISO 27001 erfüllt hatten. In einem Zeitraum von knapp 1,5 Jahren wurde dann Schritt für Schritt das Informationssicherheits-Managementsystem (ISMS) bis zur Zertifizierungsreife aufgebaut. Riskmanagement, Dokumentation, Policies und Mitarbeiter-Awareness waren dabei die großen Themenfelder."

Fotocredit: iStock nmcandre

„Fehler sollen gemeldet werden - nicht um persönliches Verschulden zu betonen, sondern um die Prozesse zu optimieren."



Fotocredit: beigestellt von Danube IT Services

Für jede Berufsgruppe, vom IT-Admin bis zum Top-Management, gibt es praktikable Security-Richtlinien.

- **Haben Sie einen Tipp für die Implementierung?**

  „Das wichtigste ist, die Mitarbeiter von vorn herein einzubeziehen. Das Management sollte von Anfang an klar kommunizieren, dass ein zertifiziertes Security-System einen großen Nutzen bringt und die **Arbeitsplätze langfristig sichert.** Wir haben generell einmal pro Monat ein Meeting mit allen Mitarbeitern. Diese Plattform habe ich als Geschäftsführer gezielt genutzt, um das Thema Informationssicherheit immer wieder zu positionieren."

- **Waren definierte Prozesse im Unternehmen vorhanden?**

  „Seit der Unternehmensgründung im Jahr 2007 wurden alle IT-Services nach ITIL, der IT Infrastructure Library, aufgebaut. Viele Prozesse daraus überschneiden sich mit den Anforderungen der ISO 27001. Dazu gehören Change, Configuration, **Incident und Problem Management** oder Desaster Recovery. Wir konnten das ISMS daher auf vorhandenen Abläufen aufsetzen und Synergien nutzen."

- **Wie motivieren Sie Ihre Mitarbeiter, Policies und Richtlinien im Alltag umzusetzen?**

  „Wir pflegen eine ‚offene Fehlerkultur.' Security-relevante Fehler – vom Sicherheitsvorfall über menschliches Versagen bis hin zu Hard- oder Softwarefehlern – sollen umgehend gemeldet werden, aber nicht um persönliches Verschulden zu betonen, sondern um die dahinterliegenden Prozesse zu optimieren. Daher sammeln wir die **Meldungen unserer Mitarbeiter** und lassen diese geordnet in den kontinuierlichen Verbesserungsprozess einfließen. Darüber hinaus haben wir alle sechs Monate eine Awareness-Veranstaltung, in denen aktuelle Datenverlust- und Spionagefälle aus den Medien präsentieret werden, um wieder aufzurütteln und das Sicherheitshandbuch gemeinsam durchzugehen."

- **Arbeiten Sie mit positionsbezogenen Security-Richtlinien?**

  „Ja, in der Kürze liegt die Würze! Für jede Berufsgruppe vom IT-Administrator bis zum Top Management gibt es praktikable Security-Richtlinien. So haben wir etwa für den Vertrieb eine eigene **Security-bezogene Prozessdarstellung** erarbeitet, die Sicherheitsanforderungen von der Angebotserstellung bis zur Annahme beschreibt. Dabei sollten Richtlinien und Policies generell nicht zu starr sein, sonst weichen die Leute aus. Lebbare Prozesse konnten wir durch Einbeziehung aller Mitarbeiter implementieren."

- **Welches abschließende Resümee geben Sie?**

  „Manche Unternehmen denken zunächst, dass Informationssicherheit vor allem Geld kostet. Wir sind aber überzeugt, dass sauber aufgesetzte Security-Prozesse langfristig einen Gewinn bringen. Am Leben gehalten wird das System durch die Zertifizierung, weil die Mitarbeiter motiviert sind. Insgesamt soll und kann ein ISMS rentabel sein."

Firmenprofil:
Fabasoft ist ein führender europäischer Softwarehersteller und Cloud-Anbieter mit 200 Mitarbeitern am Hauptsitz in Linz. Die Softwareprodukte und Cloud-Dienste von Fabasoft sorgen für das einheitliche Erfassen, Ordnen und Aufbewahren aller digitalen Geschäftsunterlagen im Unternehmen (Enterprise Content Management). Auf dieser Basis beschleunigen sie die vollständige Digitalisierung von Businessprozessen.


Fotocredit: beigestellt von Fabasoft

Im Interview:
Quality-und Information-Security-Manager Magdalena Moser

- **Frau Moser, was waren die Motive für die ISMS-Einführung nach ISO 27001?**

  „Als Dienstleister halten wir sensible und geschäftsrelevante Daten von Kunden. Diese gilt es zu schützen – nachweisbar, mittels Zertifizierung. Vertrauliches Papier kann man im Tresor lagern. Für komplexen Datenschutz mit digitalen, analogen und mentalen Informationen wirkt ISO 27001 wie ein Tresor – ein **wirksames System mit Struktur** und Kontrollmechanismen. Das Zertifikat ist auch eine wichtige Grundlage für unsere Dienstleistungen im Bereich Cloud Computing und Software-as-a-Service (SaaS).“

- **Welcher Bereich des Unternehmens wurde zertifiziert?**

  „Die ISO-27001-Zertifizierung wurde für den Hauptstandort in Linz durchgeführt. Geplant ist bei der nächsten Re-Zertifizierung eine **Erweiterung auf alle Niederlassungen.** Zusätzlich zu der seit 2008 bestehenden ISO-27001-Zertifizierung sind die Produkte Fabasoft Folio Cloud und Fabasoft Folio SaaS nach ISO 20000-1 zertifiziert. Beide haben ihre IT-Sicherheitsschwerpunkte und wirken in Kombination am stärksten.“

- **Welche Wettbewerbsvorteile lukrieren Sie aus dem Zertifikat?**

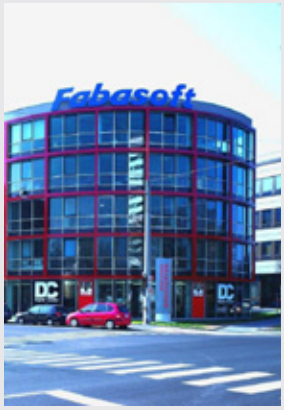
  „Die ISO-27001-Zertifizierung ist ein anerkannter Standard für Informationssicherheit. Wir zeigen damit unseren Kunden, dass die Sicherheit ihrer Daten für uns oberste Priorität hat. Mit den Zertifizierungen **setzen wir ein Zeichen** und präsentieren diese auf unseren Webseiten, auf Kundenevents und legen diese bei Ausschreibungen bei. Sie sind für unsere Kunden ein Nachweis über den erreichten Grad an IT-Sicherheit durch eine vertrauenswürdige und unabhängige Instanz. Die CIS als Zertifizierungsgesellschaft hat aufgrund ihrer profunden Expertise ein sehr gutes Renommee in der Branche.“

- **Waren definierte Prozesse vorhanden oder war dieser Schritt Neuland?**

  „Wir sind konzernweit nach ISO 9001 zertifiziert und haben ISO 27001 und ISO 20000-1 dadurch auch leichter integrieren können. Die geforderten IT- und Security-Prozesse waren bereits definiert. Wir haben die Anforderungen der ISO 27001 großteils schon gelebt, daher war es ein logischer Schritt, dies mit einer Zertifizierung sichtbar zu machen. Wir konnten das gesamte System ohne Berater innerhalb von acht Monaten implementieren.“

Fotocredit: istockphoto andipantz

„ISO 27001 wirkt wie ein ‚Tresor' für komplexen Datenschutz: mit digitalen, analogen und mentalen Informationen – zentral, lokal, mobil und in den Köpfen der Mitarbeiter gespeichert."



Fotocredit: beigestellt von Fabasoft

■ **Welche Punkte mussten neu erarbeitet werden?**

„Dokumentation und Handbuch wurden verfeinert. Ein spannender Aspekt war die Mitarbeiter-Awareness, wobei unser Vorstand durch Begeisterung und Engagement für das Thema eine **große Vorbildwirkung** hat. Neue Mitarbeiter durchlaufen unsere Academy, wo Informationssicherheit ein fester Bestandteil geworden ist. Weiters wurde eine Informationssicherheitsvereinbarung veröffentlicht und von jedem Mitarbeiter unterzeichnet. Dies hat stark zu Diskussionen angeregt und so half uns die Mundpropaganda bei der Awareness-Bildung."

■ **Wie haben Sie Risikomanagement nach ISO 27001 umgesetzt?**

Die große Herausforderung war, Risiken und Maßnahmen zusammenzuführen. Es galt, die vorhandenen „Puzzleteile" systematisch zu erfassen. Dadurch erhielten wir einen wertvollen Gesamtüberblick und konnten sicher sein, **kein Risiko zu übersehen** und keine Doubletten mitzutragen. Als sinnvoller Erstellungsprozess hat sich herauskristallisiert: Risiken schriftlich erfassen, diskutieren, kürzen. Dann erst Maßnahmen definieren. So verhindert man ein Überladen des Systems."

■ **Welche Methode haben Sie für die Risikoanalyse verwendet?**

„Die qualitative Methode ALARP. Diese hat uns aufgrund ihres einfachen Ansatzes überzeugt. In der Formel ‚Eintrittswahrscheinlichkeit x Auswirkung = Risiko' werden keine monetären Werte eingesetzt, was bei Imageschaden schwierig wäre, sondern, Schulnoten. Die Ergebnisse werden grafisch als Matrix nach dem Ampelsystem rot-grün-gelb dargestellt. Um die Maßnahmenwirksamkeit messen zu können, haben wir unser strategisches Kennzahlensystem direkt mit dem Risikomanagement verknüpft."

■ **Haben Sie einen Tipp für die Implementierung von ISO 27001?**

„Zeitpuffer einplanen und immer wieder einen Schritt zurückzugehen, um das System als Ganzes zu betrachten. Die Gratwanderung bewegt sich zwischen: **So viel wie notwendig,** so wenig wie möglich. Ein überladenes System wird in der Praxis nicht gelebt. Das System muss schlank und effizient sein."

Firmenprofil:
Die POOL4TOOL AG ist ein SaaS-Spezialist im SAP-Umfeld mit Sitz in Wien und über 80 Mitarbeitern an insgesamt 6 Standorten in Europa, Asien und Amerika. Das Produktportfolio unterstützt die Prozesskette von der Produktentstehung über den strategischen und operativen Einkauf bis hin zur EDI-Kommunikation mit den Lieferanten sowie die globale Produktkosten-Kalkulation.

Fotocredit: beigestellt von POOL4TOOL

Im Interview:
Chief Technical Officer
Michael Rösch

- **Herr Rösch, was waren die Motive für die Einführung von Informationssicherheit nach ISO 27001?**

  „Informationssicherheit ist für uns als Anbieter webbasierter Mietsoftware ein Business Need und nicht nur in der Automobilindustrie hochaktuell. Einer unserer Kunden, ein großes Zulieferunternehmen, verlangte explizit eine Zertifizierung nach ISO 27001 – vorausschauend, während er selbst noch vor der Implementierung stand. "

- **Waren definierte Prozesse vorhanden oder war dieser Schritt Neuland?**

  „Die Implementierung gestaltete sich leichter und schneller als erwartet. Vor allem, weil wir aufgrund unserer Geschäftsbeziehung zu einem US-börsennotierten Unternehmen bereits SOX-konforme Prozesse im Hause hatten. Die **Anforderungen von ISO 27001** und Sarbanes Oxley überschneiden sich inhaltlich, daher konnten wir die Implementierung der ISO 27001 direkt auf den bereits definierten Prozessen aufsetzen."

- **Welche Strategie haben Sie für Implementierung und Zertifizierung verfolgt?**

  „Zur effizienten Umsetzung des Standards haben wir einen Berater hinzugezogen: Die Analyse der Prozesse, das Überarbeiten der Dokumentation, die Durchführung einer Risikoanalyse sowie die Klassifizierung von Dokumenten haben wir mit externer Hilfe umgesetzt. So konnten wir die **Implementierung innerhalb eines halben Jahres** bewältigen. Zertifiziert wurde der gesamte Standort Wien mit Software-Entwicklung, Support und Administration.
  Als **Vorbereitung für das Zertifizierungsaudit** haben wir ein Stage Review der CIS in Anspruch genommen. Die Zertifizierung im ersten Anlauf zu erlangen, ist überaus wichtig für die Motivation der Mitarbeiter, die das System dauerhaft ‚leben' sollen."

- **Welchen internen Nutzen zieht das Unternehmen aus ISO 27001?**

  „Die lückenlose Dokumentation aller Prozesse schafft Transparenz für das gesamte Unternehmen. Heikle Fragen wie die Vorgehensweise beim Ausscheiden von Mitarbeitern sind damit klar geregelt. Durch das **Incident- und Change Management** im Rahmen der ISO 27001 haben wir unsere Support-Prozesse verbessert und sämtliche dahinterliegende Workflows sowie den Einsatz von Trouble Tickets optimiert. So profitieren wir von der gesteigerten Effizienz und den klaren Abläufen. Unsere Kunden spüren dies in Form kürzerer Reaktions- und Durchlaufzeiten bei der Anfragebearbeitung. Daher war es uns auch wichtig, die Einführung der ISO 27001 mit einem Zertifikat zu besiegeln, um die interne Optimierung unserer Prozesse auch für unsere Kunden sichtbar zu machen."

Fotocredit: iStockphoto Shapecharge

„Durch Incident- und Change Management nach ISO 27001 haben wir Support-Prozesse sowie den Einsatz von Trouble Tickets verbessert. Unsere Kunden spüren dies in Form kürzerer Anfragebearbeitung."

- **Und die Vorteile gegenüber dem Mitbewerb?**

  „Standardisierte Prozesse, anerkannt und geprüft durch die unabhängige Zertifizierungsorganisation CIS, sind ein handfester **Wettbewerbsvorteil am Markt:** Die Nachfrage von Seiten unserer Kunden nach einer ISO 27001-Zertifizierung ist im vergangenen Jahr deutlich gestiegen. Das Zertifikat vermittelt unseren Kunden die Sicherheit, einen verlässlichen Partner zu haben."

- **Wie haben Sie Risikomanagement nach ISO 27001 umgesetzt?**

  „Der Bereich Risikomanagement war Neuland für uns, so dass wir diesen Aspekt mit einem Berater als Coach umgesetzt haben. Die **Schwerpunkte lagen dabei** vor allem auf Vertragsthemen, Haftungsfragen und weiteren juristischen Belangen, denn Ausfallsicherheit war bereits durch die SOX-Anforderungen abgedeckt."

- **Ist auch eine ISO-20000-Zertifizierung geplant?**

  „Ja, diese ist in Planung. Und zwar als integriertes System mit ISO 27001, um Synergien im Betrieb bis hin zu Kombinationsaudits nutzen zu können. POOL4TOOL bildet bereits ITIL- konforme Prozesse über das eigene Ticketing Modul ab. ISO 20000 ermöglicht es, die **ITIL-Konformität mittels Zertifikat** nachzuweisen. Daher streben wir eine Zertifizierung nach ISO 20000 an – ein weiterer Wettbewerbsvorsprung im internationalen Konkurrenzkampf."

Fotocredit: beigestellt von POOL4TOOL

Fotocredit: iStockphoto nico - blue

Das Zertifikat macht Wettbewerbsvorsprung sichtbar

Fotocredit: Anna Rauchberger

Von der Implementierung zum Zertifikat

- **Informationssicherheit nach ISO 27001**
- **IT-Service-Management nach ISO 20000**

Informationsgespräch
CIS-Erstgespräch: Details zum Zertifizierungsprozess. Dann Registrierung, Projektplanung.

Analyse
Interne Evaluierung des Verbesserungspotentials, Bewertung vorhandener Maßnahmen.*

Implementierung
Maßnahmenumsetzung nach ISO 27001 und/oder ISO 20000 im Unternehmen.*

*Die CIS als unabhängige Prüfstelle ist nicht involviert

CIS Stage Review (Vorbeurteilung)
Optional: Projektbegleitende Prüfung der implementierten Elemente durch CIS-Auditoren.

CIS System & Risk Review (Vorbegutachtung)
CIS prüft die Interpretation der Normforderungen und Dokumentation, „Generalprobe".

CIS Certification Audit
Überprüfung des Systems durch multiple Stichproben. Auditbericht mit zukünftigem Verbesserungspotenzial. Das CIS-Zertifikat nach ISO 27001 / ISO 20000 gilt 3 Jahre.

CIS Surveillance Audit
Das einmal pro Jahr durchgeführte Surveillance Audit überprüft die Effektivität des gesamten Managementsystems sowie seine ständige Verbesserung.

CIS Recertification Audit
Nach 3 Jahren haben Sie die Möglichkeit, das abgelaufene Zertifikat erfolgreich zu erneuern.

CIS - Certification & Information Security Services GmbH · A - 1010 Wien · Salztorgasse 2/6/14 A · T: +43 (0)1 532 98 90, F: +43 (0)1 532 98 90 109 · office@cis-cert.com · www.cis-cert.com