Foto: Sergey Nivens – Fotolia

Geltungsbereich des IT-Sicherheitsgesetz

Durch Strukturanalyse den Blick auf das Wesentliche fokussieren

Von Prof. Dr. Andreas Becker und Randolf Skerka

Mit der am 29.06.2017 erfolgten Veröffentlichung der ersten Verordnung zur Änderung der BSI-Kritisverordnung (KritisV) sind nun auch diejenigen Krankenhäuser, die mindestens 30.000 vollstationäre Fälle pro Jahr versorgen, verpflichtet Sicherheitsmaßnahmen nach dem Stand der Technik umzusetzen und Sicherheitsvorfälle an das BSI zu melden.

Kurzfristig muss dem BSI bis zum 29.12.2017 eine Kontaktstelle benannt werden, über die das Krankenhaus jederzeit, das heißt 24 Stunden am Tag, sieben Tage die Woche, erreichbar ist. An diese Adresse wird das BSI IT-Sicherheitsinformationen versenden.

Zudem sind betroffene Krankenhäuser gemäß § 8a Absatz 3 BSIG verpflichtet, bis zum 29. Juni 2019 den Nachweis zu erbringen, dass ein angemessenes Maß an IT-Sicherheit erreicht ist.

Das wesentliche Ziel des IT-Sicherheitsgesetztes ist es sicherzustellen, dass Betreiber Kritischer Infrastrukturen durch das nachgewiesene Maß an IT-Sicherheit die Versorgungssicherheit ihrer für die Bevölkerung kritischer Dienstleistungen (kDL) gewährleisten können.

Maßgeblich für die Frage, auf welche Bereiche eines Krankenhauses die Anforderungen des Sicherheitsgesetztes anzuwenden sind, sind die kritischen Dienstleistungen. Das sind diejenigen Dienstleistungen zur Versorgung der Allgemeinheit, deren Ausfall oder Beeinträchtigung zu erhebli-

Das Thema IT-Sicherheit gewinnt im Gesundheitswesen zunehmend an Bedeutung. Die Digitalisierung von Prozessen und die Vernetzung von Programmen erhöht zwar die Effektivität, macht Krankenhäuser jedoch auch angreifbar. Der Gesetzgeber folgte dem Ruf nach mehr Sicherheit mit dem im Juli 2015 in Kraft getretene IT-Sicherheitsgesetz. Doch wie wirken sich die Gesetzesvorschriften konkret aus? Diese Fragen beantworten Randolf-Heiko Skerka, Experte für Informationssicherheits-Managementsysteme, und Prof. Dr. Andreas Becker, Berater für Einrichtungen im Gesundheitswesen.

Keywords: *IT-Sicherheit, Geltungsbereich, Strukturanalyse, BSIG*

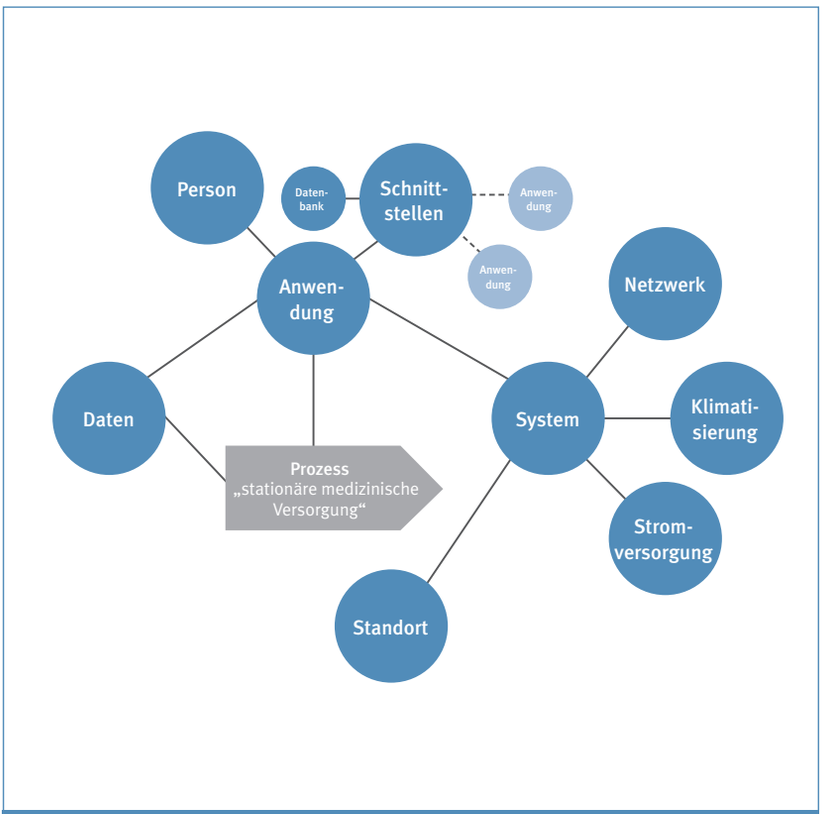

Abb: Schematisches Ergebnis einer exemplarischen Strukturanalyse

chen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde. Im Sektor Gesundheitswesen sind in der BSI-Kritisverordnung als kritische Dienstleistungen definiert:

- Die stationäre medizinische Versorgung,
- die Versorgung mit unmittelbar lebenserhaltenden Medizinprodukten, die Verbrauchsgüter sind und
- die Versorgung mit verschreibungspflichtigen Arzneimitteln und Blut- und Plasmakonzentraten zur Anwendung im oder am menschlichen Körper sowie
- die Laboratoriumsdiagnostik.

Für Krankenhäuser ist mindestens die stationäre medizinische Versorgung als kritische Dienstleitung relevant. Weitere Dienstleistungen eines Krankenhauses können als kritisch zählen, sofern eine der oben aufgeführten Dienstleistung aus dem Gesundheitssektor vom Krankenhaus erbracht und der jeweilige Schwellwert aus dem Anhang 5 der BSI-Kritisverordnung überschritten wird.

Der Fokus liegt auf der „kritischen Dienstleistung“

Das IT-Sicherheitsgesetz ist nicht auf das gesamte Krankenhaus, sondern nur auf denjenigen Teil anzuwenden, der für die Erbringung der kritischen Dienstleistung relevant ist. Das BSI definiert in seiner Orientierungshilfe zur Prüfung nach § 8a Absatz 3 BSIG den Geltungsbereich als den Bereich der „... die informationstechnischen Systeme, Komponenten und Prozesse, Rollen beziehungsweise Personen [umfasst,] die für die Funktionsfähigkeit der von Betreibern nach BSI-KritisV betriebenen Kritischen Infrastrukturen maßgeblich sind beziehungsweise auf diese Einfluss haben“.

Um den Aufwand für die Umsetzung der Anforderungen möglichst weit zu minimieren, ohne hierbei die gesetzlichen Anforderungen zu vernachlässigen, gilt es, den individuellen Geltungsbereich möglichst stark einzugrenzen.

Mit einer Strukturanalyse die IT-Abhängigkeit der „kritischen Dienstleistung“ ermitteln

Bei der Festlegung des individuellen Geltungsbereiches des IT-Sicherheitsgesetztes im Krankenhaus wird daher bei der kritischen Dienstleistung „stationäre medizinische Versorgung“ begonnen. Im Ergebnis einer durchzuführenden Analyse muss ermittelt werden, welche Abhängigkeit von der IT in diesem Geschäftsprozess besteht, also welche IT-Komponenten und auch Prozesse den gesetzlichen Vorgaben und damit dem Stand der Technik entsprechen müssen.

Für eine solche Analyse hat sich die Methode der Strukturanalyse etabliert, deren Ziel es unter anderem ist, die Abhängigkeiten eines Prozesses von der IT zu ermitteln (▶Abb.).

Die Vorgehensweise der Strukturanalyse ist sehr systematisch. Sie umfasst mehrere Schritte, die in der Regel iterativ durchlaufen werden, da sich aus jedem Schritt Erkenntnisse ergeben können, die Auswirkungen auf die Ergebnisse vorheriger Schritte haben können. Diese Schritte umfassen:

„Für eine solche Analyse hat sich die Methode der Strukturanalyse etabliert, deren Ziel es unter anderem ist, die Abhängigkeiten eines Prozesses von der IT zu ermitteln.“

- *Ermittlung der relevanten IT-Anwendungen*
  In diesem Schritt wird ermittelt, durch welche IT-Anwendungen der Prozess der „stationären medizinischen Versorgung“ unterstützt wird und wie hoch die Abhängigkeit des Prozesses von dieser IT-Anwendung ist. Hierzu wird die hypothetische Frage beantwortet, welche Auswirkung der Ausfall der IT-Anwendung auf den Prozess hat.

- *Identifikation relevanter Daten*
  Nachdem die IT-Anwendungen identifiziert wurden, wird ermittelt, welche für den Prozess der „stationären medizinischen Versorgung“ relevanten Daten verarbeitet werden. Hierzu wird zusätzlich die hypothetische Frage beantwortet, welche Auswirkung es hat, wenn die Daten nicht zur Verfügung stehen oder nicht korrekt sind.
- *Identifikation relevanter IT-Systeme*
  Nachdem die relevanten Daten und IT-Anwendungen identifiziert wurden werden diejenigen IT-Systeme identifiziert, die für den Betrieb der Anwendungen erforderlich sind.
- *Erfassung weiterer Komponenten*
  Da für den Betrieb einer IT-Infrastruktur weitere Komponenten erforderlich sind, werden abschließend die für den Betrieb der IT erforderlichen Personen, die Räumlichkeiten, Netzwerkinfrastruktur et cetera erfasst.

Im Ergebnis einer Strukturanalyse sind die Abhängigkeiten des Prozesses der „stationären medizinischen Versorgung“ von unter anderem Anwendungen, Daten, Systemen, Personen und Standorten ermittelt, so dass damit der Geltungsbereich identifiziert und die erforderlichen Maßnahmen zur Erreichung des Standes der Technik umgesetzt werden können.

Da IT-Infrastrukturen heutzutage von der Vernetzung von Anwendungen miteinander und der gemeinsamen Nutzung von IT-Ressourcen profitieren, besteht die besondere Herausforderung bei der Ermittlung des Geltungsbereiches einerseits darin, die Vollständigkeit der erfassten Komponenten zu erreichen, aber auch andererseits darin die Grenze zu denjenigen Bereichen zu ziehen, die keinen Beitrag zum betrachteten Prozesses der „stationären medizinischen Versorgung“ haben. Durch die saubere Abgrenzung des Geltungsbereiches gelingt es leichter sowohl den Aufwand zur Umsetzung der Anforderungen des IT-Sicherheitsgesetztes zu minimieren als auch die erforderlichen Ressourcen zur Erreichung des Standes der Technik gezielt einzusetzen. ■

„Durch die saubere Abgrenzung des Geltungsbereiches gelingt es leichter sowohl den Aufwand zur Umsetzung der Anforderungen des IT-Sicherheitsgesetztes zu minimieren als auch die erforderlichen Ressourcen zur Erreichung des Standes der Technik gezielt einzusetzen.“

Prof. Dr. Andreas Becker
Qualifikation
“Spezielle Prüfverfahrens-Kompetenz
für § 8a BSIG“
Institut Prof. Dr. Becker
Nonnenweg 120a
51503 Rösrath

Prof. Dr. Andreas_Becker

Randolf Skerka
SRC Security Research & Consulting GmbH
Emil-Nolde-Str. 7
53113 Bonn