Foto: fotohansel – Fotolia

Erfahrungsbericht zum IT-Sicherheitsgesetz

Erstes Klinikum durchläuft Prüfung nach §8a BSIG

Von Randolf-Heiko Skerka, Prof. Dr. Andreas Becker, Ralf Plomann

Die unter die BSI-KritisV fallenden Krankenhäuser sind gemäß § 8a Absatz 3 BSIG verpflichtet, bis zum 29. Juni 2019 den Nachweis zu erbringen, dass ein angemessenes Maß an IT-Sicherheit erreicht ist. Obwohl noch über ein Jahr Zeit bis Ablauf der Frist vorhanden ist, hat das Katholische Klinikum Lünen/Werne entschieden, möglichst frühzeitig den Prüfungsprozess zu durchlaufen. So konnte es am 23.04.2018 die durch die Prüfende Stelle erstellten Nachweise beim Bundesamt für Sicherheit in der Informationstechnik (BSI) einreichen. Damit ist das Katholische Klinikum Lünen/Werne einer der ersten Betreiber Kritischer Infrastrukturen überhaupt, der Nachweise beim BSI eingereicht hat und damit in einen offenen Dialog mit dem BSI eingetreten ist.

Keywords: *IT, Qualitätsmanagement, Recht*

Neben der Einhaltung der gesetzlichen Anforderung war es von Beginn an eines der Ziele des Klinikums Lünen/Werne, einen möglichst großen Nutzen aus der gesetzlich vorgegebenen Prüfung zu ziehen. Der Wille, den Status Quo der IT-Sicherheit bewerten zu lassen und ggf. zu verbessern, war vorhanden. So wurde die Fachexpertise des Prüfungsteams nicht nur dazu genutzt, um – wie es das BSI-Gesetz fordert – festzustellen, ob der Stand der Technik umgesetzt ist und welche Sicherheitsmängel bestehen, sondern auch, um festgestellte Defizite zu priorisieren. So konnte das Klinikum einen Nutzen aus der Prüfung in den folgenden Bereichen ziehen:

1. Identifikation von „Quick Wins“. Im Rahmen des Prüfungsprozesses wurden vom Prüfungsteam diverse Bereiche identifiziert, in denen mit relativ wenig Aufwand das Maß an IT-Sicherheit erhöht werden konnte. Der Kosten-Nutzen-Vergleich sprach dabei deutlich für den erzielten Nutzen. So ließ sich mit überschaubaren Kosten bereits eines der vorrangigen Ziele des BSI-Gesetztes, nämlich die Erhöhung der faktischen IT-Sicherheit – und damit die Erhöhung der Versorgungssicherheit – bei Betreibern Kritischer Infrastrukturen, erreichen. Wichtig war dabei für das Klinikum, dass die bereits vorhandenen Ressourcen des Hauses genutzt wurden und keine Investitionen in neue Technologie erforderlich war. Ein Beispiel eines solchen „Quick Wins“ waren Hinweise für die Agenda der bereits stattfindenden strukturierten Gesprächsrunden zwischen der Geschäftsführung, IT-Leitung und medizinischer Leitung. So wird gewährleistet, dass das Thema „IT-Sicherheit“ zu einem festen Bestandteil in den internen Abstimmungsrunden wurde.

2. Bestätigung des umgesetzten IT-Sicherheitskonzeptes. Wie bei vielen anderen Betreibern Kritischer Infrastrukturen, wurde in der Vergangenheit auch im Klinikum Lünen/Werne keine tiefgehende systematische Analyse des IT-Sicherheitskonzeptes und der fakti-

schen IT-Sicherheit vorgenommen. Das IT-Sicherheitskonzept, welches durch die Verantwortlichen des Klinikums sukzessive entwickelt wurde und historisch gewachsen ist, musste noch nie auf einen kritischen Prüfstand gestellt werden, die IT-Systeme wurden noch nie detailliert unabhängig geprüft. Lediglich im Rahmen der Jahresabschlussprüfungen wurden einzelne Aspekte betrachtet, jedoch mit einem anderen Ziel. Das Prüfungsteam konnte in vielen Bereichen die Überlegungen des Klinikums bestätigen und Hinweise zu Defiziten im IT-Sicherheitskonzept geben. An vielen Stellen bedeutete dies auch, dass die in der Vergangenheit getätigten Investitionen als sinnvoll eingeschätzt wurden.

3. Erhöhung des (IT-)Sicherheitsbewusstseins. Das Bewusstsein für IT-Sicherheit innerhalb der zentralen IT sowie der Geschäftsführung war von Beginn an hoch. Insbesondere die IT-Affinität der Geschäftsführung wirkte sich hierbei vorteilhaft aus. Da im Rahmen der Prüfung die klinischen und unterstützenden Bereiche des Klinikums einbezogen und Interviews mit dem medizinischen Fachpersonal geführt wurden, erhöhte sich in vielen Bereichen das Bewusstsein für die Abhängigkeit von IT sowie möglicher Ersatzprozesse.

Die identifizierten Quick Wins und auch die Bestätigung der in der Vergangenheit getätigten Investitionen in die IT-Sicherheit sind für ein Krankenhaus, aufgrund der generell angespannten Finanzlage im Gesundheitswesen, nicht zu vernachlässigende Aspekte.

Branchenspezifische Defizite

Im Rahmen der Prüfung wurden neben verschiedenen individuellen Defiziten, die das Klinikum beseitigen muss, auch Defizite festgestellt, die sowohl bei vergleichbaren Kliniken, als auch in vergleichbarer Form bei Betreibern Kritischer Infrastrukturen in anderen Sektoren zu erwarten sind. Für Betreiber Kritischer Infrastrukturen liegt die Herausforderung im Umgang mit konkurrierenden Anforderungen. Wie andere Kliniken auch, betreibt auch das Klinikum Lünen/Werne eine Vielzahl von unter die Medizinprodukte-Betreiberverordnung (MPBetreibV) fallende Medizintechnik. Die MPBetreibV konkurriert an verschiedenen Stellen mit den Anforderungen des BSI-Gesetzes, denn „Instandhaltungsmaßnahmen sind unter Berücksichtigung der Angaben des Herstellers durchzuführen“. In der Regel lassen die Hersteller der Medizinprodukte keine Änderung an den Komponenten zu, so dass insbesondere Sicherheitsaktualisierungen nur dann installiert werden können, wenn diese durch den Hersteller freigegeben sind. Zudem werden von vielen Herstellern weiterhin Medizinprodukte angeboten, die auf Betriebssystemen aufsetzen, die vom Betriebssystemhersteller nicht mehr gewartet werden. Auch mit dieser – wie auch in anderen Kliniken zu erwartenden – Situation musste das Klinikum umgehen.

Eine ähnliche Situation ist auch in anderen Sektoren, in denen Branchenlösungen eingesetzt werden, vorzufinden. Im Energiesektor ist ein vergleichbares Problem beispielsweise bei der eingesetzten Leittechnik vorzufinden, bei der maßgeblich durch den Hersteller der Lösung bestimmt wird, welches Maß an IT-Sicherheit erreicht werden kann.

Was hat das Klinikum richtiggemacht?

Aus Sicht des Prüfungsteams gab es verschiedene Faktoren, die – obwohl auch zu beseitigende Defizite festgestellt wurden – zu einem nahezu reibungslosen Prüfungsablauf geführt haben. Hierzu gehörten exemplarisch:

1. Offene Einstellung der Geschäftsführung zur gesetzlichen Vorgabe. Die Geschäftsführung verfolgte keine „Vogel-Strauß-Taktik“, sondern stand der verpflichtenden Prüfung von Beginn an positiv gegenüber und fokussierte sich auf den hieraus zu ziehenden Nutzen.
2. Gute Abstimmung zwischen der IT und Geschäftsführung. Das insgesamt gute Ergebnis lässt sich aus Sicht des Prüfungsteams nicht zuletzt aus der guten Abstimmung zwischen Geschäftsführung und IT-Leitung ableiten. Das Bewusstsein für IT-Sicherheit war daher auch zu Beginn des Prüfungsprozesses vorhanden und musste auf weitere Bereiche der Klinik ausgeweitet werden.
3. Bewusstsein für die Bedeutung von IT-Sicherheit in den klinischen Bereichen. Auch in den klinischen Bereichen war bereits ein Bewusstsein für die Bedeutung der IT-Sicherheit vorhanden. Besonders positiv machte sich jedoch bemerkbar, dass die verantwortlichen Personen durch bekannte Ersatzprozesse ein hohes Maß der Versorgung auch ohne IT sicherstellen können.
4. Sinnvoller Einsatz von IT. Der sinnvolle Umgang mit Ressourcen zeigte sich auch innerhalb der IT. An verschiedenen Stellen wurden IT-Komponenten mit einem sehr guten Kosten-Nutzen-Verhältnis eingesetzt. Exemplarisch ist eine Lösung zur Inventarisierung der umfangreichen Infrastruktur zu erwähnen, mit der automatisiert alle Komponenten identifiziert und neu hinzugekommene erkannt werden können.

Neben diesen positiven Punkten gab es allerdings auch verschiedene negative. Insbesondere der Umstand, dass zu Beginn der Prüfung keine intensive Abstimmung zwischen der zentralen IT, der Haus- und Gebäudetechnik und der Medizintechnik zum Thema IT-Sicherheit bestand, ist ein Punkt, der verbessert werden musste.

Resümee

Die Einreichung der Prüfergebnisse beim BSI hat für das Klinikum Lünen/Werne die Erstellung eines verbindlichen Maßnahmenplans zur Beseitigung der festgestellten Defizite zur Folge. Wann welches Defizit beseitigt werden kann, muss nun ermittelt werden. Insbesondere vor dem Hintergrund der

Phase	Tätigkeit
Schritt 1	Vorbereitung der Prüfung
Schritt 2	Erstellung Prüfplan
Schritt 3	Durchführung der Prüfung
Schritt 3a	Dokumentenprüfung
Schritt 3b	Prüfungen Vor-Ort
Schritt 4	Fertigstellung des Prüfberichtes
Schritt 5	Einreichung der Nachweise beim BSI*

Erstellung des Prüfberichtes

Einreichung der Nachweisunterlagen beim BSI

Abb.: Die einzelnen Phasen der Prüfung

zu erwartenden Kosten der Umsetzung ist dies in einigen Bereichen kein Kinderspiel.

Aus Sicht des Prüfungsteams hat sich gezeigt, dass die Interviews im Klinikum „auf Augenhöhe“ geführt werden müssen. Ein klassischer IT-Prüfer kann keine sinnvollen Gespräche mit einem Chefarzt führen. Hierzu ist ein Fachexperte mit tiefen Kenntnissen sowohl in den klinischen Abläufen als auch in der Medizin erforderlich. Ohne diese Fachexpertise hätten verschiedene Sachverhalte, die aus isolierter IT-Sicht ggf. kritisch sind, nicht beurteilt werden können.

Betreibern, die zukünftig eine Prüfung nach §8a BSIG ausschreiben kann daher geraten werden, auf folgende Aspekte bei der Auswahl eines geeigneten Partners zu achten:

- Eignung der Prüfenden Stelle sicherstellen. Um sicherzustellen, dass die Prüfungen im Sinne des BSI durchgeführt werden, hat das BSI in seinen Orientierungshilfen Anforderungen an „Prüfende Stellen“ definiert. Nur bei Prüfenden Stellen, die diese Anforderungen einhalten, kann sichergestellt werden, dass ausreichende Erfahrung mit vergleichbaren Prüfungen besteht.
- Qualifikation des Prüfungsteams. Neben der durch mindestens ein Mitglied des Prüfungsteams nachzuweisenden „zusätzlichen Prüfverfahrenskompetenz“ muss auch die fachliche Kompetenz im Prüfungsteam vorhanden sein. Neben einer korrekten Beurteilung von Sachverhalten ist nur so sichergestellt, dass Interviews innerhalb der klinischen Bereiche effizient durchgeführt werden.
- Eignung des Fachexperten. Um Gespräche auf Augenhöhe durchzuführen und das klinische Personal zur Teilnahme an der Prüfung und den Interviews zu motivieren, ist es von besonderer Bedeutung, dass ein Mediziner mit der Kenntnis der Abläufe in Krankenhäusern die Prüfung als Fachexperte begleitet.

Zusammenfassend lässt sich feststellen, dass die Prüfung für alle Beteiligte zu neuen Erkenntnissen geführt hat. Das beginnt mit dem Klinikum Lünen/Werne, der Prüfenden Stelle, aber auch dem BSI, von dem hilfreiche Rückmeldungen in verschiedenen Phasen der Prüfung stammten (▶ Abb.). ■

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

Randolf-Heiko Skerka

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

Ralf Plomann
IT-Leiter
Klinikum Lünen/Werne