

Medizintechnik und IT – eine Beziehung mit Risiken

Medizintechnik und IT waren lange Zeit getrennte Welten. Damit ist es vorbei: So entwickeln sich neue Potentiale, aber auch erhebliche Risiken. Datenschutz und Sicherheit fordern Gehör.

Martin Ortgies, Königslutter/Braunschweig

Die Medizintechnik wird immer stärker in die IT-Netzwerke und die elektronischen Prozesse integriert. Die ersten Kliniken gehen bereits dazu über, die Betreuung der IT und der Medizintechnik organisatorisch zusammenzulegen. Wird in einem gewachsenen medizinischen IT-Netzwerk etwas verändert, z. B. ein neues Gerät integriert, kann das weitgehende Folgen für die Netzverfügbarkeit haben. Werden Geräte unterschiedlicher Hersteller in einem Netzwerk betrieben, kann es etwa zu gegenseitigen Störungen kommen. Werden diese Störungen nicht sofort erkannt, ist die Funktionssicherheit der Geräte oder die komplette Netzverfügbarkeit gefährdet.

Deshalb empfiehlt die IEC-Norm 80001-1 ein systematisches Risikomanagement. „Der sichere Betrieb der Medizintechnik ist in Verbindung mit der weitgehend etablierten elektronischen Patientenakte eine der größten Herausforderungen der nächsten Jahre. Hier herrscht noch ein großes Defizit an Wissen und Erfahrung. Die seit März

europaweit gültige Norm IEC 80001-1 beschreibt ein Risikomanagement in medizinischen IT-Netzwerken und liefert zusammen mit der ISO 27001 eine produktive Hilfe bei der notwendigen Anpassung der Prozesse“, empfiehlt Maik Opitz, IT-Security-Experte bei DS Data Systems. Als zertifizierter ISO-27001/IT-Grundschutz-Auditor beim BSI und bei der Dekra zugelassener ISO-27001-Auditor hat er bereits mehrere Kliniken zertifiziert.

Erfahrungen mit EPA

Nach den regelmäßigen Umfragen der FH Osnabrück gehört die elektronische Patientenakte zu den wichtigsten IT-Prioritäten der deutschen Krankenhäuser. Nach 56 % in 2009 (IT-Report Gesundheitswesen 2009/2010) nutzen heute vermutlich bereits bis zu zwei Drittel eine voll funktionsfähige EPA bzw. sind dabei, diese aufzubauen. Mit der stärkeren internen und externen IT-Vernetzung ist die Funktionsfähigkeit eines Krankenhauses immer mehr von der Verfügbarkeit und der Sicherheit der IT-Systeme abhängig. Trotzdem haben die meisten Institute darauf noch nicht angemessen reagiert: Die jederzeitige Sicherheit und Stabilität der internen Prozesse, der IT-Infrastruktur, der Medizintechnik und der Patientendaten sind nicht angemessen gewährleistet. Notwendig wäre ein übergeordneter Sicherheitsprozess, z. B. ein Informationssicherheits-Managementsystem (ISMS), wie es das Bundesamt für Sicherheit in der Informationstechnik für erforderlich hält. „In dem Maße, wie die IT-Vernetzung zunimmt, erhöht sich auch der Schutzbedarf insbesondere

für vertrauliche Patientendaten. Mit der internationalen Sicherheitsnorm ISO 27001 kann das Krankenhaus den Nachweis führen, dass auch die Anforderungen des Datenschutzes erfüllt sind“, erläutert Opitz. Er sieht im Best-Practice-Ansatz des BSI beim IT-Grundschutz in Verbindung mit der ISO 27001 eine sehr hilfreiche Unterstützung für die Kliniken: „Die Verfügbarkeit der Systeme steigt, und die Vertraulichkeit und Integrität der Informationen wird nachweislich besser gewährleistet. Die IT-Grundschutz-Kataloge werden laufend erweitert, um aktuellen Anforderungen gerecht zu werden.“

Um die IT-Verfügbarkeit zu erhöhen, gebe es einen bewährten Maßnahmenkatalog mit technischen Vorkehrungen. Unterschätzt werde aber häufig, was erforderlich sei, um die Vertraulichkeit und Integrität der Daten sicherzustellen. „Jedes Klinikum muss gewährleisten, dass die Daten richtig sind, nicht unrechtmäßig verändert werden und dass keine Unberechtigten darauf zugreifen können“, berichtet der BSI-Auditor. So dürften in der Regel nur Ärzte und das klinische Personal Zugriff auf die Daten in ihrer Station haben. Eine aktuelle Herausforderung sei die Absicherung der klinischen Prozesse rund um SAP, KIS, PACS, RIS, der Medizintechnik und einer Vielzahl an zuliefernden Informationssystemen. „Die erforderlichen abgesicherten Prozesse sind in den Kliniken in der Regel noch nicht vorhanden. Sie sind für den sicheren Betrieb einer EPA allerdings eine Pflichtvoraussetzung. Hier gibt es dringenden Handlungsbedarf, denn zurzeit werden die Anforderungen des Datenschutzes regelmäßig missachtet“,

verweist der Sicherheitsexperte auf aktuelle Probleme.

Sicherheits-Management

Das Städtische Klinikum hat bereits einige Jahre Erfahrung mit diesem Sicherheitskonzept. 2008 wurde in Braunschweig erstmals einem Klinikum bescheinigt, dass zentrale Komponenten seiner IT-Sicherheits-Organisation den strengen Sicherheitsanforderungen der ISO-Norm 27001 auf der Basis von IT-Grundschutz gerecht werden. „Generell hat die Zertifizierung und deren Vorbereitung die Gesamtsicherheit enorm erhöht. Wir haben die Sicherheitsrichtlinien formuliert, uns intensiv mit den Prozessen auseinandergesetzt und das Sicherheitsbewusstsein des Managements erhöht“, fasst Dr. Christoph Seidel, Geschäftsbereichsleiter IT und Unternehmensentwicklung und CIO beim Städtischen Klinikum Braunschweig, die Erfahrungen zusammen. Wenn ein unabhängiger Dritter bestätige, dass für die IT-Sicherheit alles Notwendige getan und nach dem aktuellen Stand der Technik umgesetzt werde, schaffe das auch eine persönliche Absicherung. Der CIO weiter: „Ich kann anderen Unternehmen nur empfehlen, sich auch der Hilfe durch einen externen Berater zu bedienen. Man muss dessen Ratschläge aber auch ernst nehmen. Der Coach kann auf kritische Punkte hinweisen, aber nicht die Abhilfe forcieren.“

| www.datasystems.de |