Foto: kamasigns – Fotolia

Planung und Durchführung einer Prüfung

„Lüner Empfehlung" zur Auswahl einer Prüfenden Stelle für eine Prüfung gem. § 8a (3) BSIG

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

In jeder Prüfung gem. § 8a (3) BSIG sind die Besonderheiten des Betreibers und der Branche, in der der Betreiber tätig ist, von Bedeutung. Im Krankenhausumfeld ist dies u. a. die IT-Durchdringung und IT-Abhängigkeit der klinischen – und unterstützenden – Prozesse. Betreibern, die zukünftig eine Prüfung nach §8a BSIG ausschreiben, wird daher geraten, auf die in der „Lüner Empfehlung" genannten Aspekte bei der Auswahl eines geeigneten Partners zu achten.

Um sicherzustellen, dass die Prüfungen im Sinne des BSI durchgeführt werden, hat das BSI in seinen Orientierungshilfen Anforderungen an „Prüfende Stellen" und die Prüfungsdurchführung definiert. Nur bei Prüfenden Stellen und Prüfungen, die diese Anforderungen einhalten, ist sichergestellt, dass ausreichende Erfahrung mit vergleichbaren Prüfungen besteht.

Das von der Prüfenden Stelle benannte Prüfteam wird Befragungen und Interviews der Ansprechpartner im Krankenhaus durchführen und Sachverhalte – innerhalb der IT und der klinischen Bereiche – in Augenschein nehmen und beurteilen. Daher ist es erforderlich, dass das Prüfteam die in der „Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG" definierten Anforderungen erfüllt und die erforderlichen Kompetenzen vorhanden sind. In Ergänzung zur durch mindestens ein Mitglied des Prüfungsteams nachzuweisenden „zusätzlichen Prüfverfahrenskompetenz" muss auch die fachliche (medizinische) Kompetenz im Prüfungsteam vorhanden sein. Neben einer korrekten Beurteilung von Sachverhalten ist nur auf diese Weise sichergestellt, dass Interviews innerhalb der klinischen Bereiche effizient und auf Augenhöhe mit dem medizinischen Personal durchgeführt werden.

Das Katholische Klinikum Lünen/Werne war eines der ersten Krankenhäuser, welches 2018 der Verpflichtung gemäß § 8a Absatz 3 Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) nachgekommen ist, den Nachweis zu erbringen, dass ein angemessenes Maß an IT-Sicherheit besteht. Damit war das Katholische Klinikum Lünen/Werne einer der ersten Betreiber Kritischer Infrastrukturen überhaupt, der Nachweise beim Bundesamt für Sicherheit in der Informationstechnik (BSI) eingereicht hat. Die im Rahmen der Prüfung gewonnenen Erfahrungen mit der Prüfenden Stelle, dem Prüfteam sowie der Planung und Durchführung der Prüfung mündeten in der nachfolgenden „Lüner Empfehlung". Diese soll anderen Krankenhäusern ermöglichen, von den gemachten Erfahrungen zu profitieren.

Keywords: *Digitalisierung, IT, Risikomanagement*

Die Prüfung zur Erbringung der Nachweise nach §8a (3) BSIG wird Personalressourcen innerhalb des Krankenhauses binden. Um die Beeinflussung der Abläufe des Krankenhauses soweit möglich zu minimieren, ist zusätzlich zur Kenntnis der Abläufe eines Krankenhauses auch eine gute vorbereitende Planung und Durchführung der Prüfung durch das Prüfteam sowie eine gute Kommunikation zwischen den Beteiligten des Krankenhauses und dem Prüfteam von Bedeutung.

„Die Prüfung muss durch das Krankenhaus unterstützt werden. Das Prüfteam benötigt beispielsweise auskunftsfähige Ansprechpartner, Zugriff auf Dokumente etc. Aus diesem Grund ist auch innerhalb des Krankenhauses eine gute Organisation erforderlich, damit der Prüfungsprozess reibungslos verläuft."

Die Prüfung muss durch das Krankenhaus unterstützt werden. Das Prüfteam benötigt beispielsweise auskunftsfähige Ansprechpartner, Zugriff auf Dokumente etc. Aus diesem Grund ist auch innerhalb des Krankenhauses eine gute Organisation erforderlich, damit der Prüfungsprozess reibungslos verläuft. Alle genannten Aspekte lassen sich in der nachfolgenden „Lüner Empfehlung" zusammenfassen.

Lüner Empfehlung

Prüfende Stelle

- Achten Sie bei der Auswahl der prüfenden Stelle darauf, ob sie die fachlichen und organisatorischen Anforderungen des BSI (1) erfüllt.
- Fordern Sie im Rahmen des Auswahlprozesses bzw. einer Ausschreibung geeignete Nachweise an.

Prüfteam

- Das Prüfteam muss die erforderlichen Anforderungen erfüllen und über die erforderliche Kompetenz verfügen (2).
- Fordern Sie im Rahmen des Auswahlprozesses bzw. einer Ausschreibung geeignete Nachweise zu den folgenden Bereichen an: spezielle Prüfverfahrens-Kompetenz für § 8a BSIG, Audit-Kompetenz, IT-Sicherheits-Kompetenz bzw. Informationssicherheits-Kompetenz und Branchen-Kompetenz.
- Gleichen Sie die Nachweise und Auskünfte mit den Anforderungen des BSI ab (3).
- Hat das Prüfteam bereits Prüfungen im KRITIS Bereich „Gesundheit" in Organisationen vergleichbar mit Ihrer Unternehmensgröße durchgeführt?
- Hat das Prüfteam bereits mindestens einen Prüfplan speziell für den Bereich „Gesundheit: Krankenhäuser" erarbeitet?
- Vermittelt das Prüfteam eine fachliche (logische) Empathie für das Geschäftsfeld Krankenhaus und die Menschen, die dort tätig sind?

Planung der Prüfung

Im Rahmen des Auswahlprozesses bzw. einer Ausschreibung sollte die prüfende Stelle zu den folgenden Punkten geeignete Auskünfte geben (4):

- Welche Prüfgrundlage wird vorgeschlagen?
- Wie werden bereits vorhandene aktuelle Prüfungen (nicht älter als ein Jahr!) berücksichtigt?
- Falls eine ISO/IEC 27001-Zertifizierung geplant ist: Wie wird sichergestellt, dass die Schutzziele der kritischen Dienstleistungen und auch die branchenspezifischen Besonderheiten angemessen berücksichtigt werden [siehe hierzu auch (5)]?
- Sind die Prüfthemen konkret beschrieben?
- Wurde der Scope unter Berücksichtigung der Vollständigkeit, der Eignung, Erforderlichkeit, Wirksamkeit und Angemessenheit der Funktionsfähigkeit der kritischen Dienstleistung gewählt?
- Werden die möglichen Prüfmethoden unter Berücksichtigung der kritischen Dienstleistung angemessen beschrieben?
- Ist der ermittelte Prüfaufwand realistisch und berücksichtigt er die Größe der Organisation, die Kritikalität gemäß BSI-KritisV, die Komplexität des zu prüfenden Scopes, die IT-Abhängigkeit bzw. die IT-Durchdringung der kritischen Dienstleistung und die Frage, ob ein Penetrationstest durchgeführt werden muss?
- Gibt der Prüfplan Auskunft zum Prüfteam, den Prüfobjekten, den Prüfzielen, den Prüfmethoden, den benötigten Ansprechpartnern und den zeitlichen Abläufen?
- Falls eine Stichprobenauswahl zur Prüfung des Scopes getroffen wurde: Umfasst diese auch wirklich alle kritischen Prozesse und wurde sie risikoorientiert gewählt?
- Der Prüfbericht soll alle für die Bewertung relevanten Informationen enthalten und alle Prüfschritte nachvollziehbar und wiederholbar dokumentieren sowie die Prüfentscheidungen begründet darlegen.
- Gibt es in der Prüfungsmethodik eine sinnhafte Verteilung zwischen Dokumentenaudit und Praxisanteilen vor Ort im Unter-

„Fordern Sie im Rahmen des Auswahlprozesses bzw. einer Ausschreibung geeignete Nachweise zu den folgenden Bereichen an: spezielle Prüfverfahrens-Kompetenz für § 8a BSIG, Audit-Kompetenz, IT-Sicherheits-Kompetenz bzw. Informationssicherheits-Kompetenz und Branchen-Kompetenz."

nehmen? Insbesondere: Gibt es einen ausreichenden Kontakt zu den verschiedenen Berufsgruppen im Krankenhaus? Ein „Theorie“-Audit sollte vermieden werden!

- Betrachtet das Prüfteam das Krankenhaus als ganzes Organisationskonstrukt oder nur solitär Technologie und deren Anwendung? Da Technologie bereichsübergreifend zur Anwendung kommt, kann eine rein technische und segmentierte Sicht das Ergebnis der Prüfung nachteilig relativieren.
- Hat der Auftraggeber (in diesem Fall das Krankenhaus) selbst die zeitlichen und personellen Ressourcen verfügbar, um den Prüfungsprozess jederzeit auch bei evtl. steigendem Prüfungsumfang im vollen Umfang zu unterstützen?
- Gibt es beim Auftraggeber (Krankenhaus) eine klare Verantwortung in der internen Prüfungsbegleitung (SPOC- Single Point of Contact) und ist diese Person ausreichend motiviert und qualifiziert, den Prozess zu begleiten?
- Wurden vor der Prüfung alle Bereiche und Abteilungen des Auftraggebers (Krankenhaus) über das Vorhaben und die Wichtigkeit der Kooperation informiert und zur Mitarbeit verpflichtet? (Pflege, Medizin, Technik, Verwaltung etc.)
- Wurden die durch das Prüfungsverfahren entstehenden Kosten (und möglichen Folgekosten) in ausreichendem Umfang mit den Finanzverantwortlichen besprochen?
- Ist festgelegt, in welcher Form, welcher Art und in welchem Umfang ein Prüfbericht durch das Prüfteam zu erstellen ist? Und entspricht dieser Bericht formal den Erwartungen des BSI?
- Ist mit dem Prüfteam ausreichend geklärt, wie bei verschiedenen Auffassungen zu eventuellen Feststellungen der Prüfung zwischen Auftraggeber und Prüfern ein Konsens im Bericht erzielt werden kann?

Eine Berücksichtigung dieser Punkte und der Vorgehensweise ist hilfreich, um die Prüfung bestmöglich vorzubereiten.

Quellen

1. Orientierungshilfe zu Nachweisen gemäß § 8a (3) BSIG. Bundesamt für Sicherheit in der Informationstechnik. Version 0.9.02 vom 30.06.2017. Hier: Abschnitt 3, Prüfende Stelle.
2. Hier: Abschnitt 4, Das Prüfteam.
3 Hier: Insbesondere Abschnitt 4.3, Nachweis der Eignung
4 Hier: Abschnitt 5, Durchführung der Prüfung. ■

Literatur beim Verfasser

Ralf Plomann
IT-Leiter
Klinikum Lünen/Werne

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

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