Case Study

Harzklinikum Dorothea Christiane Erxleben

QSEC

Harzklinikum Dorothea Christiane Erxleben

Datenschutz, Informationssicherheit und Risikomanagement als Managementaufgabe

Softwaregestütztes Sicherheitsmanagement nach B3S Gesundheit, ISO 27001 und DSGVO mit QSEC

Hardy Krüger, Datenschutzbeauftragter, Informationssicherheitsbeauftragter und Leiter Dokumentenmanagement berichtet über Herausforderungen und Erfahrungen eines Datenschutz- und Informationssicherheitsmanagementsystems (DIMS) nach B3S mit QSEC

Die Harzklinikum Dorothea Christiane Erxleben GmbH ist aus der Fusion der kommunalen Krankenhäuser Klinikum Dorothea Christiane Erxleben Quedlinburg GmbH und Harz-Klinikum Wernigerode-Blankenburg GmbH im Juni 2012 entstanden.

Das größte kommunale Krankenhaus in Sachsen-Anhalt, nach den beiden landeseigenen Universitätskliniken in Magdeburg und Halle/Saale, hat rund 2000 Mitarbeiterinnen und Mitarbeiter, circa 1000 stationäre Betten und einen Jahresumsatz von ungefähr 150 Millionen Euro. Das Harzklinikum zählt damit zu den bedeutenden Einrichtungen im Gesundheitswesen des Landes Sachsen-Anhalt.

Viele anerkannte medizinische Schwerpunkte zeugen von einem großen Leistungs- und Behandlungsspektrum. Das wird auch im ambulanten Bereich stetig weiterentwickelt: Aktuell werden mehr als 50 Facharztpraxen in der Harzregion und teils auch darüber hinaus betrieben.

Das Harzklinikum Dorothea Christiane Erxleben mit seinem Unternehmenssitz in Quedlinburg hat Kliniken in Blankenburg, Quedlinburg und Wernigerode. Als kommunales Haus pflegt das Harzklinikum eine enge und vertrauensvolle Zusammenarbeit mit zahlreichen Partnern in der Harzregion. Beispielhaft sind das Diakonie-Krankenhaus Harz GmbH in Elbingerode, die Paracelsus Harzklinik in Bad Suderode und die Celenus Teufelsbad Fachklinik GmbH in Blankenburg zu nennen.

„Gesundheit braucht Kompetenz“ - so der Leitsatz des Harzklinikums - charakterisiert den Anspruch des Harzklinikums an eine moderne leitliniendefinierte und patientenorientierte Medizin, Behandlung, Versorgung und Betreuung.

Insgesamt steckt großes Potenzial im Harzklinikum. Das gilt es stetig weiter zu entwickeln und auszubauen. Die Mitarbeiterinnen und Mitarbeiter aller Berufsgruppen arbeiten mit Engagement, Kompetenz und Erfahrung an diesem Ziel. Der Patient ist der Mittelpunkt des Handelns.

Die Ausgangssituation

KRITIS – Betreiber wie die Harzklinikum Dorothea Christiane Erxleben GmbH sind aufgrund der KRITIS-Verordnung als Krankenhaus mit mehr als 30.000 vollstationären Fällen pro Jahr verpflichtet Ihre IT-Sicherheitsmaßnahmen auf den jeweils aktuellen Stand der Technik zu bringen, zu halten und die Erfüllung der Anforderungen an Betreiber kritischer Infrastrukturen alle zwei Jahre nachzuweisen. Damit diese Verpflichtungen erfüllt werden können, wird seitens des BSI auf die Umsetzung des anerkannten branchenspezifischen Sicherheitsstandards (B3S Gesundheitswesen) verwiesen. In der Praxis wird der Aufbau eines Informationssicherheitsmanagementsystems, das die B3S Anforderungen erfüllt und auch das Risikomanagement entsprechend berücksichtigt, unerlässlich.

Die Anforderung in Bezug auf die Umsetzung der obengenannten Herausforderung und der gleichzeitige Wunsch auch die Datenschutzanforderungen, einschließlich Reifegrad in einem Managementsystem umzusetzen, führte dazu im Markt nach einem Lösungsanbieter zu suchen, der eine geeignete Lösung für alle Anforderungen anbietet.

Der Entscheidungsprozess - warum QSEC?

Einige wesentliche Kriterien für den Entscheidungsprozess seitens der Harzklinikum Dorothea Christiane Erxleben GmbH waren,

- eine geeignete datenbankbasierte Softwarelösung zu evaluieren, die der Vielzahl der Anforderungen entsprechen würde.
- eine vollumfängliche Umsetzung der Anforderungen an das Datenschutz-, Informationssicherheits- und Risikomanagement in einer Softwarelösung, einschließlich der Integration aller B3S Gesundheitswesen Vorgaben.

- die Evaluation einer Softwarelösung in welcher einerseits standardisierte Prozesse des Klinikums userfreundlich und ressourcensparend abgebildet werden können und andererseits mit welcher sehr individuelle und einer ständigen Veränderung unterliegende Prozesse einfach abgebildet und flexibel angepasst werden können.

- eine Lösung zu evaluieren, die umfassend, nutzerfreundlich, flexibel anpassbar ist und es ermöglicht den etablierten IT-Dienstleister CANCOM in dem gesamten Prozess mit einzubinden.

- die Möglichkeit die Fachabteilungen mit der Lösung von spezifischen Fragestellungen zu ihren Arbeitsprozessen über schulungsarme Workflowprozesse zu integrieren.

Der IT-Dienstleister CANCOM wurde als Dienstleistungspartner der Harzklinikum Dorothea Christiane Erxleben GmbH in den Auswahlprozess mit einbezogen.

Die Gespräche mit den Anbietern und die Evaluation der in Betracht kommenden Softwarelösungen ergaben, dass Nexis GRC mit der Datenschutz-, GRC und ISMS Softwarelösung QSEC den Anforderungskriterien am besten entsprach. Insbesondere der umfassende Content von QSEC mit unterschiedlichen Anwendermodi für Experten und Anwender aus den Fachabteilungen sowie die überzeugende Integration von Datenschutz- und Informationssicherheitsfunktionalitäten sprachen für eine Zusammenarbeit mit Nexis GRC und QSEC.

Ferner bewies Nexis GRC in allen Phasen der Evaluierung tiefe Fachkompetenz bei gleichzeitiger Flexibilität eines Mittelstandsunternehmens im Hinblick auf die fachlichen Anforderungen.

Die Einführungsphase

Die Umsetzung des Projekts „Datenschutz- und ISMS-Tooleinführung mit QSEC“ startete im August 2020.

1. In der 1. Projektphase wurde QSEC nach den Vorgaben des Harzklinikums ausgeprägt, wobei die Anforderungen des B3S und des Datenschutzes im Mittelpunkt standen. Die Konzepte für Unternehmensstruktur und Untersuchungsbereiche wurden erstellt und in das QSEC-System übernommen.

   Dabei wurde bereits mit der Planung festgelegt, dass alle 3 Standorte der Harzklinikum Dorothea Christiane Erxleben GmbH nach B3S Gesundheitswesen auditiert werden sollten.

   Im Zuge dieser Planung wurde die gesamte Legal-Entity-Struktur erfasst und die Berechtigungsanforderungen festgelegt. Die erforderlichen Dokumente (Leitlinien, Richtlinien etc.) wurden erstellt, verabschiedet, ins System übernommen und mit den Controls der B3S verbunden. Ebenso wurde in dieser Projektphase die SoA (Statement of Applicability) erstellt.

2. In der 2. Projektphase wurden im Risikomanagement die Risikokataloge für die zugeordneten Asset-Gruppen bearbeitet und die ermittelten Risiken in einem Risikobehandlungsplan bewertet. Gleichzeitig wurden die Workflows für Dokumentenfreigaben und Aktionsbestätigungen eingeführt.

   Besonders hervorzuheben ist die erfreulich reibungslose Einbindung der Fachabteilungen in den Bestätigungsworkflow. Über die in QSEC integrierten Workflow-Funktionalitäten konnte dieser Prozess mit hoher Akzeptanz der Fachabteilungen ohne große Schulungsaufwendungen etabliert werden.

   Im Mai 2021 hat das Harzklinikum die Auditierung u. a. auch durch QSEC erfolgreich bestanden und sieht auch zukünftigen Audits mit deutlich reduziertem Aufwand entgegen. Alle Prozesse können durch QSEC nachhaltig und permanent gepflegt und entwickelt werden, wodurch alle erforderlichen Daten bei Bedarf tagesaktuell zur Verfügung stehen.

3. Im nächsten Schritt ist eine Erweiterung des QSEC Systems geplant, durch die ein E-Learning System für alle Mitarbeiter der Harzklinikum Dorothea Christiane Erxleben GmbH in die QSEC Oberfläche integriert werden soll.

FAZIT

Mit QSEC kann die Harzklinikum Dorothea Christiane Erxleben GmbH alle Aktivitäten zu den Themen Datenschutz, ISMS, B3S Gesundheit und zum Risikomanagement nachhaltig darstellen, lückenlos belegen und verfügt über eine hervorragende Basis in Bezug auf alle compliance- und risikorelevanten Entscheidungen.

„Die Auditierung unserer Infrastruktur wurde mit der Unterstützung von QSEC wesentlich einfacher und effizienter. Aufgrund der positiven Bewertung der Auditoren in Bezug auf die Leistungsfähigkeit des Systems werden wir QSEC in weiteren Schritten entsprechend unserer Anfordernisse ausbauen.“

Hardy Krüger: Datenschutzbeauftragter, Informationssicherheitsbeauftragter und Leiter Dokumentenmanagement

Harzklinikum Dorothea Christina Erxleben GmbH

Kontakt
Nexis GRC GmbH • Zimmerstraße 1, 22085 Hamburg • +49 40 650336-0 • info@nexis-qsec.com