Foto: sdecoret – Fotolia

(K)eine Aufgabe für die IT?

Informationssicherheit und ISMS

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 Informationssicherhetis-Managementsysteme und Prof. Dr. Andreas Becker, Berater für Einrichtungen im Gesundheitswesen

Im Juli 2015 ist das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)“ in Kraft getreten. Der in der Zwischenzeit vorliegende Referentenentwurf des Bundesministeriums des Inneren zur ersten „Verordnung zur Änderung der BSI-Kritisverordnung“ beinhaltet insbesondere auch den neuen § 6 „Sektor Gesundheit“. In diesem werden die folgenden vier kritischen Dienstleistungen im Sinne des § 10 Absatz 1 Satz 1 des BSI-Gesetzes für den Sektor Gesundheit identifiziert:

1. Medizinische Versorgung in den Bereichen Aufnahme, Diagnose, Therapie, Unterbringung/Pflege und Entlassung

2. Versorgung mit Medizinprodukten, die Verbrauchsgüter sind, in den Bereichen Herstellung und Abgabe

3. Versorgung mit verschreibungspflichtigen Arzneimitteln in den Bereichen Herstellung, Distribution und Abgabe

4. Laboratoriumsdiagnostik in den Bereichen Transport und Analytik

Welche Krankenhäuser gehören dazu?

Im Anhang 5 des Referentenentwurfs ist ein Krankenhaus definiert als „Standort oder Betriebsstätten eines nach § 108 des fünften Buches Sozialgesetzbuch in der jeweils geltenden Fassung zugelassenen Krankenhauses, die für die Erbringung stationärer Versorgungsleistungen notwendig sind“.

Gemäß der Begründung zum Referentenentwurf (Teil B) sind „räumlich getrennte Standorte oder Betriebsstätten eines Krankenhauses als Anlage anzusehen, wenn sie aus planungsrechtlicher Sicht, etwa aus organisatorischen, technischen, medizinischen oder sicherheitsbezogenen Aspekten, als Einheit betrachtet werden“.

Sowohl medizinische Gebrauchsgüter wie CT- oder Röntgenapparate als auch Labore werden als Nebeneinrichtungen von Krankenhäusern gezählt. In Bezug auf das IT-Sicherheitsgesetz sind diese Nebeneinrichtungen für Krankenhäuser nicht separat noch einmal zu berücksichtigen.

Der für die Anlagenkategorie Krankenhaus vorgesehene Schwellwert liegt im derzeitigen Entwurf bei einer vollstationären Fallzahl von 30.000 pro Jahr. Im Referentenentwurf wird davon ausgegangen, dass 110 Kranken-

häuser als kritisch einzustufen sind, da sie aufgrund von Größe und erbrachtem Leistungsspektrum eine hinreichende Bedeutung für die medizinische Versorgung der Allgemeinheit haben.

Interessanterweise beruft man sich bei der Festlegung des Schwellenwertes auf die „Einschätzung von Experten und betroffenen Branchenverbänden“ (Begründung, Teil B), eine weiterführende Rationale wird nicht genannt. Würden die 110 in Frage kommenden Krankenhäuser im Mittel 50.000 Patienten pro Jahr vollstationär versorgen, so wären dies insgesamt 5,5 Millionen Fälle. Bezogen auf das Jahr 2015 mit rund 19 Millionen vollstationäre Fällen entspricht dieser Wert rund 29 %. Es kann daher spekuliert werden, dass der aktuelle Schwellenwert nur zum Einstieg gewählt wurde und in den nächsten Jahren abgesenkt wird.

IT-Sicherheit ist nicht gleich Informationssicherheit

Auch wenn es sich um ein Gesetz zur IT-Sicherheit handelt, ist davon auszugehen, dass auch für den Sektor Gesundheit ein Informationssicherheitsmanagementsystem (ISMS) in den betroffenen Krankenhäusern einzuführen ist. Dabei ist IT-Sicherheit nicht gleich Informationssicherheit.

Üblicherweise verantwortet die IT-Abteilung die Betreuung der IT-Systeme und damit auch deren Sicherheit. Dazu gehören sowohl die Betreuung (zum Beispiel das Benutzer- und Rechtemanagement) als auch der Schutz (zum Beispiel das Patch- und Konfigurationsmanagement) der IT-Systeme beziehungsweise der elektronisch gespeicherten Daten, aber auch die Gewährleistung der Funktionalität, Verfügbarkeit und der Zuverlässigkeit.

Bei der Informationssicherheit steht allgemein der Schutz von Informationen im Fokus. Dabei werden neben digitalen auch analoge Informationen berücksichtigt. Darunter können zum Beispiel Patientenunterlagen oder auch ausgestellte Rezepte und abgeschlossene Verträge in Papierform fallen. Einen kontinuierlichen Prozess in der Informationssicherheit stellen das Identifizieren und Bewerten von Risiken, verbunden mit der Umsetzung von Maßnahmen zur Reduzierung oder sogar Eliminierung dar.

„Auch wenn es sich um ein Gesetz zur IT-Sicherheit handelt, ist davon auszugehen, dass auch für den Sektor Gesundheit ein Informationssicherheitsmanagementsystem (ISMS) in den betroffenen Krankenhäusern einzuführen ist.“

Die hierfür zugrundeliegenden Schutzziele umfassen die Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität. Im Glossar des IT-Grundschutz-Katalogs des BSI sind diese Begriffe wie folgt definiert:

- *Vertraulichkeit:*
  „Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in der zulässigen Weise zugänglich sein.“

- *Integrität:*
  „Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.“

- *Verfügbarkeit:*
  „Die Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Anwendungen oder IT-Netzen oder auch von Informationen ist vorhanden, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.“

- *Authentizität:*
  „Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.“

Die Informationssicherheit beinhaltet zahlreiche Bereiche, wie zum Beispiel Personal, Organisation, Verantwortlichkeiten und physischer Sicherheit, aber insbesondere auch die Sicherheit und das Management der IT-Systeme. Somit ist die IT-Sicherheit ein Bestandteil der Informationssicherheit. Die Verantwortung für die Informationssicherheit und das damit verbundene ISMS sollte bei der Geschäftsführung liegen. Da die IT-Abteilung einen wichtigen Teil des gesamten Managementsystems darstellt, sollte sie frühzeitig und intensiv in den Aufbau und den Betrieb des ISMS eingebunden sein (▶Abb., Seite 60).

Bestehendes nutzen

In Krankenhäusern ist bereits heute die Qualitätsmanagement- ▶

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

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

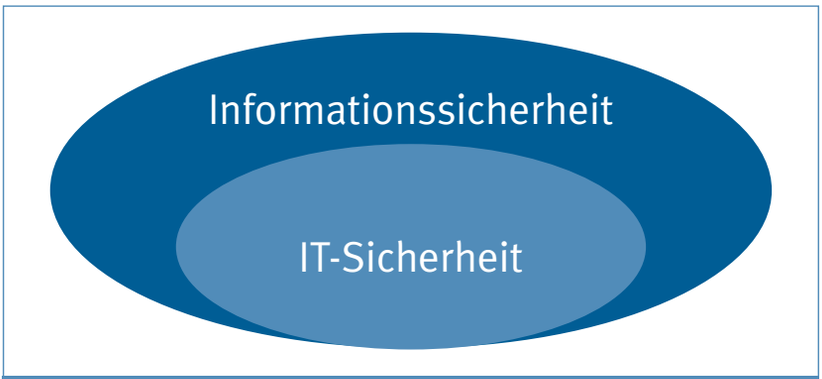

Abb.: IT-Sicherheit ist ein Bestandteil der Informationssicherheit.

Richtlinie des Gemeinsamen Bundesausschusses (QM-RL) umzusetzen. Diese dort aufgeführten Prozesse zum Qualitäts- und Risikomanagement sowie die konsequente Forderung zur Anwendung des PDCA-Zyklus können als Basis für das Implementieren eines ISMS fungieren. So kann beispielsweise ein ISMS nach ISO 27001 ohne weiteres in ein vorhandenes Qualitätsmanagement nach ISO 9001 integriert werden. Aufgrund der einheitlichen Struktur gängiger Managementsysteme und der Forderung von Transparenz, Dokumentation und der Einbindung aller Mitarbeiter ist davon auszugehen, dass sehr wahrscheinlich wesentliche Management-Prozesse bereits vorhanden sind.

Diese sollten vergleichsweise einfach um die Gegebenheiten der Informationssicherheit erweitert und genutzt werden können. Dadurch lassen sich zum einen die notwendigen Ressourcen bündeln beispielsweise durch kombinierte Audits, zum anderen steigt durch eine schlanke Organisation die Akzeptanz der Mitarbeiter für die Managementsysteme und schafft klare Strukturen sowie widerspruchsfreie Kommunikation nach Innen und Außen.

Die grundsätzliche Herangehensweise zum Aufbau eines ISMS besteht dabei insbesondere aus den folgenden Schritten:

1. *Anforderungen identifizieren:*
   Der erste Schritt für den Aufbau eines ISMS ist die Bestimmung der anwendbaren Gesetze und anderer Auflagen. Dies können sowohl externe Anforderungen, beispielsweise aufgrund existierender Verträge, als auch interne Anforderungen sein, weil unter Umständen bereits andere Managementsysteme, wie zum Beispiel ein QMS nach ISO 9001 existieren, in die das ISMS integriert werden soll.

2. *Sicherheitspolitik definieren:*
   Ziel ist die abstrakte Festlegung des zu erreichenden Sicherheitsniveaus.

3. *Definition des Geltungsbereich:*
   Ziel ist die Bestimmung der zu schützenden Prozesse. Darauf aufbauend können zu berücksichtigende Systeme, Informationen, Personen und weitere Ressourcen identifiziert werden. Dabei wird auf Basis der zuvor erkannten Anforderungen festgelegt, welche „Geschäftsprozesse“ geschützt werden sollen. Im Kontext des IT-Sicherheitsgesetzes wird hier insbesondere der Geschäftsprozess „stationäre Krankenversorgung“ zu sehen sein.

4. *Inventarisierung der Werte:*
   Bevor eine Konzeption zum Schutz erfolgen kann, müssen zuvor die schützenswerten Informationen beziehungsweise Werte oder Assets, und darauf aufbauend die zugrunde liegenden IT-Systeme sowie die für den ordnungsgemäßen Betrieb benötigten Ressourcen erfasst werden.

5. *Bestimmung des Schutzbedarfs:*
   Mit dem Ziel, die stationäre Krankenversorgung zu schützen, muss für alle erfassten Assets deren Schutzbedarf bestimmt werden. Darauf aufbauend vererbt sich der Schutzbedarf auf die zur Verarbeitung genutzten beziehungsweise die die stationäre Krankenversorgung unterstützenden Systeme, die dafür genutzten Räume und so weiter. Die weitere Anforderung der ISO 27001, jedem Asset einen Verantwortlichen zuzuordnen, kann in diesem Schritt direkt mit erledigt werden.

6. *Risikoanalyse:*
   Ausgehend von den identifizierten Assets und deren Schutzbedarf kann eine Risikoanalyse durchgeführt werden. Dabei wird idealerweise der bereits im Qualitätsmanagement vorhandene Prozess erweitert, um Risiken im Zusammenhang mit dem Verlust von Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität zu ermitteln, deren Eintrittswahrscheinlichkeit und Schadensschwere einzuschätzen sowie Kriterien für die Risikoakzeptanz oder Risikobehandlung festzulegen. Allgemeine Bedrohungen sind in generischen Katalogen zusammengestellt (wie den Gefährdungskatalogen des IT-Grundschutzes des BSI), spezifische Bedrohungen können hierbei zum Beispiel aus der „KRITIS-Sektorstudie Gesundheit“ entnommen werden. Die Einschätzung von Eintrittswahrscheinlichkeiten und Größe der Schäden kann kategorisiert erfolgen, da häufig statistische Informationen für schädigende Ereignisse nicht verfügbar oder repräsentativ sind.

7. *Auswahl und Umsetzung der Maßnahmen:*
   Nach Kenntnis und Bewertung der allgemeinen und spezifischen Risiken können angemessene Maßnahmen zum Schutz der Assets ausgewählt und umgesetzt werden. Die Risikobehandlung ist durch Maßnahmen möglich, die die Eintrittswahrscheinlichkeiten oder hervorgerufenen Schäden verringern, durch Umstrukturierung von Prozessen die Risiken verringern, Risiken transferieren (beispielsweise durch Versicherungen) oder dadurch, dass Risiken bewusst akzep-

tiert werden, wenn eine andere Behandlung nicht wirtschaftlich oder umsetzbar erscheint. Der Risikobehandlungsplan ist Teil der Pflichtdokumentation und sollte auch Informationen darüber enthalten, wann Maßnahmen umgesetzt werden sollen.

8. *Prüfung der Umsetzung und Bewertung der Maßnahmen:*
Die Wirksamkeit von Maßnahmen kann erst einsetzen, wenn sie implementiert wurden, aber auch dann ist es möglich, dass sie in einem konkreten Fall wirkungslos (geworden) sind. Neben der Revision (Prüfung der Umsetzung) ist daher auch eine Bewertung von Maßnahmen unabdingbar (Vollständigkeits- beziehungsweise Aktualisierungsprüfung). Der Umsetzungsstatus jeder Maßnahme muss dokumentiert sein, damit die Gesamtsicherheitslage jederzeit bewertet werden kann. Dies ist neben den eigentlichen Audits, bei denen der Dokumentationsstand aktiv geprüft wird, insbesondere bei Änderungen der Rahmenbedingungen sehr hilfreich, zum Beispiel für die Bewertung, ob ein neues Risiko eine aktuelle Gefahrenquelle darstellt, oder ausreichende Maßnahmen zum Schutz bereits implementiert wurden.

Informationssicherheit ist nicht nur ein Thema der IT-Abteilung, sondern adressiert jeden einzelnen Mitarbeiter. Es ist daher von Bedeutung, dass alle Mitarbeiter die Notwendigkeit des Schutzes von Informationen verstehen und sich aktiv an diesem Prozess beteiligen. Eine hohe Akzeptanz wird einfacher erreicht, wenn sich neue Regelungen nahtlos in den gelebten Alltag integrieren und von den Beteiligten verstanden wird, dass dem eventuell zusätzlich entstehenden Aufwand auch ein bedeutender Nutzen entgegensteht. Informationssicherheit ist generell ein dauerhafter Prozess und kein Produkt, welches einmalig eingekauft wird. Ein Return on Investment kann demnach nur eintreten, wenn die Sicherheitskonzeption dauerhaft Anwendung findet, gleichermaßen wirksam und angemessen ist, und von jedem Mitarbeiter getragen wird. ■

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