Foto: Zerbor – Fotolia

Prüfung zum IT-Sicherheitsgesetz

Nachweis bis Juni 2019 – Durchfallen nicht eingeplant

Von Randolf Skerka und Prof. Dr. Andreas Becker

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.

Keyword: *IT-Sicherheit, BSIG, Prüfung, Prozessablauf, Prüfungsvorbereitung*

Mit der am 31.05.2017 erfolgten Zustimmung der Bundesregierung zum Referentenentwurf der ersten Verordnung zur Änderung der BSI-Kritisverordnung (KritisV) wird diese noch im Juni 2017 in Kraft treten. Damit sind nun auch bestimmte Krankenhäuser verpflichtet, u.a. ein angemessenes Niveau an IT-Sicherheit herzustellen. Insbesondere sind diese Krankenhäuser damit gemäß § 8a Absatz 3 BSIG verpflichtet, innerhalb der kommenden zwei Jahre - also bis Juni 2019 - den Nachweis zu erbringen, dass dort ein angemessenes Maß an IT-Sicherheit erreicht ist, wo eine kritische Dienstleistung erbracht wird. Die BSI-Kritisverordnung definiert im Sektor Gesundheit als kritische Dienstleistung (kDL) die:

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

Für Krankenhäuser ist daher zumindest die kritische Dienstleistung „stationäre medizinische Versorgung“ von Bedeutung, sofern hier eine Versorgungsleistung von mindestens 30.000 vollstationären Fällen/Jahr erreicht wird. Es wird geschätzt, dass dies auf 110 Krankenhäuser zutrifft.

Das sicherzustellende Mindestniveau an IT-Sicherheit müssen betroffene Krankenhäuser dem BSI alle zwei Jahre nachweisen (▶Abb.). Hierzu sind dem BSI

erstmalig spätestens im Juni 2019 die entsprechenden Nachweise vorzulegen.

Die Erbringung des Nachweises setzt eine Prüfung durch einen qualifizierten Prüfer voraus, der die attestierte Befähigung besitzt, Prüfungen gemäß § 8a Absatz 3 des BSI-Gesetzes durchzuführen. Die betroffenen Krankenhäuser können die „Prüfende Stelle“ frei auswählen, welche ihrerseits das Prüfteam bestimmt. Hierbei ist darauf zu achten, dass die ausgewählte Prüfende Stelle auf der Webseite des BSI gelistet ist und über qualifizierte Prüfer verfügt. Ansonsten besteht die Gefahr, dass das BSI die am Ende des Prüfprozesses einzureichenden Nachweise ablehnt.

Die Durchführung der Prüfung erfolgt auf Basis einer durch den Prüfer festgelegten Vorgehensweise. Im Ergebnis der Prüfung wird eine „Liste der Sicherheitsmängel“ erstellt, die vom Krankenhaus mit dem „Nachweisdokument zu § 8a Absatz 3 BSIG“ beim BSI einzureichen ist.

Die konkrete Prüfdauer hängt von den spezifischen Gegebenheiten des Krankenhauses ab, da hier starke Unterschiede bei den verschiedenen Krankenhäusern zu erwarten sind. Die durch das BSI geschätzte Prüfdauer umfasst 20–40 Personentage.

Die Prüfdauer kann gegebenenfalls verkürzt werden, sofern frühere oder andere Prüfnachweise noch gültig sind und herangezogen werden können. Dabei sind sowohl Änderungen innerhalb der geprüften Anlage als auch bei der Gefährdungslage zu beachten.

Wie muss sich ein Krankenhaus auf die Prüfung vorbereiten?

Für das Krankenhaus ist der wesentliche erste Schritt die Festlegung des Geltungsbereiches (Scope), der den Anforderungen der BSI-Kritisverordnung unterliegt. Es wird zu erwarten sein, dass alle weiteren Schritte der Prüfung durch den Prüfer unterstützt werden und die nachfolgenden Schritte umfassen:

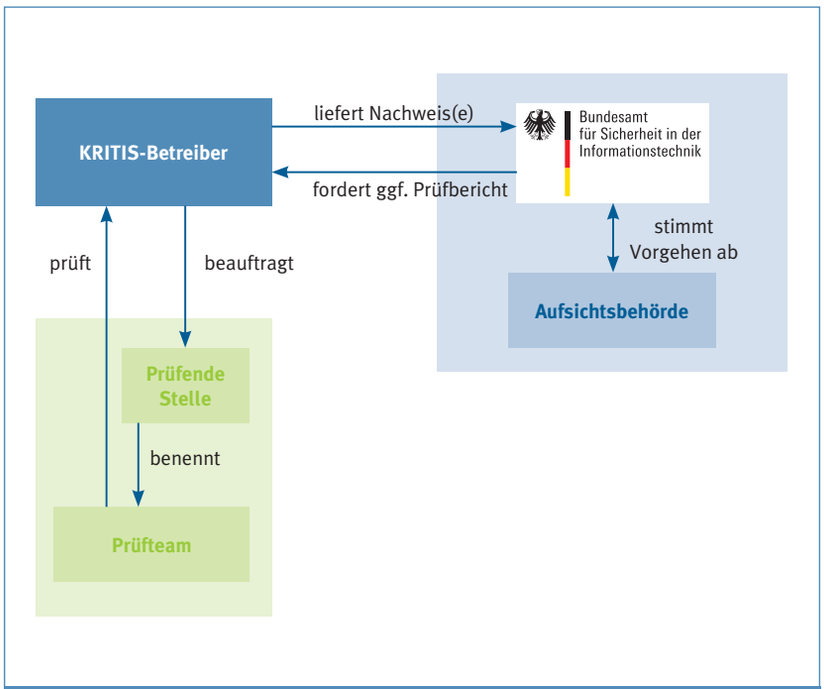

Abb. 1: Prozessablauf der Prüfung gem. § 8a Absatz 3 BSIG

1. Festlegung der Prüfgrundlage
2. Prüfung der Scopes
3. Erstellung des Prüfplans
4. Durchführung der Prüfung
5. Dokumentation des Prüfergebnisses im Prüfbericht
6. Einreichung der Nachweise beim BSI

Festlegung der Prüfgrundlage

Vor Beginn der Prüfung nach § 8a Absatz 3 BSIG muss die Prüfgrundlage festgelegt werden. Da für Krankenhäuser derzeit kein Branchenspezifischer Sicherheitsstandard (B3S) mit Eignungsfeststellung des BSI vorliegt, muss sichergestellt werden, dass die Anforderungen nach § 8a Absatz 1 BSIG auf geeignete Weise im Prüfprozess validiert werden können. Es ist zu erwarten, dass der Prüfer vor der Durchführung der Prüfung gemeinsam mit dem Krankenhaus ein geeignetes und nachvollziehbar dokumentiertes Prüfverfahren für den Geltungsbereich definieren und abstimmen wird.

Das zu definierende Prüfverfahren muss sich hierbei an der „Orientierungshilfe zu branchenspezifischen Sicherheitsstandards (B3S) nach § 8a Absatz 2 BSIG“ orientieren und die Prüfung der darin aufgeführten Aspekte berücksichtigen. Zusätzlich können weitere Quellen hinzugezogen werden, wie zum Beispiel andere B3S gemäß § 8a Absatz 2 BSIG, deren Eignung bereits durch das BSI festgestellt wurde (hierbei ist allerdings der Geltungsbereich zu beachten) oder einschlägige Standards (zum Beispiel Zertifizierungsschemata für ISO 27001 [Nativ oder auf Basis von IT-Grundschutz], ISO/IEC 17021-1, ISO/IEC 27006).

Im Ergebnis liegt eine Prüfgrundlage vor, mit der die Prüfung nach § 8 a BSIG individuell für das Krankenhaus durchgeführt werden kann.

Prüfung des Scopes

Eine der ersten Prüfhandlungen ist die Überprüfung, ob der Scope durch das Krankenhaus korrekt gewählt wurde. Hierzu werden die Vollständigkeit, Eignung, Erforderlichkeit, Wirksamkeit und Angemessenheit sowie die Funktionsfähigkeit der kritischen Dienstleistung überprüft.

Grundlage des Scope sind hierbei die in der BSI-Kritisverordnung aufgeführten kritischen Dienstleistungen, die „stationäre medizinische Versorgung“.

Die Prüfung der Eignung des Scopes im Sinne von § 8a Absatz 3 BSIG ist Teil des Prüfergebnisses und wird durch den Prüfer ausdrücklich bestätigt. ▶

Erstellung des Prüfplans

Jeder Prüfung liegt ein durch den Prüfer erstellter Prüfplan zugrunde. In diesem Prüfplan wird das Prüfteam, die Prüfobjekte, die Prüfziele sowie die beabsichtigte Prüfmethode im Vorfeld der Prüfung festgelegt. Ebenfalls werden die Rollen im Prüfteam und die benötigten Ansprechpartner beim Krankenhaus sowie die zeitlichen Abläufe festgeschrieben.

Eine komplette Prüfung des gesamten Scopes ist in der Regel nicht mit wirtschaftlich vertretbarem Aufwand möglich, daher kann die Prüfung auf Basis einer angemessenen Stichprobenauswahl erfolgen. Diese muss mindestens alle kritischen Prozesse umfassen. Bei der Wahl der Stichproben kann risikoorientiert vorgegangen werden (Berücksichtigung von Wahrscheinlichkeit und Auswirkungen auf die Erbringung der kDL), allerdings ist darauf zu achten, dass in der Gesamtheit der Stichproben eine gute Abdeckung der Kritischen Infrastruktur, aber auch netztopologische Abdeckung erzielt wird.

Durchführung der Prüfung

Nach der Abstimmung der Prüfgrundlage und des Prüfplans wird die Prüfung nach § 8 a BSIG durchgeführt. Im Ergebnis werden die erforderlichen Nachweisdokumente erstellt.

Festlegung der Prüfthemen

Da derzeit kein B3S als Prüfgrundlage für Krankenhäuser existiert, werden die Prüfthemen aus der Orientierungshilfe zur Erstellung eines B3S abgeleitet. Insbesondere die Mapping-Tabelle zu Orientierungshilfe B3S liefert Prüfthemen, die zu berücksichtigen sind, wie zum Beispiel das Continuity Management für kDL, physische Sicherheit, Personelle und organisatorische Sicherheit oder auch Branchenspezifische Technik.

Dokumentenprüfung

Aus den festgelegten Prüfthemen und gegebenenfalls vorhandener Prüfungen resultiert der Umfang der Dokumentenprüfung. Für die Dokumentenprüfung muss das Krankenhaus dem Prüfer etwa folgende Dokumente bereitstellen:

- Konzept und Dokumentation des Risikomanagements inkl. Risikoanalyse
- Beschreibung des Informationssicherheitsmanagementsystems (ISMS)
- Notfallkonzept und Beschreibung des Continuity Managements
- Dokumentation der Prozesse zur baulichen und physischen Sicherheit (zum Beispiel Zutrittskontrolle oder Brandschutzmaßnahmen)
- Dokumentation der personellen und organisatorischen Sicherheit (beispielsweise Aufzeichnungen über Mitarbeiterschulungen, Sensibilisierungskampagnen, Berechtigungsmanagement)
- Konzepte und Dokumentation zur Vorfallerkennung und -bearbeitung (etwa Beschreibung zu Incident Management, Detektion von Angriffen, Forensik)
- Konzepte und Dokumentation von Überprüfungen (wie Prüfberichte der internen Revision sowie anderer durchgeführter Audits, Übungen, systematische Log-Auswertungen und so weiter)
- Sicherheitskonzept (inkl. Darstellung umgesetzter und geplanter Maßnahmen), insbesondere der branchenspezifischen Maßnahmen

Die konkret vorzulegenden Dokumente werden im Rahmen der Prüfung zwischen dem Prüfer und dem Krankenhaus abgestimmt.

Vor-Ort-Prüfung

Im Rahmen der Vor-Ort-Prüfung werden die aus der Dokumentenprüfung gewonnenen Erkenntnisse verifiziert. Insbesondere wird geprüft, ob die dokumentierten Konzepte wie beschrieben umgesetzt sind. Hierbei werden zum Beispiel Sachverhalte in Augenschein genommen, Befragungen durchgeführte, Systeme begutachtet, Aufzeichnungen der Organisation bewertet oder physische Umgebungen begangen.

Der Vor-Ort-Prüfung liegt ein Prüfplan zugrunde, aus dem unter anderem die zu besichtigenden Standorte, die zu befragenden Personen (Rollen) und Zeiträume hervorgehen.

Dokumentation des Prüfergebnisses im Prüfbericht

Als Nachweis gemäß § 8a Absatz 3 BSIG über die Umsetzung der Anforderungen nach § 8a Absatz 1 BSIG wird der Prüfer einen Prüfbericht erstellen. Dieser wird entsprechend der durch das BSI in „Orientierungshilfe zu Nachweisen gemäß § 8a Absatz 3 BSIG“ definierten Vorgaben formuliert und beinhaltet insbesondere festgestellte Sicherheitsmängel und hieraus abgeleitete Empfehlungen.

Abweichung zu den Anforderungen gemäß § 8a Absatz 1 BSIG sind als „Mangel“ definiert und werden durch den Prüfer dokumentiert und bewertet. Grundsätzlich werden alle Feststellungen, die ein Risiko für die kritische Dienstleistung darstellen oder eine korrigierende Maßnahme benötigen, die nicht ohne Zeit oder Ressourcenaufwand umgesetzt werden können, in den Prüfbericht aufgenommen.

Die geplante Nachverfolgung, zu ergreifende Maßnahmen und die Frist zur Beseitigung der Sicherheitsmängel wird festgelegt. Dabei wird eine einheitliche Mängelbewertung basierend auf den vom BSI definierten Mängelkategorien vorgenommen, die auch in der Mängelliste des Nachweisdokuments, das an das BSI gesendet wird, genutzt. Handlungsbedarf besteht für das Krankenhaus bei Mängeln der folgenden Kategorien:

- *Schwerwiegende oder erhebliche Abweichung beziehungsweise Sicherheitsmangel*
  Eine „schwerwiegende Abweichung“ stellt eine gravierende Gefährdung beziehungsweise ein gravierendes Risiko dar. Eine „erhebliche Abweichung“ stellt eine große Gefährdung beziehungsweise ein großes Risiko dar. Die Abweichung muss umgehend (schwerwiegend) be-

ziehungsweise zeitnah (erheblich) beseitigt werden, da Schaden mit Bezug zur kDL zu erwarten ist.

- *Geringfügige Abweichung beziehungsweise Sicherheitsmangel*
  Eine „geringfügige Abweichung“ stellt eine Gefährdung beziehungsweise ein Risiko dar. Die zugrundeliegende Abweichung muss mittelfristig beseitigt werden. Die Vertraulichkeit, Integrität oder Verfügbarkeit der kDL kann beeinträchtigt werden.

Diese Abweichungen beziehungsweise Mängel müssen in den Prüfbericht und das Nachweisdokument aufgenommen werden. Zusätzlich kann eine Empfehlung ausgesprochen oder „keine Abweichung“ attestiert werden.

Aufbauend auf den festgestellten Mängeln muss vom Krankenhaus ein Maßnahmenplan erstellt werden, in dem zu jedem festgestellten Mangel dargestellt ob und wenn welche Maßnahmen geplant sind. Der Maßnahmenplan ist beim BSI beizufügen. Abschließend werden durch den Prüfer die Nachweisdokumente erstellt.

Einreichung der Nachweise beim BSI

Gegenüber dem BSI wird die Erfüllung der Anforderungen aus § 8a Absatz 1 BSIG durch Nachweisdokumente belegt. Damit das BSI die Eignung der Prüfung, die Angemessenheit und Wirksamkeit der Vorkehrungen zur Vermeidung von Störungen sowie die Schwere der aufgedeckten Sicherheitsmängel bewerten kann, sind die erforderlichen „Nachweisdokumente zu § 8a Absatz 3 BSIG“ beim BSI einzureichen. Dies sind insbesondere beizufügen:

- *Blatt KI:* Angaben zur geprüften Kritischen Infrastruktur und zum Ansprechpartner. Das Blatt KI ist vom Krankenhaus auszufüllen und zu unterschreiben. Dem Blatt KI sind als Anlagen die vom Prüfer erstellten Nachweisdokumente beizufügen:

- *Blatt PS:* Angaben zur Eignung der prüfenden Stelle und zum Prüfteam

- *Blatt PD:* Angaben zur Prüfdurchführung

- *Blatt PE:* Angaben zum Prüfergebnis und zu den aufgedeckten Sicherheitsmängeln (inklusive der Anhänge „Liste der Sicherheitsmängel“ und „Umsetzungsplan“)

Zusammenfassung

Zusammenfassend lässt sich feststellen, dass zu erwarten ist, dass der Prüfprozess für Krankenhäuser aufgrund der fehlenden konkreten Prüfgrundlagen individuell mit dem Prüfer abgestimmt werden muss. Zudem ergibt sich das Risiko, dass sich am Markt Prüfende Stellen präsentieren, deren fehlende Eignung erst am Ende des Prüfprozesses durch das BSI festgestellt werden und damit die Prüfung wertlos ist, da die Gefahr besteht, dass dem BSI die eingereichten Nachweise nicht ausreichen und die Prüfergebnisse nicht anerkannt werden. ■

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

Randolf-Heiko Skerka

Prof. Dr. Andreas Becker
Institut Prof. Dr. Becker
Rössrath