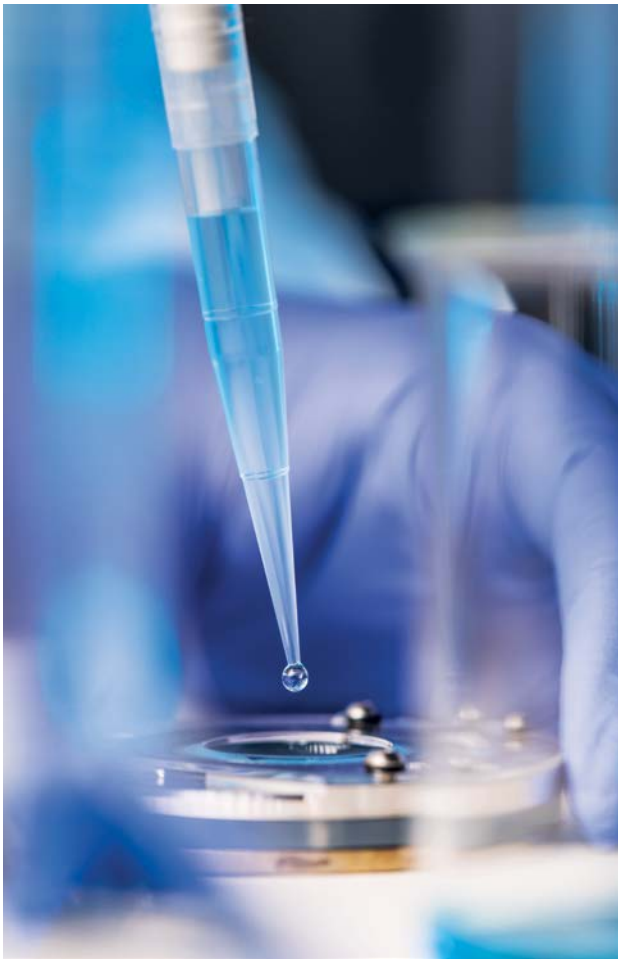
Case Study: Roche Diagnostics International AG

ISO/IEC 27001: Eine Zertifizierung, die Vertrauen schafft. Roche Diagnostics International AG setzt seit vielen Jahren auf hohe Informationssicherheit – um insbesondere Patientendaten zu schützen.

„Wenn es um sensible Daten geht, lautet unsere Maxime ‚Trust & Transparency' ", erklärt Reto Weber, ISMS Officer bei Roche Diagnostics International AG. Roche Diagnostics ist einer von zwei Geschäftsbereichen des Pharmakonzerns Roche und spezialisiert auf Produkte und Dienstleistungen zur Prävention, Diagnose sowie Therapie von Krankheiten: Die Analyse von Gewebe-, Blut- oder anderen Patientenproben liefert wichtige Informationen über Krankheiten, Risiken und das Ansprechen eines Patienten auf eine Therapie. So lässt sich ein Krankheitsfortschritt oder manchmal auch ein -ausbruch vermeiden. Die Basis dafür ist eine Vielzahl von hochsensiblen Daten, die bestmöglich geschützt werden müssen. „Nur wenn die Menschen uns glauben, dass wir das, was wir in Sachen IT-Sicherheit machen, auch gut und mit der gebotenen Sorgfalt machen, sind wir langfristig erfolgreich", so Reto Weber.

Einen konkreten Anstoß, die IT-Sicherheit am Standort Rotkreuz von unabhängiger Seite überprüfen zu lassen, lieferte der britische National Health Service (NHS), das staatliche Gesundheitssystem in Großbritannien und Nordirland. Die Behörde legte dem Unternehmen eine Zertifizierung nahe, die den Schutz der Daten englischer Patienten bestätigen sollte. „Wir hatten das ohnehin schon im Sinn, da wir bereits an einigen Cloud-Produkten arbeiteten – die Anfrage des NHS war dann aber

ÜBERBLICK	
Kunde	Roche Diagnostics International AG
Branche	Diagnostik
Profil	Roche Diagnostics International AG liefert Produkte und Dienstleistungen zur Prävention, Diagnose und Therapie von Krankheiten für Forscher, Ärzte, Patienten, Krankenhäuser und Labore weltweit.
Die Heraus-forderung	Sensible Patientendaten brauchen besonderen Schutz – und neben dem Sicherheitsversprechen des Herstellers auch ein Siegel durch eine unabhängige Instanz.
Die Lösung	Ein Informationssicherheits-Managementsystem nach ISO 27001 mit einem strukturierten, systematischen Ansatz für bestmöglichen Schutz vertraulicher Daten.
Der Nutzen	Eine Zertifizierung wie die ISO 27001 schafft Vertrauen beim Kunden – sie eignet sich ideal als Nachweis für einen hochprofessionellen, verantwortungsvollen Umgang mit sensiblen Patientendaten.



letztendlich der Startschuss“, so Reto Weber. Oberstes Ziel von Roche in Bezug auf Sicherheit: Vertrauen beim Kunden schaffen. „Egal, ob Patienten, Krankenhäuser oder Labore – alle sollen direkt sehen, dass wir Informationssicherheit sehr ernst nehmen.“ Roche verfügt zwar bereits über diverse Zertifizierungen, unter anderem nach der ISO 13485, einer Norm für ein umfassendes Qualitätsmanagementsystem für Design und Herstellung von Medizinprodukten. Hier steht jedoch die Sicherheit der Patienten und der Anwender von Medizinprodukten im Fokus, nicht aber der IT.

Die Lösung

Für Roche Diagnostics International kam nur eine ISO 27001-Zertifizierung infrage. „Nicht zuletzt, weil wir ein Managementsystem für das Thema IT-Sicherheit wollten“, erklärt Reto Weber. Die ISO 27001 für Informationssicherheits-Managementsysteme (ISMS) ist der weltweit anerkannte, branchenübergreifende und führende Standard für Informationssicherheit. Die ISO 27001 definiert Anforderungen an die Einführung, Umsetzung, Überwachung, Dokumentation und Verbesserung eines Informationssicherheits-Managementsystems. Damit bietet die Norm einen strukturierten, systematischen Ansatz für einen besseren Schutz vertraulicher Daten sowie eine höhere Verfügbarkeit von IT-Systemen. Dadurch wird das Thema Informationssicherheit fest im Unternehmensalltag und über alle Hierarchieebenen hinweg verankert.

Im ersten Schritt galt es, alle Stakeholder an einen Tisch zu holen. Eine aufwendige Aufgabe, denn es waren verschiedenste Abteilungen aus dem ganzen – globalen – Konzern involviert, wie Safety Health Environment Management, Security, die IT-Sicherheit, aber auch verschiedene Geschäftspartner, die mit Patientendaten in Berührung kommen. Das Stakeholder-Management und die Abstimmungsrunden stellten sich jedoch als ein zentraler Baustein auf dem Weg zur Zertifizierung heraus. Schnell abgeschlossen hingegen war die Suche nach einem geeigneten Prüfdienstleister. „Wir pflegen mit TÜV SÜD eine langjährige Partnerschaft – und lassen uns dort beispielsweise auch nach der ISO 13485 zertifizieren. Das hat immer zu unserer größten Zufriedenheit geklappt, deshalb war TÜV SÜD gesetzt“, so Reto Weber. Ein besonderes Plus für den Zertifizierer: die Bekanntheit seines Prüfzeichens – es steht weltweit für Qualität und Zuverlässigkeit, quer durch alle Branchen hinweg, und ist sogar bei Verbrauchern gut bekannt. „Ein Gütesiegel von einem deutschen Industrieexperten wie TÜV SÜD hat eine besondere Glaubwürdigkeit und Überzeugungskraft“, erklärt Reto Weber. „Mit solch einem Partner kann man sich gut von der Konkurrenz abheben.“

Der Nutzen

Die Zertifizierung hat sich für Roche Diagnostics International rundum gelohnt und die Ziele wurden vollständig erfüllt. Durch die Auseinandersetzung mit der ISO 27001 hat sich im Konzern manifestiert, dass Informationssicherheit eben nicht nur ein IT-Thema ist, sondern sie auch über Business-Prozesse gesteuert werden kann. „Das gefiel besonders den Entscheidungsträgern“, erinnert sich Reto Weber. „Und für unsere Kunden ist diese Bestätigung der bestmögliche Vertrauensbeweis, und die NHS ist ebenfalls zufrieden.“ Nach und nach wurden sieben Standorte – in Deutschland, der Schweiz, Spanien und den USA – zertifiziert. Auch wenn ein konkreter ROI in solch einem Umfeld kaum berechenbar ist, denn nicht stattfindende Sicherheitsvorfälle lassen sich nicht finanziell ausweisen, „schon allein aufgrund des entstandenen Kulturwandels hat sich die Zertifizierung definitiv gelohnt“, bestätigt der ISMS Officer. „Und auf Produktebene hat sie uns beispielsweise den Umzug in die Cloud

sehr erleichtert.“ Ein Beispiel ist die Diagnostik- und Kollaborationsanwendung „Tumor-Board“ für Ärzte, in der Patientendaten hochsicher abgelegt und in der Cloud gehostet werden – dank der etablierten Prozesse war der Umzug in gerade mal einem halben Jahr möglich.

„Eine Zertifizierung zu erreichen, ist das eine, viel schwerer ist es, sie auch langfristig zu halten. Denn es ist eben keine einmalige Investition und bedarf nicht zuletzt personeller Ressourcen“, gibt der ISMS-Experte zu bedenken. Die ISO 27001 verpflichtet zu kontinuierlichen Verbesserungen. „Und sie fordert von uns, dass wir uns permanent selbst hinterfragen – ist das noch gut und richtig, wie wir die Prozesse handhaben? Dabei hilft es ungemein, wenn einmal im Jahr ein externer Prüfer mit breiter Industrieerfahrung und Vergleichsmöglichkeiten unsere Prozesse und Umsetzungen unter die Lupe nimmt und bewertet, wie wir uns in Sachen Informationssicherheit entwickeln“, stellt Reto Weber klar. „Bei TÜV SÜD ist ein Audit nicht nur das Abarbeiten von Checklisten. Vielmehr wird mit Feedback und Expertise aus dem Feld ein richtiger Mehrwert geschaffen, der uns in den vergangenen Jahren schon erhebliche Fortschritte ermöglicht hat“, so Reto Weber. Dadurch ist die Zertifizierung bei Roche Diagnostics International sehr anerkannt. „Wir bekommen so viel positive Rückmeldung. Zudem kommen pro Jahr ein bis zwei Standorte und Scopes dazu – etwa die cloudbasierten Produkte im Medizinbereich“, freut sich Reto Weber.

Auch der ISMS Officer bei Roche hat die Erfahrung gemacht, dass für eine sinnvolle Umsetzung das Top-Management mit an Bord sein muss. „Ein Tipp, den ich in diesem Zusammenhang jedem geben würde: die Sache in den Vordergrund stellen und nicht die Norm, die ja nur ein Mittel zum Zweck ist. In unserem Fall war die Sache der Schutz von Patientendaten – dass das eine wichtige, unterstützenswerte Angelegenheit ist, versteht jeder sofort“, erklärt Reto Weber. Ebenfalls wichtig: frühzeitig über operative Ressourcen zu sprechen. „Denn man braucht Personal, das keinen Interessenskonflikt hat, um auch mal unbequeme Entscheidungen treffen zu können“, erklärt Reto Weber.

Das Fazit des ISMS Officer bei Roche: „Die Verantwortung für die Patientendaten liegt bei uns – deshalb wollen wir sämtliche, aber speziell diese hochsensiblen Daten bestmöglich absichern. Uns ist bewusst, welches Vertrauen uns entgegengebracht wird, dieses wollen wir natürlich auch rechtfertigen. Das geht am besten über international anerkannte Normen und Standards – deren Umsetzung wir dann von den Besten überprüfen lassen“, resümiert Reto Weber. „Denn wenn meine Daten oder die meiner Familie mal in einem System auftauchen sollten, dann möchte ich auch, dass sie wirklich gut geschützt sind – das ist unser täglicher Anspruch, und genau so gehen wir mit den uns anvertrauten Daten um. Das Managementsystem der ISO 27001 unterstützt uns dabei ideal.“

Wir freuen uns über Ihre Kontaktaufnahme

www.tuev-sued.de/ms/iso-27001
ms-anfragen@tuev-sued.de

Mehr Sicherheit. Mehr Wert.

Datensicherheit ist ein zentrales Thema für die Diagnostik. Eine ISO/IEC 27001-Zertifiz ierung bestätigt, dass die IT-Systeme und Informationen verfügbar, vertraulich und integer sind. Im Rahmen eines ISMS werden Schwachstellen in der Informationssicherheit konsequent aufgedeckt und behoben; ein systematisches Risikomanagement macht Risiken kontrollierbar. Diese Transparenz steigert das Vertrauen von Kunden und Partnern.

TÜV SÜD ist ein führender Dienstleister in den Bereichen Prüfung, Begutachtung, Auditierung, Zertifizierung, Schulung und Knowledge Services und sorgt für Qualität, Sicherheit und Nachhaltigkeit. Das Unternehmen ist an über 800 Standorten weltweit vertreten und verfügt über Akkreditierungen in Europa, Amerika, dem Nahen Osten und Asien. Mit intelligenten Lösungen schafft TÜV SÜD echten Mehrwert für Unternehmen, Verbraucher und Umwelt.

TÜV SÜD Management Service GmbH
Ridlerstraße 57
80339 München
Deutschland
Tel.: 0800 5791-5000
www.tuev-sued.de/tms