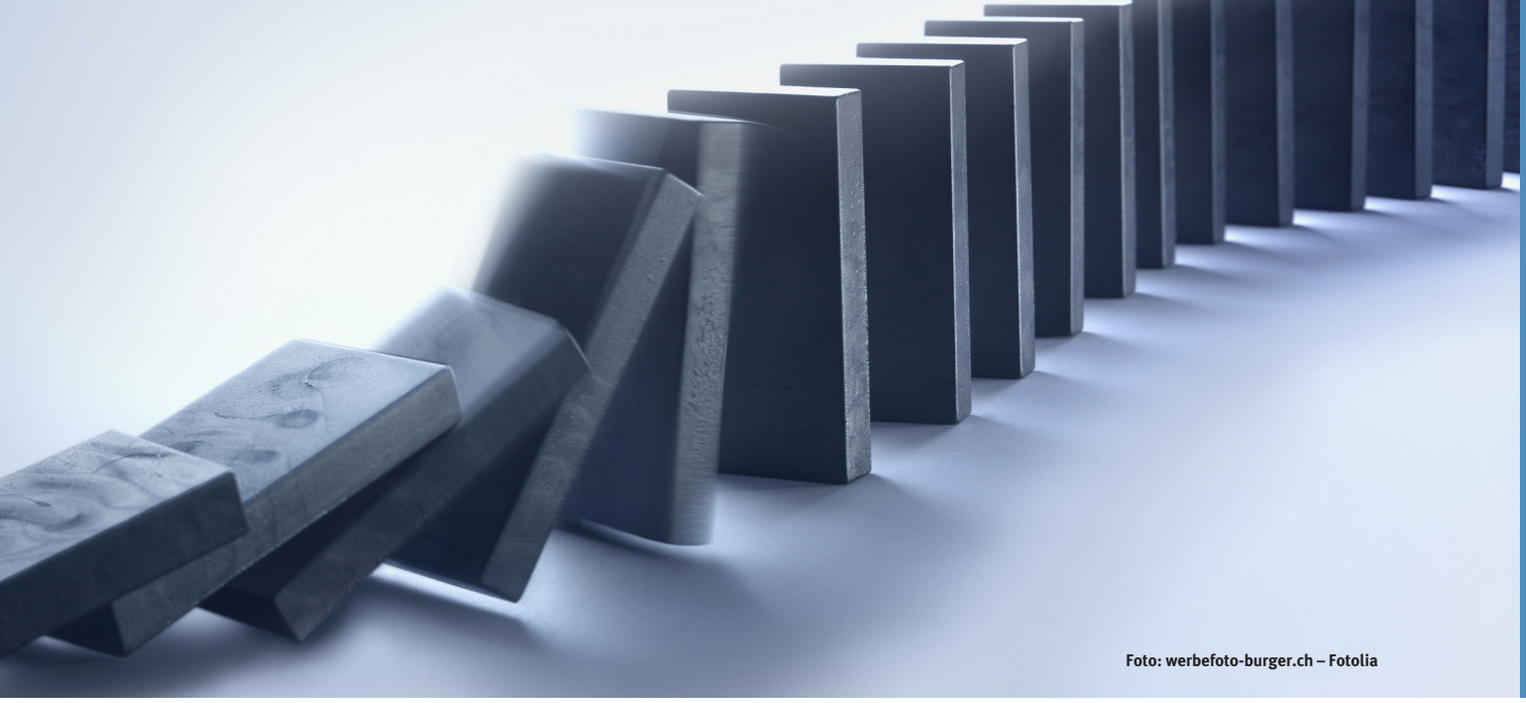

Foto: werbefoto-burger.ch – Fotolia

Ein wichtiger Impuls

Auswirkungen des IT-Sicherheitsgesetzes auf Krankenhäuser

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 getretenen IT-Sicherheitsgesetz. Doch wie wirken sich die Gesetzesvorschriften konkret aus? Was ist wirklich notwendig und was nicht? Diese Fragen beantworten Randolf-Heiko Skerka, Experte für Informationssicherheits-Managementsysteme und Prof. Dr. Andreas Becker, Berater für Einrichtungen im Gesundheitswesen.

Das Thema „IT-Sicherheit" spielt im Gesundheitswesen nicht erst seit dem Frühjahr 2016, als die Ransomware „Locky" in deutschen Krankenhäusern zahlreiche Störungen verursachte, eine wichtige Rolle. Die zunehmende Digitalisierung vieler Prozesse (z. B. durch Krankenhausinformationssysteme (KIS) oder elektronische Patientenakten) führt dazu, dass IT- und Informationssicherheit an Bedeutung gewinnen und die Öffentlichkeit ein angemessenes Maß an IT-Sicherheit innerhalb des Gesundheitswesens fordert. Dies lässt sich unter anderem aus dem allgemein gestiegenen Interesse zum Thema IT-Sicherheit und Datenschutz ableiten.

Der Gesetzgeber folgte diesem Trend mit dem im Juli 2015 in Kraft getretenen „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz). Das IT-Sicherheitsgesetz wurde mit dem Ziel in Kraft gesetzt, diejenigen („kritischen") Infrastrukturen zu schützen, die für das Gemeinwesen von zentraler Bedeutung sind. Zu den Kritischen Infrastrukturen gehören: „[...] Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden" (§ 2 Absatz 10). Neben dem Gesundheitswesen sind aus Sicht des Gesetzgebers demnach auch andere Branchen von wesentlicher Bedeutung. Derzeit wirkt sich das IT-Sicherheitsgesetz besonders auf Energieversorgungsunternehmen aus.

Randolf-Heiko Skerka
Bereichsleiter Informationssicherheits-Managementsysteme
SRC Security Research & Consulting GmbH
Bonn

Prof. Dr. Andreas Becker
Institut Prof. Dr. Becker
Rösrath

Die Drei Säulen des IT-Sicherheitsgesetzes

Die Sicherheitskonzeption durch das IT-Sicherheitsgesetz baut generell auf drei Säulen auf:

1. Sicherstellung eines Mindestniveaus an IT-Sicherheit (Art. 1 §8a (1))

Dies verpflichtet die Betreiber kritischer Infrastrukturen, technische und organisatorische Vorkehrungen nach dem Stand der Technik zur Vermeidung von IT-Störungen/Ausfällen zu treffen.

2. Nachweis des angemessenen Mindestniveaus an IT-Sicherheit (Art. 1 §8a (3))

Das sicherzustellende Mindestniveau an IT-Sicherheit müssen betroffene Unternehmen durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachweisen.

3. Meldepflicht erheblicher IT-Sicherheitsvorfälle an das BSI (Art. 1 §8b)

Über eine einzurichtende Kontaktstelle müssen sowohl sicherheitsrelevante Informationen (z. B. über kritische Sicherheitsvorfälle) an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet, als auch von diesem entgegengenommen werden können (z. B. Informationen über branchenspezifische, systematische Angriffe).

Da bislang konkrete Antworten auf die Frage „WER hat WAS bis WANN zu tun?“ ausstehen, führt das IT-Sicherheitsgesetz und dessen Anforderungen im Gesundheitswesen zu breiten Diskussionen und großer Verunsicherung. In diesem Artikel soll – soweit möglich – der voraussichtliche Handlungsbedarf für Krankenhäuser unter Berücksichtigung des erwarteten Zeithorizonts abgeschätzt und beleuchtet werden. Diese Fragen werden erst mit den auf das IT-Sicherheitsgesetz aufbauenden Rechtsverordnungen beantwortet.

Für die Sektoren Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung wurde die Rechtsverordnung bereits im Mai 2016 veröffentlicht. Die unter anderem für das Gesundheitswesen relevante Rechtsverordnung soll bis Anfang 2017 als Änderungsverordnung folgen.

Sektorstudie „Gesundheit“, Branchenstandard und Rechtsverordnung

In die Rechtsverordnungen fließen Informationen ein, die im Rahmen von Sektorstudien erhoben wurden. Die im Auftrag des BSI erstellte und Anfang Mai 2016 veröffentlichte „Sektorstudie Gesundheit“ bieten einen umfassenden Überblick über den spezifischen Stand der IT-Sicherheit und die IT-gestützten kritischen Dienstleistungen im Gesundheitssektor. Neben der Beurteilung akuter Sicherheitslücken sollte untersucht werden, welche Auswirkungen Störungen oder gar Ausfälle der eingesetzten IT-Systeme auf die Qualität der kritischen Versorgungsdienstleistungen haben könnten. Die Studie lässt sich grob in die folgenden fünf Themengebiete einteilen:

- Überblick über den Sektor „Gesundheitswesen“
- kritische Versorgungsdienstleistungen des Gesundheitswesens
- IT- und TK-Vorfälle (z. B. die Auswirkungen der Schadsoftware „Locky“ zu Beginn des Jahres 2016)
- regulatorische Vorgaben sowie Stand der Technik der IT-Sicherheit
- aus den Erkenntnissen resultierende Handlungsempfehlungen

Das Niveau der IT-Sicherheit wurde für die einzelnen Branchen des Sektors Gesundheit in den Kategorien Netzwerksicherheit, Endgerätesicherheit, Nachrichtensicherheit, Websicherheit, Datensicherheit, Identitäts- und Zugriffsverwaltung sowie mobile Sicherheit analysiert. Die Ergebnisse wurden im Rahmen von Interviews mit Vertretern des Sektors Gesundheitswesen ermittelt. Dazu haben Betreiber, Verbände und weitere Experten ihre Einschätzungen bezüglich des Umsetzungsgrades verschiedener Sicherheitskonzepte innerhalb des Gesundheitswesens abgegeben.

Im Rahmen der Untersuchung hat sich gezeigt, dass die stationäre Versorgung in vielen Krankenhäusern stark durch IT unterstützt wird und die effiziente und effektive Erbringung der Versorgungsdienstleistung maßgeblich von den genutzten IT-Systemen abhänge. In der Folge hängt die Versorgungsleistung eines Krankenhauses stark von der unterstützenden IT ab.

Dabei variiere der Grad der IT-Sicherheit in der Branche zwischen den einzelnen Leistungserbringern laut der Studie stark. Während große Häuser, insbesondere Universitätskliniken, um die Bedeutung des Themas „IT-Sicherheit“ wissen und zum Teil aktiv, beispielsweise durch die Umsetzung von Sicherheitsmaßnahmen entsprechend eines Sicherheitskonzeptes angehen, behandeln kleineren Krankenhäusern in ländlichen Gebieten das Thema aus Budget- und Personalmangel eher mit untergeordneter Priorität. Dort sind die Komplexität der Anwendungslandschaft und damit die Herausforderungen für die IT-Sicherheit etwas geringer (Sektorstudie „Gesundheit“, S. 158).

Erst mit der noch ausstehenden Rechtsverordnung wird beantwortet, welche Krankenhäuser die Vorgaben des IT-Sicherheitsgesetzes umsetzen müssen und welches Maß an IT-Sicherheit zu erreichen ist. Erste Hinweise gibt die bereits im Mai 2016 veröffentlichte erste „Ministerverordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“ (BSI KRITIS-VO), welche Vorgaben für die Sektoren Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung definiert. Als Kritische Infrastruktur in diesen Sektoren gilt demnach eine Anlage, welche die Versorgung von 500.000 Personen sicherstellt. Dass diese Zahl auch für das Gesundheitswesen als Maßstab gelten wird, ist wahrscheinlich, wird aber erst Anfang 2017 mit der erforderlichen Änderungsverordnung festgelegt sein.

Zusammenfassend lässt sich feststellen, dass sich ohne die Rechtsverordnung kein konkreter Handlungsbedarf ableiten lässt. Aus den Erfahrungen der Sektoren Energie, Informationstechnik und Telekommunikation sowie Wasser und Ernährung, für die bereits eine Rechtsverordnung veröffentlicht wurde, lässt sich aber ableiten, dass insbesondere große Krankenhäuser die Vorgaben werden umsetzen müssen. Welches Maß an IT-Sicherheit jedoch zu erreichen ist, ist nicht konkret bekannt. Für diejenigen Häuser, die sich bisher nicht oder nur im geringen Maße mit IT-Sicherheit auseinandergesetzt haben, dürfte jedoch Handlungsbedarf bestehen.

Die Herausgeber der Sektorstudie haben verschiedene Handlungsempfehlungen für die Betreiber im Gesundheitswesen erarbeitet. Die nachfolgend aufgeführten, wichtigsten Handlungsanweisungen sollten laut Sektorstudie so schnell wie möglich umgesetzt werden, um den Grad der IT-Sicherheit in der Einrichtung zu erhöhen. Die akuten technischen Maßnahmen umfassen (Sektorstudie „Gesundheit“, S. 170):

- Absicherung von unkontrollierten Fernwartungszugängen
- Adressierung von potenziellen Schwachstellen in IT-basierten insbesondere vernetzten Medizinprodukten
- Ausbau von Netzwerkzugangskontrollen & Mobile Device Management
- Trennung von medizinischen und nichtmedizinischen Netzwerken

Weiter werden kurzfristig zu behebende Handlungsanweisungen zur der Kategorie „Notwendige Schritte zur Umsetzung der Vorgaben aus dem IT-Sicherheitsgesetz“ vorgestellt (Sektorstudie „Gesundheit“, S. 171):

- Aktivere Mitgestaltung der Umsetzung des IT-Sicherheitsgesetzes durch die Branchen
- Gründung eigener Branchenarbeitskreise beziehungsweise Teilnahme an existierenden Arbeitskreisen
- Intensivierung der Arbeit im existierenden Branchenarbeitskreis, insbesondere zur Entwicklung und Umsetzung von Branchenstandards

Das Fazit der Sektorstudie ist, dass der deutsche Gesundheitssektor im Vergleich zu den anderen Sektoren verhältnismäßig geringeres Bedrohungspotenzial hinsichtlich des Ausfalls kritischer Infrastrukturen besitzt. Aber aufgrund des bestehenden Kostendrucks in diesem Sektor, blieben dringend erforderliche Investitionen in eine zunehmende Professionalisierung der IT noch immer aus. Die Studie kommt zu dem Schluss, dass die vorhandenen IT-Sicherheitslücken bislang noch nicht offensiv aufgedeckt beziehungsweise ausgenutzt wurden. Davon auszugehen, dass dies so bleibe, wäre allerdings fahrlässig. Durch die starke Zunahme an Branchen und sektorübergreifender Vernetzung zwischen den Beteiligten ▶

des Gesundheitswesens sei eine gestiegene Gefährdung durch Ausfälle von größeren Teilen der Infrastruktur zu erwarten, unter anderem durch die Einführung der Telematikinfrastruktur (TI), die einen Großteil der Leistungserbringer, sämtliche Kostenträger und die gesetzlich versicherten Bürger miteinander vernetze. Die konsequente Umsetzung des IT-Sicherheitsgesetzes in Verbindung mit den empfohlenen Maßnahmen werde dazu beitragen, das gestiegene Gefährdungspotenzial wirkungsvoll zu adressieren (Sektorstudie „Gesundheit", S. 177):

Generelle Bedeutung von Informationssicherheit im Krankenhaus

Die Herausgeber der Sektorstudie stellten fest, dass über die verschiedenen Branchen hinweg in den durchgeführten Interviews eine tendenziell eher ablehnende Haltung gegenüber dem „IT-Sicherheitsgesetz" festzustellen war (Sektorstudie „Gesundheit", S. 175).

Ursache ist, dass der Sinn des IT-Sicherheitsgesetzes durch die Verantwortlichen in Frage gestellt wird. Diese sehen nur die zusätzlichen Kosten und den Mehraufwand der zur Einhaltung der Vorschriften betrieben werden muss. Die übrigen Krankenhausvorschriften berühren das Thema IT-Sicherheit nur am Rande, obwohl die IT-Sicherheit in Krankenhäusern, in denen eine gut funktionierende und sichere IT für das Patientenwohl von besonderer Bedeutung ist, zunehmend an Bedeutung gewinnt.

Die Haftungsfrage, das Aufsetzen eines Qualitätsmanagements und die grundsätzliche Notwendigkeit eines Risikomanagementsystems sollten den Krankenhäusern nicht erst seit dem IT-Sicherheitsgesetz bekannt sein. Dies sind auch zentrale Themen der KontraG, GmbHG, AGG und der KQM-RL. Diese Aspekte, die den Grundstein für ein Informationssicherheits-Managementsystem (ISMS) legen, sollten bereits in jedem Krankenhaus vorhanden sein.

25. Juli 2015	**Inkrafttreten des IT-Sicherheitsgesetzes**
03. Mai 2016	**Inkrafttreten der Rechtsverordnung Teil 1**
Zur Bestimmung Kritischer Infrastrukturen für vier der sieben KRITIS-Sektoren (ITK, Energie, Wasser, Ernährung)	
Q1 2017	**Inkrafttreten der Rechtsverordnung Teil 2**
Zur Bestimmung Kritischer Infrastrukturen für die letzten drei der sieben KRITIS-Sektoren (Finanz- und Versicherungswesen, Transport und Verkehr sowie Gesundheit)	
bis Q3 2017	**Benennung Kontaktstelle für Vorfallsmeldungen**
Betroffene Unternehmen aus den Sektoren Finanz- und Versicherungswesen, Transport und Verkehr sowie Gesundheit haben ab Veröffentlichung der Rechtsverordnung sechs Monate Zeit, dem BSI eine Kontaktstelle für Vorfallsmeldungen zu benennen.	
vorr. Q1 2019	**Umsetzung der Anforderungen des IT-Sicherheitsgesetzes für u. a. Gesundheitswesen**
Betroffene Unternehmen aus den Sektoren Finanz- und Versicherungswesen, Transport und Verkehr sowie Gesundheit haben ab Veröffentlichung der Rechtsverordnung zwei Jahre Zeit, ihre IT nach dem Stand der Technik abzusichern.	

Abb.: Zeitachse in Bezug auf KRITIS

Wie sieht die Zeitachse in Bezug auf KRITIS aus

Seit dem Zeitpunkt der Veröffentlichung des IT-Sicherheitsgesetztes im Juli 2015 läuft ein Zeitplan ab, der in der Abbildung ▶ dargestellt wird. Wesentlich ist der Zeitpunkt der Veröffentlichung der für die Krankenhäuser relevanten Rechtsverordnung, die Anfang 2017 erwartet wird.

Auch wenn derzeit die Zertifizierungen nach ISO/IEC 27001 oder nach ISO 27001 auf Basis von IT-Grundschutz in den Fokus gerückt werden, muss vor einem Aktionismus und „vorrausschauendem Gehorsam" durch vorschnelle Umsetzung und Zertifizierungen gewarnt werden. Ob vorliegende Zertifizierungen ausreichen, den Nachweis eines angemessenen Niveaus an IT-Sicherheit zu erbringen, entscheidet das BSI. Es kann erwartet werden, dass sich branchenspezifische Standards und Nachweisverfahren etablieren, um den Anforderungen des IT-Sicherheitsgesetzes gerecht zu werden. Auch die bereits bestehenden Zertifizierungen in diesem Umfeld werden eine Rolle spielen.

Impuls zur Verbesserung

Obwohl das IT-Sicherheitsgesetz wenig konkret ist, lässt sich ableiten, dass ein Impuls zur Verbesserung der IT-Sicherheit in diejenigen Branchen gegeben wird, die für das Gemeinwohl von wesentlicher Bedeutung sind. Den Branchen der Betreiber Kritischer Infrastrukturen wird zunächst die Möglichkeit gegeben, eigenständig (in Abstimmung mit dem BSI) zu definieren, welches Maß an IT-Sicherheit erforderlich ist. „Entwarnung" kann aber nur gegeben werden, wenn sich die Krankenhäuser verstärkt mit dem Thema IT-Sicherheit und dessen Auswirkung beschäftigen. Krankenhäuser, die sich noch nicht systematisch um IT-Sicherheit kümmern, werden einen hohen Initialaufwand haben, den Anforderungen des Gesetzes gerecht zu werden. Ihnen bleibt nur übrig, diese Aufgabe auf eine möglichst lange Zeitleiste zu verteilen. ■

Literatur beim Verfasser

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

Prof. Dr. Andreas Becker
Institut Prof. Dr. Becker
Nonnenweg 120a
51503 Rösrath