THE AUDIT COMPANY

Digitalisierung – neue Anforderungen an den KRITIS-Sektor Gesundheit

Kennen Sie auch solche Meldungen aus der Presse? Im Februar 2016 griff ein sogenannter Erpressungstrojaner in einem Krankenhaus in Neuss (NRW) um sich. Ein achtloser Mausklick eines einzigen unachtsamen Mitarbeiters und schon war es passiert: Die IT-Systeme der Klinik waren erst einen Monat nach diesem Vorfall in Bezug auf die Patientenversorgung und – im Sinne des klinischen Risikomanagements – für die Gewährleistung der Patientensicherheit wieder einsatzbereit. Entstandene Kosten für die Klinik: Eine Millionen Euro.

Das IT-Sicherheitsgesetz

Mit der Einfachheit des modernen Datentransfers und dem oftmals sorglosen Umgang durch eine Fülle von Nutzern wird schnell vergessen, wie leicht es Unbefugte haben, an bedeutende Unternehmenswerte zu gelangen. Auch bei Medizinprodukten bestehen eklatante Risiken, die nicht zu unterschätzen sind. Bereits im Jahr 2015 sind Infusionspumpen mit WLAN-Steuerung (also via Funknetz) von einem der größten Hersteller in das Zentrum der Sicherheitsexperten gerückt: Aufgrund gravierender technischer Sicherheitsmängel war es relativ einfach möglich, alle Infusionspumpen innerhalb eines Netzwerks zu übernehmen und somit beliebig die Ausgabe und Dosierung von Medikamenten zu manipulieren. Das mögliche Ausmaß zu Lasten der Patientensicherheit kann also verheerend sein!

Dies sind anschauliche Beispiele dafür, warum IT-Sicherheit bzw. der technische und organisatorische Schutz von Einrichtungen und deren IT-Infrastruktur in den Fokus von Politik und Gesetzgebung gerückt sind. Immer wieder geraten weiterentwickelte Erpressungstrojaner in Umlauf oder Hersteller vernachlässigen Sicherheitsthemen in der Entwicklung (Security by Design). Die Konsequenz daraus ist unter anderem das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, das "IT-Sicherheitsgesetz", das zum 25. Juli 2015 in Kraft getreten ist. Sinn und Zweck des IT-Sicherheitsgesetzes ist einerseits die signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland. Andererseits ist der Schutz kritischer Infrastrukturen wesentlich, die gerade für das Funktionieren des Gemeinwesens von zentraler Bedeutung sind.

Infolgedessen wurden Betreiber „Kritischer Infrastrukturen“ (KRITIS-Betreiber) verpflichtet, einen Mindeststandard an IT-Sicherheit einzuhalten und erhebliche IT-Sicherheitsvorfälle an das BSI (Bundesamt für Sicherheit in der Informationstechnik) zu melden. Im Mai 2016 ist die Rechtsverordnung zur Umsetzung des IT-Sicherheitsgesetzes in Kraft getreten, die eine nähere Bestimmung der Kritischen Infrastrukturen bezogen auf die neun Sektoren der KRITIS-Betreiber beinhaltet: Der „1. Korb“ umfasste die Sektoren Energie, Informationstechnik und Telekommunikation, Wasser, Ernährung sowie Medien und Kultur. Am 30. Juni 2017 wurden mit dem „2. Korb“ nun auch die Sektoren Gesundheit, Transport und Verkehr sowie Finanz- und Versicherungswesen mit spezifischen Kriterien und Schwellwerten involviert. Angaben zum Sektor Staat und Verwaltung stehen nach wie vor aus.

DQS GmbH
Deutsche Gesellschaft zur Zertifizierung von Managementsystemen

August-Schanz-Straße 21
60433 Frankfurt am Main

Tel. +49 69 95427-0
info@dqs.de

www.dqs.de

THE AUDIT COMPANY

Kritische Infrastrukturen nach Sektoren	
Sektoren	**Bereiche**
Energie	Elektrizität, Gas, Mineralöl
Informationstechnik und Telekommunikation	Informationstechnik, Telekommunikation
Gesundheit	medizinische Versorgung, Arzneimittel und Impfstoffe, Labore
Wasser	öffentliche Wasserversorgung, öffentliche Abwasserbeseitigung
Ernährung	Ernährungswirtschaft, Lebensmittelhandel
Transport und Verkehr	Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik
Finanz- und Versicherungswesen	Banken, Börsen, Versicherungen, Finanzdienstleister
Staat und Verwaltung	Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/Rettungswesen inkl. Katastrophenschutz
Medien und Kultur	Rundfunk, gedruckte / elektronische Presse, Kulturgut, symbolträchtige Bauwerke

Demnach gilt z. B. ein Krankenhaus mit mindestens 30.000 vollstationären Fällen pro Jahr als KRITIS-Betreiber und unterliegt damit bei Inkrafttreten verbindlich den Anforderungen dieser Gesetzgebung. Nach Inkrafttreten der jeweiligen branchenspezifischen IT-Sicherheitsverordnungen haben die KRITIS-Betreiber jeweils sechs Monate Zeit, die Vorfalls-Meldepflicht beim BSI zu realisieren. Weitere zwei Jahre verbleiben den Betreibern sicherheitskritischer Anlagen, die Sicherheitsrichtlinien nach dem aktuellen Stand der Technik zu realisieren. Teilweise existieren bereits Umsetzungsleitfäden oder ähnliche Dokumente, die einen Orientierungsrahmen geben. Offiziell verabschiedete Branchenstandards mit detaillierteren Übersetzungen zu den jeweiligen Anforderungen stehen jedoch aktuell meist noch aus.

Zusätzlich zu diesen Anforderungen treten im Mai 2018 die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) in Kraft. Diese Vorgaben betreffen zwar nicht ausschließlich das Gesundheitswesen, aufgrund der Verarbeitung hoch sensibler, personenbezogener Informationen steht dieses jedoch besonders im Fokus. Im Artikel 32 der DS-GVO wird wie bei den bisher dargestellten Anforderungen von der Umsetzung technischer und organisatorischer Maßnahmen auf Basis des „aktuellen Stand der Technik“ gesprochen. Ein entscheidender und zielführender Lösungsansatz kann daher die sofortige Auseinandersetzung mit der ISO/IEC 27001 sein, um diese verschiedenen gesetzlichen und behördlichen Anforderungen zu erfüllen und sich frühzeitig mit dieser komplexen Thematik auseinanderzusetzen. Das gilt auch dann, wenn die Organisationen nicht über den Schwellenwerten liegen und noch keine Branchenstandards vorliegen.

Dabei steht für die KRITIS-Betreiber keine punktuelle Umsetzung im Mittelpunkt, sondern vielmehr die Aufgabe zur zielgerichteten und nachhaltigen Einbindung in das bestehende Managementsystem – an Art und Umfang zur Größe der Organisation ausgerichtet sowie unter Einbeziehung von Umsatz- und Ergebnisgrößen und der Anzahl an Mitarbeitern. Die beste Chance zur Einhaltung der gesetzlichen Vorgaben besteht darin, dass diese in zuverlässige und sichere Prozesse implementiert werden. Transparente und eindeutig festgelegte Verantwortungen für Führungskräfte und Mitarbeiter tragen dazu bei, durch regelmäßige und der Organisation angemessene Wirksamkeitsprüfungen, z. B. in Form von Audits, die Funktionsfähigkeit und Wirksamkeit des Gesamtsystems überwachen zu können.

„Proaktives statt reaktives Handeln“ und damit „Prävention statt Reaktion“ ist keine Herausforderung, sondern ein Vorgehen, das gesetzlich endlich klar spezifiziert wurde. Nun gilt es, die neuen Anforderungen so früh wie möglich zu bewerten und in den Einrichtungen zu implementieren. Angesichts der Komplexität sicherlich keine leichte Aufgabe. Die Notwendigkeit sollte dabei nicht in Frage gestellt werden, sondern vielmehr die nachhaltige Chance gesehen werden, für die Patienten und alle weiteren Beteiligten mehr Sicherheit in der medizinischen Versorgung zu gewährleisten.

Sprechen Sie mit uns.
Ihre Ansprechpartnerin:
Nadja.Goetz@dqs.de
Tel. +49 69 95427-386

Andreas Altena
Geschäftsführer Sollence GmbH
DQS-Auditor

Angelika Müller
Geschäftsführerin Sollence GmbH
DQS-Auditorin