Einführung und Zertifizierung eines ISMS nach ISO 27001 bei der Uniklinik RWTH Aachen

AuraSec

UNIKLINIK RWTH AACHEN

Die Uniklinik RWTH Aachen – Spezifika und Besonderheiten

Die Uniklinik RWTH Aachen verbindet als Supramaximalversorger patientenorientierte Medizin und Pflege, Lehre sowie Forschung auf internationalem Niveau. Mit 34 Fachkliniken, 25 Instituten und fünf fachübergreifenden Einheiten deckt die Uniklinik das gesamte medizinische Spektrum ab. Hervorragend qualifizierte Teams aus Ärzten, Pflegern und Wissenschaftlern setzen sich kompetent für die Gesundheit der Patienten ein. Die Bündelung von Krankenversorgung, Forschung und Lehre in einem Zentralgebäude bietet beste Voraussetzungen für einen intensiven interdisziplinären Austausch und eine enge klinische und wissenschaftliche Vernetzung. Rund 6.000 Mitarbeiterinnen und Mitarbeiter sorgen für patientenorientierte Medizin und eine Pflege nach anerkannten Qualitätsstandards. Die Uniklinik versorgt mit 1.400 Betten rund 45.000 stationäre und 200.000 ambulante Fälle im Jahr.

Ausgangslage / Herausforderungen – strategische Implikationen im UKA

Die Uniklinik RWTH Aachen hat sich bereits vor der Einführung des IT-Sicherheitsgesetzes mit dem Thema Informationssicherheit auseinandergesetzt und mit der Entwicklung der sicheren elektronischen Fallakte HIS konkrete Anforderung umgesetzt.

Allen Beteiligten war klar, dass die Uniklinik RWTH Aachen als Betreiber kritischer Infrastrukturen (KRITIS) im Sektor Gesundheit unter die Geltung des IT-Sicherheitsgesetzes fallen wird. Auch wenn die finalen Kriterien und Parameter zu diesem Zeitpunkt noch vom BSI erarbeitet wurden, waren die Eckpfeiler klar umrissen:

- angemessene, dem Stand der Technik entsprechende Maßnahmen zur IT-Sicherheit,
- Nachweis über diese Maßnahmen mindestens alle 2 Jahre,
- Meldepflicht von IT-Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnik (BSI),
- Warn- und Alarmierungskontakte mit jederzeitiger Erreichbarkeit.

Die Uniklinik RWTH Aachen stuft die Informationssicherheit und IT-Prozesse als strategisches Werkzeug und damit kritischen Erfolgsfaktor für die Leistungs-Steuerung und -Erbringung ein. Insofern erfolgte eine Kompetenzfeld-Einrichtung. In deren Mittelpunkt stehen eine IT-Ausrichtung mit Blick auf Verfügbarkeit / Datensicherheit, Flexibilität, Zukunftssicherheit / Innovation unter Berücksichtigung der ISMS-Anforderungen mittels definierter Services/Prozesse.

IT-Sicherheitsgesetz

Unsere moderne Gesellschaft ist heute mehr als jemals zuvor von technischen Systemen abhängig. Ohne Strom wäre eine industrielle Produktion nicht mehr denkbar, ohne die stetige Versorgung mit Trinkwasser das Leben kaum vorstellbar und ohne funktionierende Informations- und Kommunikationstechnik keine Krankenversorgung und kein Bankgeschäft machbar. Nahezu jeder Bereich unseres täglichen Lebens wird durch moderne Technik unterstützt. Alle diese technischen Systeme und Einrichtungen benötigen wiederum bestimmte Basisdienste, um ordnungsgemäß zu funktionieren. Diese für unsere Gesellschaft so bedeutsamen Basisdienste werden als Kritische Infrastrukturen (KRITIS) bezeichnet. Somit war die Sicherstellung der Versorgung der Bevölkerung auch in Krisensituationen einer der Motoren für die Einführung des IT-Sicherheitsgesetzes.

Steigende Sicherheitsanforderungen an Betreiber „kritischer Infrastrukturen“ bedürfen einer konsequenten Umsetzung im Informationssicherheits- / IT-Service-Management.

KRITIS-Sektor „Gesundheit“

Mit der Einteilung Kritischer Infrastrukturen in 9 Sektoren und 29 Branchen liegt eine zwischen Bund und Ländern abgestimmte Grundlage für die Kooperation von Staat und Wirtschaft beim Schutz Kritischer Infrastrukturen vor. In den KRITIS-Sektoren wird das Gesundheitswesen direkt angesprochen und die Branche wie folgt definiert:

:: medizinische Versorgung
:: Arzneimittel und Impfstoffe
:: Labore

Die Branchenverbände sind aufgefordert, innerhalb von zwei Jahren branchenspezifische Regelungen zu erstellen.

Cyberangriffe

Die aktuellsten Ereignisse, bei denen Cyberangriffe erheblichen Einfluss auf den Betrieb einzelner Krankenhäuser hatten, zeigen dass niemand vor Angriffen auf seine IT Infrastruktur sicher sein kann. Vor diesem Hintergrund erscheint es fahrlässig, nicht zu handeln, denn die Verantwortlichen müssen sicherstellen, dass die Informationssicherheit zu jedem Zeitpunkt gewährleistet ist, um eigene Haftungsrisiken zu minimieren.

Die Situation, dass Kliniken in jüngerer Vergangenheit häufiger zu Zielen von Cyber-Angriffen wurden zeigt, dass ein modernes Klinikum nur mit einer funktionieren IT und einem institutionalisierten Sicherheitsmanagement betrieben werden können. Ein Informationssicherheitsmanagement (ISMS) ist insofern Voraussetzung und Zielsetzung zugleich.

Welcher Standard – die Auswahl der ISO / IEC 27001 war konsequent und folgerichtig

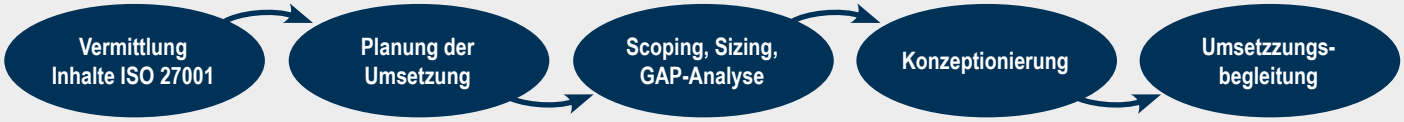
Auf der Suche nach einem angemessen Standard verglich die Uniklinik RWTH Aachen nationale wie internationale Normen. Nachdem auch das BSI seinen IT-Grundschutz nach der ISO/IEC 27001 ausgerichtet hatte, war schnell klar dass diese Norm ausreichende Flexibilität und Skalierbarkeit bietet und die Uniklinik RWTH Aachen bei ihren Zielen unterstützt, ein ISMS zeitnah einzuführen, kontinuierlich weiterzuentwickeln und bestehende Entwicklungen einzubeziehen.

Erprobtes Vorgehen – Sicherung Projekterfolg

Die primären Ziele eines ISMS sind Integrität, Vertraulichkeit und Verfügbarkeit der Informationen und Betriebssicherheit und Verfügbarkeit der informationsverarbeitenden Systeme.

Zur Umsetzung eines ISMS nach der ISO 27001 sind verschiedene Vorbereitungen nötig, um das Ziel einer Zertifizierung zu erreichen. In einem ersten Schritte sind die Verantwortlichkeiten zu definieren und die notwendigen personellen Ressourcen bereitzustellen. Wenn diese Voraussetzungen geschaffen sind, hat sich in der praktischen Umsetzung ein modulares Vorgehen bewährt, um eine ISO 27001-Zertifizierung vorzubereiten und die Zertifizierungsreife innerhalb eines zuvor definierten Zeitraums sicher zu erreichen.

Unser erprobtes Vorgehen zur ISMS-Einführung



Überblick
:: Ziele
:: Inhalte
:: Anforderungen

Festlegung
:: Zielsetzung
:: Vorgehen
:: Projektablauf
:: Projektsetup

Identifikation
:: Key Player
:: Steakholder

Definition
:: Scope
:: Projektumfang
:: GAP-Analyse: IST- / SOLL-Vergleich
:: Aufwandsschätzung
:: erster Projektplan

Zentrale Maßnahmen
:: Risiko-Analyse
:: Maßnahmenplan
:: Prozess-Definition und -Dokumentation
:: Dokumentenprüfung und -erstellung

Je nach Scope & GAP'S
:: Maßnahmenüber-wachung / -begleitung
:: interne Audits
:: Schulung und Sensibilisierung

Abschluss
:: Ready for ZERT

Nach dem die Entscheidung für die ISMS-Einführung und die Unterstützung durch das Management bzw. die Unternehmensleitung feststand, wurden allen Beteiligten die zentralen Inhalte der ISO / IEC 27001-Norm vermittelt.

Anschließend erfolgte die Planung der Umsetzung unter Berücksichtigung der spezifischen Zielsetzungen des UKA.

In Scoping- und Sizing-Workshops wurden der Rahmen und das Vorgehen zur Zertifizierung mit den Beteiligten im Detail abgesteckt. Dabei muss gerade in einer universitären Einrichtung der Maximalversorgung darauf geachtet werden, dass sowohl die Krankenversorgung wie auch Forschung und Lehre spezifische Erfordernisse mit sich bringen, die bei der Implementierung eines ISMS zu beachten sind. Im Mittelpunkt steht dabei die Verfügbarkeit. In diesem Zusammenhang wurde eine GAP Analyse durchgeführt mittels derer der aktuelle Umsetzungsstand an den Anforderungen der ISO /IEC 27001 ermittelt wurde.

Auf Basis der GAP-Analyse konnten die Maßnahmen konkret priorisiert, geplant und analog der Norm zur anschließenden Umsetzung konzeptioniert werden. Zentrales Thema war hierbei die Etablierung des ISMS. Darin werden Verfahren und Maßnahmen festgeschrieben, die Informa-tionssicherheit definieren, steuern, kontrollieren und kontinuierlich verbessern (Plan-Do-Check-Act).

Nun setzten die Projektbeteiligten in der Uniklinik RWTH Aachen die definierten Maßnahmen mit Unterstützung des AuraSec-Teams um, führten interne Audits durch und bereiteten das externe Audit vor. Das erfolgreiche externe Audit durch den TÜV Rheinland Cert GmbH erfolgte im Oktober 2015.

Warum die AuraSec GmbH – Branchen- und ISMS-Experten

Da die ISO / IEC 27001 branchenneutral gefasst ist, ist es notwendig, die Prozesse, Kennzahlen und Benchmarks zur Informationssicherheit auf das Gesundheitswesen zu übertragen. In der Überzeugung dass die Implementierung eines ISMS nach ISO / IEC 27001 für die Weiterentwicklung der Informationssicherheit im Klinikum die richtige Entscheidung ist, hat sich die Leitung des GB-IT dafür entschieden, sich der Unterstützung eines Spezialisten für dieses Thema zu sichern. Bei der Auswahl eines Spezialisten fiel die Wahl sehr schnell auf die **AuraSec**, aufgrund Ihrer branchen- und themenspezifischen Expertise. Die **AuraSec** fokussiert sich auf die Themen „Informationssicherheit", „Datenschutz" und „Risikomanagement" – ergänzt um branchenspezifisches Fachwissen. Diese Expertise ermöglichte es, den Ist-Zustand der IT-Sicherheit in der Uniklinik RWTH Aachen schnell und effizient zu erkennen, zu bewerten und sinnvolle, ökonomisch angemessene Maßnahmen zu konzipieren und deren Umsetzung zu begleiten. Die Projektmitarbeiter der **AuraSec** sind branchenerfahrene Informationssicherheits-experten und Auditoren. Sie bringen die Erfahrungen aus verschiedensten Projekt mit: Zertifizierungen, Erarbeitung von Sicherheitskonzepten und die Erstellung von Handbüchern für komplexe IT-Prozesse sind beruflicher Alltag. Die **AuraSec** deckt mit ihren erfahrenen Projektteams und ISO 27001 Lead Auditoren alle Anforderungen einer erfolgreichen ISO / IEC 27001 Implementierung ab.

Bewertung des Vorgehens und Ergebnisses durch das UKA

»Mit dem Berater-Team der AuraSec GmbH, haben wir einen äußerst erfahrenen und kompetenten Partner für die Zertifizierung unseres ISMS auf Basis ISO 27001 gefunden. Dies hat unsere internen Ressourcen bei der Zertifizierungsvorbereitung sehr entlastet und uns in kürzester Zeit zum Erfolg geführt. Dank der guten Zusammenarbeit verfügen wir heute mit der TÜV Zertifizierung als erster universitärer Maximalversorger über ein hochwertiges Qualitätssiegel für den GB-IT. Die ständige Weiterentwicklung der Sicherheitsmaßnahmen ist ein zentraler Bestandteil unseres Managementsystems.«

Volker Lowitsch, Geschäftsbereichsleiter IT-Direktion des Uniklinik RWTH Aachen

Fazit – Ausblick

Die Uniklinik RWTH Aachen hat als erstes Universitätsklinikum in Deutschland die Zertifizierung nach ISO / IEC 27001 erreicht und richtet sich damit bereits heute an den Anforderungen des IT-Sicherheitsgesetzes aus. Bei allen Aktivitäten steht immer die Sicherheit der Patienten im Fokus. Ein wichtiges Ziel der Uniklinik RWTH Aachen ist der Ausbau telemedizinischer Angebote als Leuchtturmprojekte des GB-IT. Das ISMS unterstützt und unterstreicht die Kompetenz des Klinikums auch mit Blick auf die Beachtung der IT-Sicherheit.

Mit der erfolgreichen ISO 27001-Zertifizierung wird den KRITIS-Anforderungen in idealer Weise Rechnung getragen.

Mittels der Zertifizierung konnte ein Mehr an Vertrauen in die Sicherheit und die angebotenen Leistungen einer Einrichtung des Gesundheitswesens gewonnen werden – Gewinn durch mehr Informationssicherheit.

Darüber hinaus reduzieren der Aufbau eines ISMS und eine Zertifizierung nach ISO 27001 die Haftungsrisiken der verantwortlichen Mitarbeiter und der Geschäftsführung erheblich.

Damit erfüllt die Uniklinik RWTH bereits heute die vielfältigen Anforderungen des IT-Sicherheitsgesetzes, welches bis Ende 2018 in Kraft tritt. Die Anforderungen der ISO 27001-Norm und des IT-Sicherheitsgesetzes sind gleichzeitig Verpflichtung zu einem kontinuierlichen Verbesserungsprozess, der nunmehr fest institutionalisiert ist. Das ISMS unterstützt nicht nur IT-Prozesse sondern sorgt für eine sichere Patientenversorgung.

AuraSec

Unter den Linden 16 | 10117 Berlin
T 030 408173352 | F 05334 948624
info@aurasec.de | www.aurasec.de