Hybrider Ansatz für eine risikobasierte Informationssicherheit

Wie die Amadeus FiRe AG mit den IT-Grundschutz-Empfehlungen des BSI den Grundstein für eine systematische IT-Security legte – und dieses Fundament als Sprungbrett für die ISO 27001-Zertifizierung nutzte.

Als Personaldienstleister managt und verarbeitet die Amadeus FiRe AG täglich hochsensible personenbezogene Daten ihrer Bewerber, Mitarbeiter, Kunden und Schulungsteilnehmer – und muss in diesem streng reglementierten Umfeld ein Höchstmaß an Sorgfalt, Sicherheit und Compliance gewährleisten. Daher hat das Unternehmen schon vor Jahren mit einer Zertifizierung nach der international anerkannten Norm für Qualitätsmanagement ISO 9001 und der Umsetzung eines ganzheitlichen Sicherheitskonzepts auf der Basis der IT-Grundschutz-Vorgaben den Grundstein für eine Systematisierung seiner Informationssicherheit gelegt. Im Jahr 2020 nahm das Team dann gemeinsam mit der Networkers AG den nächsten Meilenstein in Angriff: die anspruchsvolle Zertifizierung nach ISO 27001.

Über Amadeus FiRe

Die Amadeus FiRe AG ist seit mehr als 35 Jahren der spezialisierte Personaldienstleister für Zeitarbeit, Personalvermittlung und Interim Management im kaufmännischen und IT-Bereich. Im Sektor der Personaldienstleistungen und der beruflichen Weiterbildung ist die Amadeus FiRe-Gruppe mit weit über 100 Niederlassungen bundesweit vertreten und mit dem lokalen Kandidaten- und Arbeitsmarkt bestens vertraut. Zusammen mit den konzerneigenen Fort- und Weiterbildungsinstituten bietet das Unternehmen Bewerbern, Mitarbeitern, Unternehmenskunden sowie Schulungs- und Seminarteilnehmern ein exklusives, ineinandergreifendes Dienstleistungsportfolio. Auf diese Weise entstehen einzigartige Synergien und neue Karriereperspektiven. Dabei setzt die Amadeus FiRe Gruppe stets auf nachhaltige und langfristige Partnerschaften mit den Menschen, mit denen sie zusammenarbeitet. Diese wiederum profitieren von einer zielführenden Begleitung und Unterstützung.

www.amadeus-fire.de

Networkers AG • Bandstahlstraße 2 • 58093 Hagen
Fon: +49 2331 8095 - 0 • Mail: sales@networkers.de
www.networkers.de

Seit dem Inkrafttreten der Datenschutzgrundverordnung (DSGVO) im Mai 2018 stehen Unternehmen unter hohem Druck, personenbezogene Daten standardisiert und risikobasiert zu schützen. Viele Betriebe nehmen dies zum Anlass, ihr unternehmensweites Informationssicherheitsmanagement zu systematisieren – und entscheiden sich dabei für einen von zwei Ansätzen: Entweder orientieren sie sich an den Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und setzen ihre Informationssicherheit auf der Basis des IT-Grundschutz-Kompendiums auf, um ein angemessenes Schutzniveau zu gewährleisten. Oder sie implementieren ein ganzheitliches Informationssicherheitsmanagementsystem (ISMS) und etablieren mit der ISO 27001 eine High-Level-Struktur für die Systematisierung der Informationssicherheit. Die Themen Sicherheit und Datenschutz werden damit nachhaltig in die Arbeitsabläufe integriert.

Zwei Modelle, kein Königsweg

Beide Ansätze haben zweifellos ihre Daseinsberechtigung und helfen Unternehmen dabei, kritische und sensible Daten zuverlässig zu schützen. Die Erfahrung zeigt aber auch, dass in der Praxis beide Methoden ihre Tücken haben, wie Jürgen Sonsalla, Senior Consultant und Co-Team Leader Security Services, bestätigt:

„Wer sich bei der Informationssicherheit ausschließlich auf die Vorgaben des IT-Grundschutzes verlässt, wird bei entsprechender Skalierung – etwa, wenn er neue Geschäftsbereiche integriert, ins Ausland expandiert oder in besonders streng regulierten Märkten Fuß fassen möchte – über kurz oder lang den robusten High-Level-Unterbau und das internationale Standing des DIN ISO-Standards vermissen. Und auf der anderen Seite gibt es immer wieder Unternehmen, die mit viel Eifer und Begeisterung ihre ISO 27001 Zertifizierung angehen, sich dann aber im administrativen Klein-Klein verlieren, statt die Umsetzung der erforderlichen technischen und organisatorischen Maßnahmen voranzutreiben. Die Herausforderung liegt darin, den für das jeweilige Unternehmen passenden Weg zu finden – und langfristig in den Arbeitsalltag zu integrieren.“

Kurz: Die Wahl zwischen dem IT-Grundschutz des BSI und der Zertifizierung gemäß ISO 27001 ist wegweisend, aber auch alles andere als einfach. Eine spannende Alternative zeigt das Beispiel der Amadeus FiRe AG, die sich eben nicht zwischen den beiden Ansätzen entschied, sondern einen smarten hybriden Ansatz wählte – und sich so das Beste aus beiden Welten sicherte.

Elmar Roth
Bereichsleitung Informationstechnologie
Amadeus FiRe

„Die Sicherheit unserer digitalen Assets hatte für uns schon immer höchste Priorität: Schließlich managen wir als Personaldienstleister für Kunden, Bewerber und Mitarbeiter Unmengen hochsensibler Daten, die auf keinen Fall kompromittiert werden dürfen. Ein Data Breach wäre für uns in mehr als einer Hinsicht existenzbedrohend – sowohl mit Blick auf die Folgekosten eines solchen Angriffs, als auch mit Blick auf den enormen Vertrauensverlust“, erklärt Elmar Roth, Bereichsleitung Informationstechnologie bei Amadeus FiRe. „Die Absicherung nach dem vom BSI herausgegebenen IT-Grundschutz-Kompendium war für uns als mittelständisches Unternehmen daher lange Zeit ein hervorragender Leitfaden, um einen methodischen und angemessenen Schutz unserer Anwender, Daten und Systeme sicherzustellen. Wir haben das Regelwerk gemeinsam mit der Networkers AG vor einigen Jahren implementiert, um ein robustes Fundament für unsere Informationssicherheit zu legen, unsere Prozesse zu optimieren und die Weichen für eine kontinuierliche Verbesserung zu stellen. Und das hat auch wunderbar funktioniert.“

IT-Grundschutz

Das vom Bundesamt für Sicherheit in der Informationstechnik herausgegebene IT-Grundschutz-Kompendium ist die grundlegende Veröffentlichung des IT-Grundschutzes. Zusammen mit den BSI-Standards bildet es die Basis für alle, die sich umfassend mit dem Thema Informationssicherheit befassen möchten. Anhand der sogenannten IT-Grundschutz-Bausteine beleuchtet es die relevanten Sicherheitsaspekte der IT, erläutert Gefährdungen, definiert Sicherheitsanforderungen und gibt Hinweise zur Umsetzung von Schutzmaßnahmen.

Pragmatischer Ansatz mit Ablaufdatum

So erfolgreich der pragmatische Ansatz aber auch war, wusste das Team von Anfang an, dass das relativ statische Regelwerk des BSI in der dynamischen IT-Infrastruktur mit der Zeit an seine Grenzen stoßen würde. Dies gilt umso mehr, als die Vorgaben nur bedingt geeignet sind, um auf Dauer mit sich verändernden Bedrohungslandschaften und zunehmend strengen regulatorischen Bestimmungen Schritt zu halten. Daher hielt sich Amadeus FiRe die Option offen, mittelfristig ein unternehmensweites ISMS zu implementieren, und mit der ISO 27001 Zertifizierung die Weichen für einen international

Networkers AG • Bandstahlstraße 2 • 58093 Hagen
Fon: +49 2331 8095 - 0 • Mail: sales@networkers.de
www.networkers.de

standardisierten Security-Ansatz zu stellen. Ab Mai 2018 wurden die entsprechenden Pläne dann immer konkreter, wie Thorsten Sader, Informationssicherheitsbeauftragter (ISB) bei Amadeus FiRe, erklärt:

Thorsten Sader
Informationssicherheitsbeauftrager
Amadeus FiRe

„Seitens des Gesetzgebers, seitens der internen Stakeholder und seitens der Kunden wuchs der Druck, das Thema Informationssicherheit in eine robuste High-Level-Struktur einzubetten. Unser Ziel war es, unsere Abläufe noch stärker zu systematisieren, klarer zu dokumentieren und nachhaltiger in die Abläufe einzubinden. Auf diese Weise wollten wir auch ein klares Signal nach außen setzen, dass wir das Thema sehr ernst nehmen und mit unseren Maßnahmen auf der Höhe der Zeit sind.“

Startschuss für die ISO-Zertifizierung

Wie bereits bei der Umsetzung der BSI-Empfehlungen zog das Team von Amadeus FiRe auch bei diesem Projekt schon in der Frühphase das Team der Networkers AG hinzu, um gemeinsam die Weichen für eine erfolgreiche ISO 27001 Zertifizierung zu stellen. Deren Consultants waren bestens mit der Infrastruktur vertraut und begleiten seit vielen Jahren ISO 27001 Auditierungen in Unternehmen unterschiedlichster Branchen – und waren somit der perfekte Trusted Advisor für die Planungsphase. Dabei zeichnete sich vom ersten Tag ab, dass Amadeus FiRe in vielerlei Hinsicht enorm vom robusten BSI-Fundament profitieren würde:

Das Team hat im Rahmen der Umsetzung der BSI-Grundschutzvorgaben gelernt, das Thema Informationssicherheit risikoorientiert zu betrachten. Die Verantwortlichen sind es also gewohnt, im ersten Schritt stets die potenziellen Bedrohungsszenarien und deren Eintrittswahrscheinlichkeit zu analysieren. Anschließend gilt es, ausgehend von dieser Risikobewertung das konkrete Schadenspotenzial auf ein angemessenes Maß zu reduzieren. Dieser pragmatische und praxisnahe Ansatz kam auch bei der Einführung eines ISMS nach ISO 27001 zum Tragen.

Die Systematisierung der Informationssicherheit ist ein anspruchsvolles Change-Management-Projekt. Ein solches Projekt wird nur erfolgreich sein, wenn es gelingt, alle relevanten Stakeholder mit Rückendeckung der Geschäftsführung einzubeziehen, unternehmensweit das Bewusstsein für die Security zu schärfen und nachhaltig in die Unternehmensprozesse einzubinden – kurz: Mitarbeiter aller Hierarchieebenen zur Änderung ihres Verhaltens zu bewegen. Auch hier profitierte das Team enorm von den Erfahrungen bei der BSI-Grundschutz-Implementierung.

ISO 27001

Die internationale Norm ISO/IEC 27001 definiert die Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und Verbesserung eines dokumentierten Informationssicherheitsmanagementsystems in Unternehmen. Darüber hinaus umfasst die ISO 27001 konkrete Anforderungen für den Umgang mit IT-Security-Risiken und spezifiziert Anforderungen für die Implementierung geeigneter Sicherheitsmechanismen.

Dank Grundschutz stand Amadeus FiRe nicht unter dem Druck, kurzfristig ihr Security-Standing zu verbessern. Durch die Umsetzung der BSI-Grundschutz-Prinzipien hatte Amadeus FiRe durchgehend die Gewissheit, dass die Daten und Systeme zuverlässig geschützt waren und konnte das Projekt ISO 27001 gelassen angehen.

Ende 2020 nahm das IT-Team von Amadeus FiRe die Vorbereitung der ISO 27001-Auditierung in Angriff. Das Projekt erstreckte sich über vier Phasen:

Phase 1:
Initialisierung

In der ersten Projektphase galt es, die Verantwortlichkeiten, die Ziele und den Umfang des Projekts festzulegen.

Phase 2:
Aufbau der IS-Organisation

Im zweiten Schritt stand die Bereitstellung der Ressourcen, die Schulung der beteiligten Mitarbeiter und die Vorbereitung des Projekt-Frameworks (also etwa die Definition von Dokumentenstandards) im Fokus.

Phase 3:
Implementierung des ISMS

Diese Schlüsselphase begann mit einer detaillierten Bestandsaufnahme und umfassenden Risikoanalysen. Anschließend wurden auf der Basis dieser Bewertungen geeignete Schutzmaßnahmen sowie Prozesse entwickelt und umgesetzt.

Phase 4:
Zertifizierung sowie Aufrechterhaltung und Verbesserung

Nach Abschluss der eigentlichen Zertifizierung galt es, die Weichen

für eine sichere Integration neuer Prozesse und Dienste zu stellen. Dieser zyklische Ansatz ermöglicht es, Sicherheitsmaßnahmen regelmäßig zu prüfen und kontinuierlich zu verbessern.

„Insgesamt nahmen die Implementierung des ISMS und die Vorbereitung der ISO 27001-Auditierung rund acht Monate in Anspruch“, fasst Thorsten Sader das Projekt zusammen. „Dabei haben wir den Aufwand einiger Arbeitsschritte – etwa den der Dokumentenklassifizierung – zunächst deutlich unterschätzt. Hinzu kam Corona und damit die Migration ins Homeoffice und in die Cloud. Das waren zwei dramatische Gamechanger, die die Komplexität des Projekts massiv erhöht haben. Am Ende sind wir dank des engagierten Teams aber doch im Zeitplan geblieben, und haben die Auditierung unserer Frankfurter Zentrale im Oktober 2021 im ersten Anlauf erfolgreich absolviert. Dann folgten in kurzen Abständen die nächsten 5 Standorte. Dabei haben wir vor allem von der standardisierten und skalierbaren Vorgehensweise profitiert, die wir im Alltag als praxisnah und effizient wahrgenommen haben.“

Die ISO 27701-Zertifizierung soll folgen

Im nächsten Schritt plant Amadeus FiRe nun, die Auditierung gemäß ISO 27701 anzugehen. Diese im Jahr 2020 vorgestellte Erweiterung der ISO 27001 fokussiert ganz auf den Datenschutz, ist derzeit allerdings noch nicht zertifizierbar.

Weitere Planungen für die nächsten Monate umfassen die Themen sichere Softwareentwicklung sowie die Optimierung des Notfallmanagements hinsichtlich möglicher Szenarien. ■

Amadeus FiRe AG, Konzernzentrale Frankfurt am Main

Kernziele des Projekts

- Systematische und risikobasierte Informationssicherheit
- Einführung eines DMS und Zertifizierung nach ISO 27001
- Nachhaltige Integration verbindlicher Sicherheitsstandards im Arbeitsalltag
- Informationssicherheitsmanagements nach einem weltweit anerkannten Standard
- Dokumentation des Stellenwerts von Sicherheit und Datenschutz
- Zertifizierung nach ISO 27701, sobald diese in Deutschland möglich ist

Amadeus FiRe AG, Konzernzentrale Frankfurt am Main

Fazit

„Die ISO 27001-Zertifizierung war alles andere als einfach. Aber durch Umsetzung der BSI-Grundschutz-Vorgaben und die Einführung der ISO 9001 hatten wir ein sehr gutes Fundament für das Projekt gelegt. Rückwirkend betrachtet hat sich der Aufwand auf jeden Fall gelohnt: Die Einführung eines ISMS ist für unseren rasch expandierenden Konzern eine wichtige Weichenstellung – und für unsere Kunden und Stakeholder natürlich ein wichtiges Signal, dass wir die Informations- und Datensicherheit sehr ernst nehmen.“

Elmar Roth
Bereichsleitung Informationstechnologie bei Amadeus FiRe

Networkers AG • Bandstahlstraße 2 • 58093 Hagen
Fon: +49 2331 8095 - 0 • Mail: sales@networkers.de
www.networkers.de

Über die Networkers AG und Controlware GmbH

net.workers AG

Die Networkers AG in Hagen ist ein Unternehmen der Controlware-Gruppe und seit mehr als 25 Jahren Spezialist für die Entwicklung innovativer IT-Infrastrukturen.

Das Unternehmen unterstützt mittelständische und größere Unternehmen bei der Industrialisierung ihrer IT-Umgebungen, um Effizienz, Produktivität und Qualität ihrer IT-Services zu steigern.

Die Networkers AG arbeitet mit ausgewählten Hardware- und Software-Herstellern zusammen und besitzt in der Regel den höchsten Partnerstatus sowie die höchsten Zertifizierungen dieser Unternehmen.

Als Teil der Controlware-Gruppe kann sie zudem auf deren Ressourcen zurückgreifen und so beispielsweise 24/7-Services anbieten.

www.networkers.de

controlware

Die Controlware GmbH, Dietzenbach, ist einer der führenden unabhängigen Systemintegratoren und Managed Service Provider in Deutschland.

Das 1980 gegründete Unternehmen entwickelt, implementiert und betreibt anspruchsvolle IT-Lösungen für die Data Center-, Enterprise- und Campus-Umgebungen seiner Kunden. Das Portfolio erstreckt sich von der Beratung und Planung über Installation und Wartung bis hin zu Management, Überwachung und Betrieb von Kundeninfrastrukturen durch das firmeneigene ISO 27001-zertifizierte Customer Service Center.

Das rund 840 Mitarbeiter starke Unternehmen unterhält ein flächendeckendes Vertriebs- und Servicenetz mit 16 Standorten in DACH. Zu den Unternehmen der Controlware Gruppe zählen die Controlware GmbH, die ExperTeach GmbH, die Networkers AG und die productware GmbH.

www.controlware.de

Networkers AG • Bandstahlstraße 2 • 58093 Hagen
Fon: +49 2331 8095 - 0 • Mail: sales@networkers.de
www.networkers.de