Foto: snyGGG – Fotolia

Welche Schritte zu gehen sind

Handlungsbedarf zur IT-Sicherheit für Krankenhäuser erkennbar

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 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.

Das IT-Sicherheitsgesetz, das im Jahr 2015 verabschiedet wurde, hatte bisher keine konkreten Auswirkungen auf Krankenhäuser. Die relevanten Schwellwerte, anhand derer betroffene Krankenhäuser identifiziert wurden, lagen für Krankenhäuser bisher nicht vor. Mit dem Referentenentwurf zur „Ersten Verordnung zur Änderung der BSI-Kritisverordnung“ liegen diese Schwellwerte für Krankenhäuser vor. Auch wenn die Änderungsverordnung noch nicht veröffentlicht ist, werden die Schwellwerte als stabil angesehen. Das IT-Sicherheitsgesetz grenzt die Pflicht auf Krankenhäuser ein, die ein definierendes Versorgungsgebiet mit „kritischen Dienstleistungen“ (kDL) abdecken. Anhand des aktuellen Referentenentwurfs „Erste Verordnung zur Änderung der BSI-Kritisverordnung“ lässt sich bereits ableiten dass ein Krankenhaus, dann als kritische Infrastruktur einzustufen ist, wenn es eine Kapazität von mehr als 30.000 vollstationäre Behandlungsfälle pro Jahr aufweist. Dies wird aus einer Versorgungsleistung von 500.000 versorgten Personen abgeleitet. Es wird geschätzt, dass deutschlandweit circa 110 Krankenhäuser betroffen sind.

Handlungsbedarf in drei Bereichen

Aus dem IT-Sicherheitsgesetz und der BSI-KritisV leitet sich für betroffene Krankenhäuser ein Handlungsbedarf in drei Bereichen ab:

1. *Meldepflicht erheblicher IT-Sicherheitsvorfälle an das BSI (§ 8b BSIG)*
   Über eine einzurichtende Kontaktstelle müssen sowohl sicherheitsrelevante Informationen (zum Beispiel über kritische Sicherheitsvorfälle) an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gemeldet, als auch von diesem entgegengenommen werden können (etwa Informationen über branchenspezifische, systematische Angriffe). Die Kontaktdaten müssen dem BSI spätestens sechs Monate nach Veröffentlichung der BSI-Kritisverordnung mitgeteilt werden.

2. *Sicherstellung eines Mindestniveaus an IT-Sicherheit (§ 8a Absatz 1 BSIG)*
   Krankenhäuser müssen technische und organisatorische Vorkehrungen nach dem geltenden Stand der Technik zur Vermeidung von IT-Störungen/Ausfäl-

len treffen. Bei der Umsetzung entsprechender Maßnahmen können vom BSI abgenommene Branchenspezifische Sicherheitsstandards (B3S) verwendet werden. Dies soll es Krankenhäusern ermöglichen, einheitliche und für sie spezifische Maßnahmen zu wählen. Da für Krankenhäuser derzeit kein abgenommener B3S vorliegt, müssen eigenverantwortlich geeignete Maßnahmen ausgewählt werden.
Hinweise auf die Erwartungshaltung des BSI leiten sich bereits aus der „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG“ ab. Insbesondere ist durch das Krankenhaus festzulegen, welche Qualität der kritischen Dienstleistung (kDL), insbesondere in Normallagen, gegebenenfalls aber auch in allgemeinen Großkrisen und IT-Krisenlagen sichergestellt werden soll. Zudem sind Anforderungen an das Risikomanagement und die abzudeckenden Themen der IT-Sicherheit definiert.

3. *Nachweis des angemessenen Mindestniveaus an IT-Sicherheit (§ 8a Absatz 3 BSIG)*
Das sicherzustellende Mindestniveau an IT-Sicherheit müssen Krankenhäuser durch Sicherheitsaudits nachweisen.

Die Nachweise über die Erreichung des Mindestniveaus müssen betroffene Krankenhäuser dem BSI spätestens zwei Jahre nach Veröffentlichung der BSI-KritisV vorlegen.

Die Erbringung des Nachweises setzt die Prüfung durch einen qualifizierten Prüfer voraus, der die Befähigung besitzt, Prüfungen gem. § 8a Absatz 3 des BSI-Gesetzes durchzuführen. Auf die Befähigung des Prüfers ist zu achten, da das BSI erst nach Abschluss der Prüfung die Befähigung des Prüfers kontrolliert.

Auch wenn dies nicht explizit erwähnt wird, leitet sich aus dem § 8a Absatz 1 die Konzeption und der Aufbau eines Informationssicherheitsmanagementsystems (ISMS) bei Krankenhäusern ab.

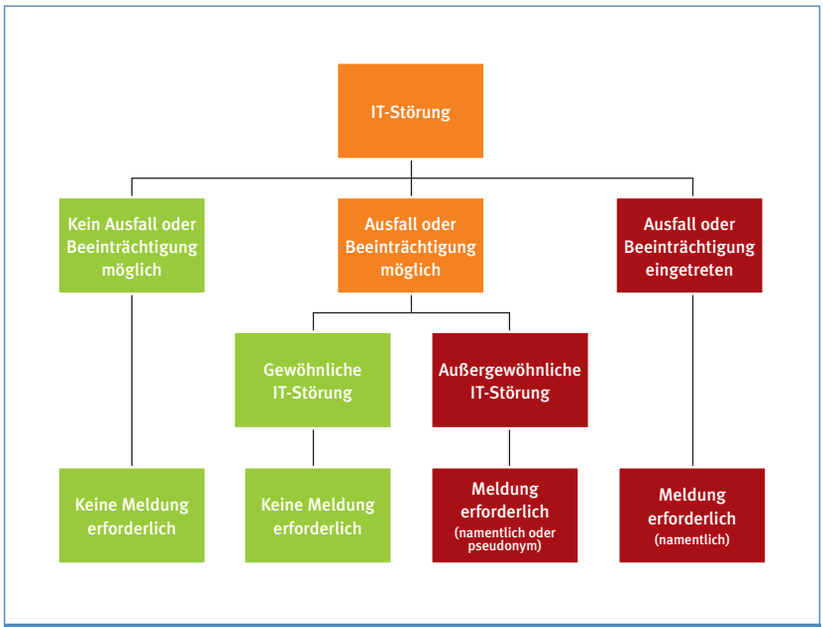

Abb. 1: Meldeprozess „IT-Störungen“

Umsetzung der Anforderungen

Die Umsetzung der Anforderungen des IT-Sicherheitsgesetzes bestehen im Wesentlichen aus den Aktivitäten:

- Etablierung einer Kontaktstelle und Registrierung beim BSI,
- Sicherstellen der Erreichung eines erforderlichen Maßes an IT-Sicherheit sowie
- Erbringen des Nachweises der Erreichung eines erforderlichen Maßes an IT-Sicherheit.

Die ersten beiden Aktivitäten können unabhängig voneinander angegangen werden, jedoch bietet sich die Kombination beider Schritte an. Nachfolgend werden die einzelnen Schritte bei der Umsetzung skizziert.

Schritt 1:
Etablierung einer Kontaktstelle
Das geänderte BSI-Gesetz (§ 8 b BSIG) verpflichtet betroffene Krankenhäuser sowohl, dem BSI erhebliche IT-Störungen in anonymisierter Form zu melden, als auch dafür Sorge zu tragen, dass das BSI ständig (7x24) in der Lage ist, den betroffenen Krankenhäusern IT-Sicherheitsinformationen über eine zu benennende Kontaktstelle mitzuteilen.
Aus den eingegangenen Meldungen leitet das BSI ein Lagebild ab, welches die Grundlage für beispielsweise Warn- und Alarmierungsmeldungen sowie konkrete Handlungsempfehlungen ist. Ziel ist es, Betreiber kritischer Infrastrukturen frühzeitig auf Angriffe oder Ausfälle vorzubereiten beziehungsweise Abwehrmaßnahmen zu ergreifen. Die Meldepflicht besteht bei Störungen, die bereits zu einem Ausfall oder Beeinträchtigung geführt haben, oder hierzu führen können (▶Abb. 1).

Um die Meldungen geordnet vom BSI entgegenzunehmen oder an dieses abzugeben, ist die Einrichtung geeigneter Meldeprozesse erforderlich. ▶

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

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

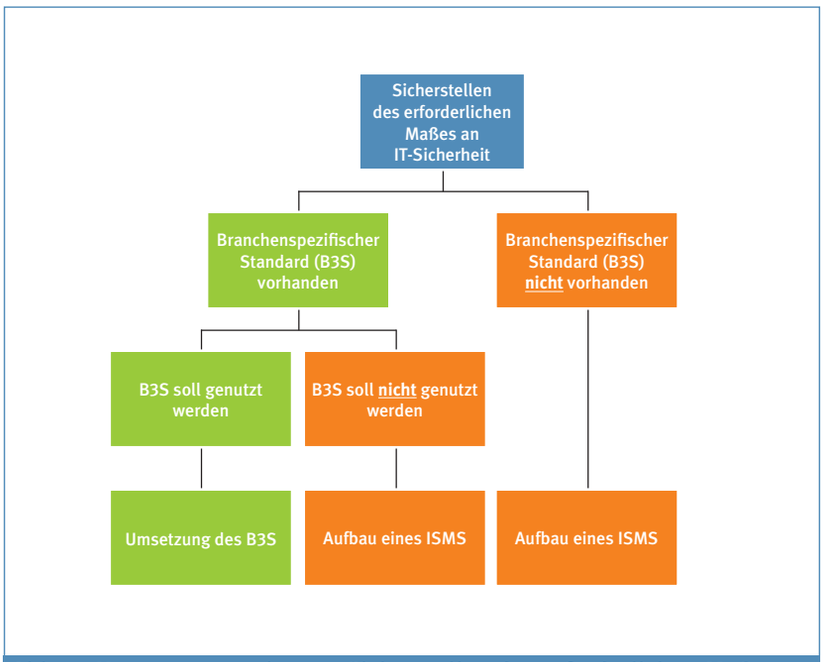

Abb. 2: Umsetzungsoptionen „Sicherstellen des erforderlichen Maßes an IT-Sicherheit“

Schritt 1a:
Festlegung des Ansprechpartners des Krankenhauses
Im Rahmen des Registrierungsprozesses muss das Krankenhaus gegenüber dem BSI einen Ansprechpartner benennen. Gemäß Registrierungsformular ist „die Aufgabe des Ansprechpartners der Organisation […], dem BSI gegenüber Änderungen bezüglich der Kontaktstelle mitzuteilen. Das BSI kontaktiert den Ansprechpartner bei allen organisatorischen Fragestellungen, zum Beispiel zur Überprüfung und/oder Ergänzung der Kontaktdaten“.

Schritt 1b:
Einrichtung und Etablierung einer Kontaktstelle gemäß § 8b Absatz 3 BSIG
Damit das BSI dem Krankenhaus IT-Sicherheitsinformationen zukommen lassen kann, ist die Erreichbarkeit der Kontaktstelle an 24 Stunden sieben Tage die Woche zu gewährleisten.

Da das BSI an die Qualität der eigenen Meldungen in Richtung des Krankenhauses, wie auch die aus Richtung des Krankenhauses kommenden Meldungen, gewisse Anforderungen stellt, und die Erreichbarkeit der Kontaktstelle sichergestellt werden muss, sind in der Regel geeignete Meldeprozesse aufzubauen und zu etablieren.

Schritt 1c:
Registrierung auf dem Melde- und Informationsportal für Betreiber

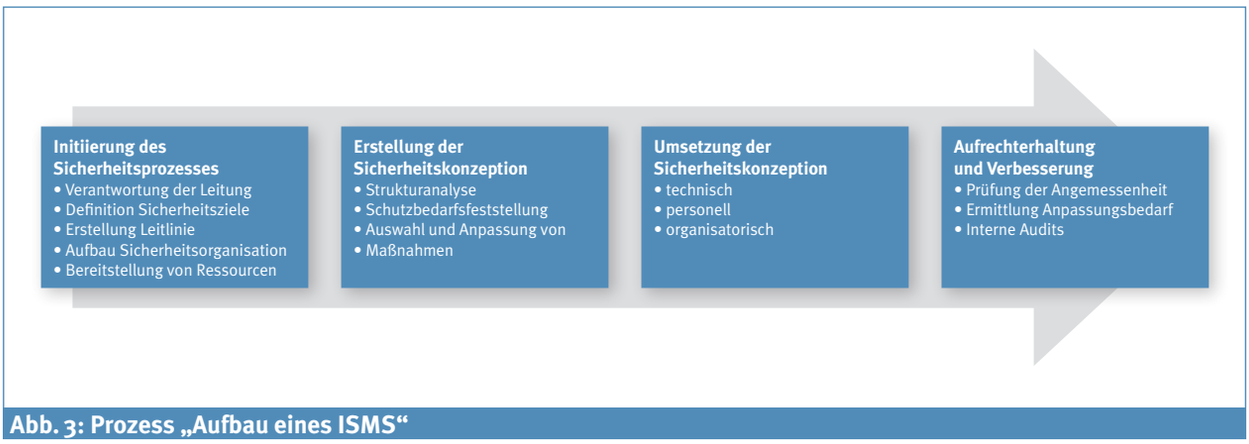

Abb. 3: Prozess „Aufbau eines ISMS“

Kritischer Infrastrukturen im Rahmen des IT-Sicherheitsgesetzes

Um der Meldepflicht nachzukommen, muss das Krankenhaus eine Registrierung auf dem „Melde- und Informationsportal für Betreiber Kritischer Infrastrukturen im Rahmen des IT-Sicherheitsgesetzes“ vornehmen. Anschließend werden die zur Meldepflicht erforderlichen Informationen (Meldeformular, Anleitung zur Durchführung einer Meldung) bereitgestellt.

Schritt 2:
Sicherstellen des erforderlichen Maßes an IT-Sicherheit

Gemäß § 8a BSIG müssen betroffene Krankenhäuser „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind“. Als Maß wird hierbei der „Stand der Technik“ angesetzt. Die Einhaltung dieser gesetzlichen Anforderung beinhaltet insbesondere die Umsetzung eines geeigneten Risikomanagements sowie die Umsetzung und den Betrieb der hieraus abgeleiteten Maßnahmen. Dies sind identische Ziele, die auch Informationssicherheits-Managementsysteme (ISMS) definieren.
Die Erreichung des Standes der Technik kann durch die Umsetzung eines vom BSI anerkannten branchenspezifischen Sicherheitsstandards (B3S) gemäß § 8a Abs. 2 BSIG erfolgen. Da für Krankenhäuser derzeit kein solcher branchenspezifischer Sicherheits- standard vorhanden ist, empfiehlt sich der Aufbau eines ISMS nach etablierten Vorgehensweisen, wie sie zum Beispiel im BSI-Standard 100-2 des BSI niedergelegt ist. Konkrete Vorgaben oder Verpflichtungen, dass eine Orientierung an vorhandenen Standards erfolgen muss, macht das BSI jedoch nicht. Insbesondere gibt es keine Pflicht, ein zertifiziertes ISMS (etwa nach ISO27001) vorzuweisen. Ob sich hieraus Vorteile für das Krankenhaus ergeben, kann und sollte das Krankenhaus individuell abschätzen (▶Abb. 2, Seite 59.).

Aufbau und Implementierung eines ISMS

Die Vorgehensweise zum Aufbau eines ISMS ist generisch und geeignet, ein ISMS nach diversen etablierten Standards umzusetzen (▶Abb. 3).

Ein ISMS sollte, wie auch andere Managementsysteme, nicht dem Selbstzweck dienen, sondern zur Wertsteigerung einer Organisation beitragen. Es ist kein Produkt „von der Stange“, sodass langfristig nur individuelle und gut umgesetzte ISMS zu einem Return of Investment (RoI) führen. Gleichzeitig muss beachtet werden, dass die Kosten für die Umsetzung von Maßnahmen der Ersparnis durch mögliche Schäden angemessen sind.
Die individuelle ISMS-Planung hat weiter den Vorteil, dass in der Regel bereits vorhandene Dokumente, Prozesse und Sicherheitsmaßnahmen direkt für den Aufbau des ISMS genutzt werden können und dadurch trotz einer Verringerung des Aufwandes eine höhere Akzeptanz bei den Beschäftigten erreicht werden kann.

Fazit

Zusammenfassend lässt sich feststellen, dass sich – auch wenn die Änderungsverordnung zur BSI-Kritisverordnung noch nicht veröffentlicht ist – der Handlungsbedarf für Krankenhäuser konkretisiert. Innerhalb der nächsten zwei Jahre müssen betroffene Krankenhäuser das erforderliche Maß an IT-Sicherheit erreichen und nachweisen. Eine Strategie des Abwartens ist nicht angebracht, da sich die Erwartungshaltung des BSI durch verschiedene Veröffentlichungen konkretisiert. ■

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