Foto: wladimir1804 – Fotolia

Eine Herausforderung zur Compliance!

Durch systematische Umsetzung Haftungsrisiken senken

Von Prof. Dr. Andreas Becker und Randolf Skerka

Unter Compliance ist die Einhaltung von gesetzlichen Bestimmungen und unternehmensinternen Richtlinien zu verstehen. Interne Richtlinien des Unternehmens können auch von Dritten entwickelte Prinzipien oder Konventionen sein, zu deren Einhaltung sich das Unternehmen selbst verpflichtet hat. Wirkt ein Unternehmen durch angemessene und miteinander verbundene Maßnahmen systematisch und effektiv auf Compliance hin, so spricht man von einem Compliance-Management-System (CMS).

Gemeinsam mit dem Risikomanagementsystem, dem internen Kontrollsystem und der internen Revision bildet das CMS die vier Elemente des „House of Governance". Die sogenannte Corporate oder Good Governance beschreibt die Steuerung und Überwachung von Geschäftsbetrieben mit dem übergeordneten Ziel einer verantwortungsvollen Unternehmensführung.

Die angemessene Beschäftigung mit Compliance oder gar die Einführung und Aufrechterhaltung eines CMS bringt zahlreiche Vorteile mit sich, so zum Beispiel:

- Schafft Vertrauen von Stakeholdern, wie Eigentümern, Vertragspartnern und der Gesellschaft, in die Organisation.
- Motiviert die Organisationsmitglieder durch klare, unmissverständliche Vorgaben.
- Sichert nachhaltig den Wert der Organisation.
- Schützt die Reputation der Organisation.
- Erleichtert oder ermöglicht die Teilnahme an Ausschreibungen und Arbeitsgemeinschaften sowie den Zugang zu Finanzierungen.
- Kann das Risiko der Haftung und Bestrafung der Organisation beziehungsweise ihrer Organe und Mitarbeiter reduzieren.

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 Prof. Dr. Andreas Becker, Berater für Einrichtungen im Gesundheitswesen und Randolf-Heiko Skerka, Experte für Informationssicherheits-Managementsysteme.

Keywords: *IT-Sicherheit, Geltungsbereich, Strukturanalyse, BSIG*

Bei der Umsetzung eines CMS bietet es sich an, sich an nationalen und internationalen Standards be- ▶

ziehungsweise Normen zu orientieren, so zum Beispiel am Prüfungsstandard des Instituts der Wirtschaftsprüfer IDW PS 980 oder an der DIN ISO 19600.

Eine explizite Rechtspflicht zur Errichtung eines CMS existiert für Krankenhäuser, unabhängig von ihrer Trägerschaft, nicht. Für die Geschäftsleitung beziehungsweise den Aufsichtsrat eines Krankenhauses bestehen jedoch rechtliche Pflichten, Compliance durch geeignete Maßnahmen sicherzustellen. Es zählt zu den allgemeinen Sorgfaltspflichten des Vorstandes beziehungsweise der Geschäftsführung, Maßnahmen im Unternehmen zu etablieren, damit die Einhaltung gesetzlicher Bestimmungen und unternehmensinterner Richtlinien sichergestellt werden kann. Den Aufsichtsgremien obliegt die Überwachungspflicht, dass die Geschäftsführung ihren Pflichten nachkommt.

Dieser Sicherstellungsauftrag gehört zu den Überwachungssorgfalten der Leitungsorgane, da davon auszugehen ist, dass rechtswidrige Handlungen durch unzureichende Organisation und nicht institutionalisierte Kontrollen erst möglich werden. Bei Aktiengesellschaften ergibt sich die grundsätzliche Verpflichtung der Organmitglieder, die Rechtmäßigkeit des Handelns im Unternehmen sicherzustellen, aus den Vorschriften des Aktiengesetzes und des Deutschen Corporate Governance Kodex, bei der GmbH folgt dies aus § 43 GmbHG. Die sich hieraus auch ergebende Überwachungspflicht wird auch durch § 130 Absatz 1 OWiG gestützt.

Treten in einem Unternehmen Compliance-Verstöße auf, kann dies zu einer ordnungsrechtlichen Außenhaftung führen (§§ 130, 30 OWiG). Daran anknüpfend kann gegen die für die Gesellschaft handelnde Person ein Bußgeld im Rahmen einer Durchgriffshaftung verhängt werden.

Compliance im Krankenhaus

Der Begriff der Compliance hat im Krankenhausbereich seit dem Inkrafttreten des Gesetzes zur Bekämpfung von Korruption im Gesundheitswesen im Juni 2016 besondere Aufmerksamkeit erfahren. Dies gilt insbesondere für intersektorale Kooperationen, die nun unter den Ergänzungen des Strafgesetzbuches (§§ 299a und b sowie 300 StGB) mit ihren durchaus erheblichen Strafandrohungen zu sehen sind. Darüber hinaus bestehen für Krankenhäuser weitere Compliance-Risiken, die verschiedene Rechtsgebiete tangieren, beispielhaft seien hier genannt: Behandlungsprozess (Behandlungsfehler, Organisationsmängel), Abrechnung, Infektionsschutz und Krankenhaushygiene, Arbeits- und Sozialversicherungsrecht.

Ganz besonders soll hier auch auf die Anforderungen an ein einrichtungsinternes Qualitätsmanagement gemäß der Richtlinie des G-BA hingewiesen werden, die auch wegen der möglichen Folgen der Nichtbeachtung aus der Compliance-Perspektive betrachtet werden muss.

Die QM-Richtlinie definiert eine Leitungsaufgabe, die nicht nur in der Einrichtung, sondern auch in der Fortentwicklung, fortdauernden Überprüfung (Zielkontrolle) und Verbesserung der Richtlinienanwendung besteht. Es handelt sich daher um eine dauerhafte Anforderung, deren Nichtbeachtung oder nicht hinreichende Beachtung sowohl im Bereich der Implementierung, der laufenden Überprüfung wie auch der Evaluation haftungsrechtliche Konsequenzen haben kann.

Die zivilrechtliche Haftung für Organisationsmängel führt im Außenverhältnis – das heißt im Verhältnis zur Patientenseite – primär zu einer Haftung des Trägers (respektive der hinter ihm stehenden Haftpflichtversicherung). Im Innenverhältnis (Krankenhausträger zur Geschäftsleitung) ist die Missachtung erforderlicher innerbetrieblicher Organisationsstrukturen ein Mangel der Geschäftsleitung mit den Folgen der Regresspflicht gemäß § 93 Absatz 2 AktG, § 43 Absatz 2 GmbHG. Dieses Risiko erschließt sich beispielhaft und recht beeindruckend aus der Richtlinien-Vorgabe zur Nutzung von Checklisten bei operativen Eingriffen, die unter Beteiligung von zwei oder mehr Ärzten beziehungsweise die unter Sedierung erfolgen. Wird die Checkliste in einem Krankenhaus nachweislich nicht gemäß der Vorgabe angewendet und ist dies den Leitungsorganen nicht bekannt oder führt nicht zu angemessenen Maßnahmen, so wird ein zumindest haftungsrechtlich erhebliches Fehlverhalten ignoriert und der Organisationsmangel aufrechterhalten.

Wenn entsprechendes Handeln in der vertikalen personellen Organisationsstruktur bekannt ist und – zumindest – geduldet wird, oder durch diese sogar bedingt ist, ist eine auch strafrechtliche Verantwortung in dieser vertikalen Organisationsstruktur in Form von Beihilfe oder Tatbeteiligung durch mittelbare Täterschaft nicht grundsätzlich zu verneinen. Allerdings stellen sich hinsichtlich der Kausalität und auch des subjektiven Tatbestands erhebliche strafrechtsdogmatische Fragen, deren Darstellung vorliegend zu weit geht. Insgesamt ist jedoch festzustellen, dass strafrechtliche Verantwortung aufgrund grober Mängel der Organisationsstruktur nicht auszuschließen ist.

Compliance und IT-Sicherheit

Das IT-Sicherheitsgesetz (IT-SIG) gibt als Artikelgesetz durch die entsprechenden Änderungen des BSI-Gesetzes eine Sicherheitskonzeption vor, die auf drei Säulen basiert:

- Sicherstellung eines Mindestniveaus an IT-Sicherheit durch angemessene organisatorische und technische Vorkehrungen unter Einhaltung des Stands der Technik (§ 8a Absatz 1 BSI-Gesetz).
- Nachweis des angemessenen Mindestniveaus an IT-Sicherheit durch Sicherheitsaudits, Prüfungen oder Zertifizierungen (§ 8a Absatz 3 BSIG).
- Meldepflicht von IT-Sicherheitsvorfällen an das BSI, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastrukturen geführt haben oder führen können (§ 8b Absatz 4 BSIG).

Datenschutz und Datensicherheit werden häufig synonym verwendet, obwohl es – juristisch gesehen – erhebliche Unterschiede gibt. Datenschutz hat den Schutz personenbezogener Daten im Sinne des Bundesdatenschutzgesetzes zum Ziel: Daten von und über Menschen. Datensicherheit hingegen umfasst alle denkbaren Arten von Daten, also auch Bilanzdaten, Forschungsergebnisse, Behandlungs- und Organisationsdaten et cetera.

Ziel der Datensicherheit ist es, Krankenhausdaten vor unbefugtem internen und externen Zugriff und die IT-Infrastruktur vor Schäden zu bewahren. Datendiebstahl, Manipulationen, Löschung, unberechtigte Einsichtnahmen und sonstige Schädigungen sollen vermieden werden. Dabei gelten die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit (§ 8a Absatz 1 BSIG) als Grundprinzipien der Datensicherheit.

Zur Erfüllung der sich aus dem IT-SIG beziehungsweise dem BSIG ergebenden Anforderungen bedarf es der Einführung einer geeigneten IT-Organisationsstruktur, die die stationäre medizinische Versorgung absichert und dabei die vielfältigen organisatorischen und thematischen Verknüpfungen berücksichtigt. Hierzu gehören die Medizin- und Gebäudetechnik sowie das CMS und das Risikomanagement. Die Leitungsorgane müssen also erkennen, dass es sich nicht um ein reines IT-Thema handelt.

Um eine eindeutige und transparente Organisation der Verantwortlichkeiten und Kompetenzen zu erreichen, sollte die Geschäftsführung eine eindeutige Leitlinie herausgeben, die die Eckpunkte der Informationssicherheit festlegt. Auf Basis dieser Leitlinie werden Verantwortlichkeiten und Kompetenzbereiche der Abteilungen untereinander abgegrenzt und andererseits das erforderliche Miteinander in Fragen der Informationssicherheit geregelt.

Handlungsempfehlungen für Leitungsorgane

Leitungsorgane von Krankenhäusern, die gemäß der BSI-Kritisverordnung (BSI-KritisV) eine kritische Infrastruktur betreiben, sollten nun schnellstmöglich prüfen, ob die von ihnen geplanten oder bereits ergriffenen Maßnahmen ausreichen, um die Anforderungen aus dem BSIG zu erfüllen.

Dabei sollten auf jeden Fall auch die Beauftragten für den Datenschutz und die Compliance beziehungsweise das CMS einbezogen werden. Der Compliance-Beauftragte sollte hierbei – insbesondere bei der Erstumsetzung des BSI-Gesetzes – auf der Erstellung eines Umsetzungsplanes drängen, der bestimmte Zeitpunkte als kritische Messpunkte definiert. Dazu gehören auf jeden Fall die Fristen für die Benennung der Kontaktstelle nach § 8b Absatz 3 BSIG (sechs Monate nach dem Inkrafttreten der BSI-KritisV am 30.06.2017) und die Erbringung des Nachweises der Erfüllung der Anforderungen bezüglich der angemessenen organisatorischen und technischen Vorkehrungen gemäß § 8a Absatz 3 BSIG (zwei Jahre nach Inkrafttreten der BSI-KritisV).

Auch sollte gewährleistet werden, dass die umgesetzten Maßnahmen regelmäßig im Rahmen des internen Auditprogrammes überprüft werden. Audits und Stichprobenkontrollen sind auch deshalb notwendig, weil sie zu den erforderlichen Aufsichtsmaßnahmen im Sinne des § 130 OWiG gehören und so einen Beitrag zum Schutz der Organisationsverantwortlichen leisten können. Ob diese Kontrollmaßnahmen durch das Qualitätsmanagement, die IT-Abteilung oder den Compliance-Beauftragten (gegebenenfalls auch kombiniert) durchgeführt werden, hängt von den individuellen organisationalen Voraussetzungen des Krankenhauses ab.

Schadenspotenzial

Ein primäres, sich direkt aus dem BSI-Gesetz ergebendes Schadenspotenzial ergibt sich aus der Nichteinhaltung der hier darin enthaltenen Vorgaben. Das BSIG sieht in § 14 für das folgende ordnungswidrige Verhalten Bußgelder vor:

- Die in § 8a Absatz 1 BSIG geforderten Maßnahmen zur Sicher-

stellung eines Mindestniveaus an IT-Sicherheit durch angemessene organisatorische und technische Vorkehrungen unter Einhaltung des Stands der Technik werden vorsätzlich oder fahrlässig nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig getroffen. Das Bußgeld kann hier bis zu 50.000 Euro betragen.

- Die vorsätzliche oder fahrlässige Zuwiderhandlung gegen eine Auflage, die das BSI im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde zur Beseitigung eines Sicherheitsmangels verfügt hat (§ 8a Absatz 3 Satz 5 BSIG), ist mit einem Bußgeld von bis zu 100.000 Euro bedroht.

- Wird die in § 8b Absatz 3 BSIG geforderte Kontaktstelle nicht vorsätzlich oder fahrlässig nicht oder nicht rechtzeitig benannt, so kann ein Bußgeld bis zu 50.000 Euro festgelegt werden.

- Wird eine Meldung über eine erhebliche Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können (§ 8b Absatz 4 Satz 1 Nummer 2 BSIG) vorsätzlich oder fahrlässig nicht unverzüglich über die Kontaktstelle an das BSI gemeldet, so droht ein Bußgeld bis 50.000 Euro.

Die Verwaltungsbehörde ist im Sinne des § 36 Absatz 1 Nummer 1 OWiG das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Als sekundäres Schadenspotenzial, das sich aus der mangelhaften Sicherstellung eines Mindestniveaus an IT-Sicherheit durch angemessene organisatorische und technische Vorkehrungen unter Einhaltung des Stands der Technik ergeben kann, können die folgenden Punkte aufgeführt werden:

Wird ein Bußgeld nach § 14 BSI-Gesetz verhängt, so besteht aus Sicht des Krankenausgeschäftsführers die Gefahr, dass die Frage seiner möglichen Haftung gegenüber dem Krankenhausträger zumindest geprüft wird.

Kommt es zu einer Kompromittierung des Datenschutzes im Sinne des Bundesdatenschutzgesetzes, so drohen Bußgelder bis zu 300.000 Euro (§ 43 Bundesdatenschutzgesetz).

Die Folgen von Sicherheitszwischenfällen können gravierend sein, so berichtete beispielsweise das Lukaskrankenhaus in Neuss von Gesamtkosten in Höhe von 1.742.000 Euro, die eine Cyberattacke mit den resultierenden Erlösausfällen und Beratungskosten für IT-Sicherheitsexperten verursachte.

Ein Reputationsschaden kann für ein Krankenhaus nicht nur durch ein spektakuläres und medienwirksames Ereignis wie eine Cyberattacke entstehen. Ebenso muss sich der daraus unter Umständen resultierende Rückgang von Patientenzahlen und damit auch Erlösen nicht zwangsläufig auf die akute Phase einer Krise beschränken.

Kommt es in Folge erheblicher Störungen oder gar Ausfällen der stationären medizinischen Versorgung, die durch eine Unterschreitung des im BSI-Gesetz geforderten Mindestniveaus an IT-Sicherheit bedingt sind, zu Patientenschäden, so ergeben sich hieraus vielfältige Risiken für den Krankenhausträger, seine Organe und auch verantwortliche Mitarbeiter. Diese Risiken können sich im schlimmsten Fall auch im Bereich des Zivil- und sogar Strafrechts bewegen.

In allen Fällen besteht natürlich auch ein erhebliches Risiko hinsichtlich der negativen Auswirkungen auf die Kosten für die Haftpflicht- beziehungsweise IT-/Cyber-Versicherung eines Krankenhauses.

Fazit

Die gemäß IT-SIG beziehungsweise BSIG einzuhaltenden gesetzlichen Bestimmungen erfordern, dass ein auf den ersten Blick „typisches IT-Thema“ auch und insbesondere unter dem Blickwinkel der Compliance zu betrachten ist.

Werden bestimmte Forderungen nicht rechtzeitig oder nicht vollständig erfüllt, so drohen daraus – erstmals ab dem 30.12.2017 – Bußgelder von bis zu 100.000 Euro.

Resultieren daraus auch Reputationsschäden, Erlösausfälle oder gar Patientenschäden, so bewegen sich die möglichen haftungsrechtlichen Folgen möglicherweise auch im Zivil- und Strafrecht.

In jedem Fall stellt sich die Frage der Verantwortlichkeit einzelner Personen und auch des Organisationsverschuldens.

Krankenhausgeschäftsführer und deren Beauftragte sind unter präventiven Gesichtspunkten gut beraten, wenn sie nun schnellstmöglich prüfen, ob die von ihnen geplanten oder bereits ergriffenen Maßnahmen ausreichen, um die Anforderungen aus dem BSIG zu erfüllen. ■

Literatur beim Verfasser

Prof. Dr. Andreas Becker
Qualifikation
„Spezielle Prüfverfahrens-Kompetenz
für § 8a BSIG“
Institut Prof. Dr. Becker

Prof. Dr. Andreas Becker

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