TÜV TRUST IT
TÜV AUSTRIA Group

Success Story

Roche

Entwicklung einer Informationssicherheits-Strategie und Aufbau eines ISMS[1] für Roche Diagnostics

Medizinische Produkte unterliegen strengen Kontrollen und Vorschriften. Der Verstoß gegen diese Vorschriften kann zu empfindlichen Strafen bis hin zum Verkaufsstopp führen. Roche Diagnostics ltd. in Burgress Hill (England) stand vor der Herausforderung die gegebenen nationalen Anforderungen zu erfüllen. Dafür bat das Unternehmen die globale Roche Diagnostics Quality & Regulatory Organisation in Rotkreuz (Schweiz) um Unterstützung. Diese beauftragte die TÜV TRUST IT mit der Identifizierung der Informationssicherheits-Strategie und der Begleitung bei der Maßnahmenumsetzung

Ausgangssituation

Die Division Diagnostics der F. Hoffmann-La Roche AG, dem drittgrößten Pharmaunternehmen der Welt, liefert Produkte zur Prävention, Diagnose und Therapie von Krankheiten für Wissenschaftler, Ärzte, Patienten, Krankenhäuser und Labore in der ganzen Welt[2]. Der nationale Gesundheitsdienst in England (NHS) stellt hohe Anforderungen an Unternehmen, die mit Patientendaten arbeiten. Diese Vorgaben mussten auch von der englischen Niederlassung der Roche Diagnostics erfüllt werden, um weiterhin im Bereich Support und Verkauf in Großbritannien tätig zu sein. Um eine konkrete Vorgehensweise aufzuzeigen, wurde zunächst ermittelt, welche Legaleinheiten im In- und Ausland von der Anforderung der NHS betroffen sind. Parallel dazu wurden die Anforderungen einer Analyse unterzogen, um den dahinter stehenden Aufwand und die benötigten Ressourcen abzuschätzen. Dabei wurde erkannt, dass die Anforderungen der NHS zu einem Großteil deckungsgleich mit dem ISO/IEC 27001 Standard sind. Als Ergebnis wurde entschieden, ein globales ISMS zu etablieren und zu zertifizieren. Hans Georg Seiberlich (Head of Global Customer Support Quality) sagt hierzu:

„Wir haben dank der TÜV TRUST IT schnell die geeignete Strategie für die Implementierung identifiziert. Wichtig war vor allem die Erkenntnis, dass nicht nur die Tochtergesellschaft die Anforderungen der NHS erfüllen muss, sondern auch jeder Dritte, dem die englische Tochtergesellschaft Patientendaten übermittelt. Darunter waren neben Lieferanten auch weitere Gesellschaften der Roche Diagnostics in verschiedenen Ländern."

Vorgehensweise

Um die Gesamtorganisation nicht zu überfordern, wurde eine Strategie gewählt, die eine schrittweise Implementierung pro Legaleinheit vorsah. Somit konnte sichergestellt werden, dass ein Lerneffekt eintritt und die Synergien für jede nachfolgende Legaleinheit optimal genutzt werden können. Ein Steering-Commitee und das zentrale Projektmanagement waren für die Koordination und Schnittstellen zwischen den Einheiten verantwortlich. Im nächsten Schritt wurde mittels simulierter Audits (Mock-Audits) die Konformität der betroffenen Legaleinheiten mit den Anforderungen der ISO/IEC 27001 bestimmt. Anhand dieser Prüfungen wurden die fehlenden Anforderungen identifiziert und ein Bebauungsplan erstellt. Dabei wurde nicht nur Wert auf die Umsetzung der technischen Anforderungen gelegt. Ein elementarer Teil des Projekts war fachübergreifend und organisatorisch geprägt.

Da Informationssicherheit nur dann nachhaltig erfolgen kann, wenn die Akzeptanz der Organisation vorhanden ist, wurde ein Top Management Commitment eingeholt und ein intensi-

1 ISMS = Informationssicherheits-Managementsystem; 2 Quelle: www.roche.de

TÜV TRUST IT
TÜV AUSTRIA Group

Success Story

ves Changemanagement betrieben.

Rob Chapman (Projektleiter):

„Durch die qualifizierte Beratung der TÜV TRUST IT war es uns möglich, den Change nachhaltig innerhalb der Organisation umzusetzen. Das ISMS und die damit verbundenen Anforderungen an Informationssicherheit ist heute ein integraler Bestandteil unserer Firmenkultur.“

Ein weiterer Anspruch bestand an die Gestaltung der Prozesse. So wurden keine unnötigen, eigens für das ISMS konzipierten Prozesse eingeführt, sondern bestehende Prozesse angepasst oder erweitert. Jan Kiefer (Senior Consultant bei der TÜV TRUST IT):

„Wir haben das Risiko- und Qualitätsmanagement nahtlos in das globale System der Roche Global integriert. Dadurch konnten wir sicherstellen, dass die Prozesse nachhaltig gelebt werden und keine ineffizienten Workarounds entstehen.“

Nutzen

Die erfolgreiche Einführung des ISMS wurde mit der Zertifizierung nach ISO/IEC 27001:2013 bestätigt. Standorte in Deutschland, der Schweiz und England sind nun Teil des globalen ISMS. Mit dem erfolgreichen Abschluss des Projekts ist der Grundstein für den Betrieb eines nachhaltigen ISMS gelegt. Hans-Georg Seiberlich:

„Mit der Auswahl der TÜV TRUST IT als Beratung für die Informationssicherheitsstrategie lagen wir goldrichtig. Die pragmatische und kompetente Herangehensweise an ein solch komplexes Projekt hat entscheidend zum Erfolg beigetragen.“

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV AUSTRIA

Waltherstraße 49–51 · D-51069 Köln
Tel.: +49 (0)221 969789 - 0
Fax: +49 (0)221 969789 -12

info@tuv-austria.com
www.it-tuv.com