Foto: Alfa27 – Fotolia

Aufsicht und Kontrolle

Interview mit Axel Weinand

Das IT-Sicherheitsgesetz hat primär Auswirkung auf die IT-Infrastruktur. Die Haftungsfrage ist in diesem Bezug etwas ins Hintertreffen geraten. Doch auch im Managementbereich hat das Gesetz im Hinblick auf die Haftung im Organisationsablauf und der Compliance Auswirkungen.

Keywords: *IT-Sicherheit, Compliance, Haftung, Organisationsverschulden*

Axel Weinand
Geschäftsführer
St.-Marien-Hospital Lünen

Herr Weinand, was bedeuten das BSI-Gesetz und die BSI-Kritisverordnung aus Ihrer Sicht als Geschäftsführer?

Zunächst finde ich es positiv, dass der Gesetzgeber die zunehmenden Risiken durch Cyber-Attacken erkannt hat und darauf reagiert. In der praktischen Umsetzung sehe ich als Krankenhaus-Geschäftsführer das Problem, die zusätzlichen Anforderungen mit den vorhandenen Mitarbeitern und begrenzten Investitionsmitteln zu erfüllen. Lamentieren hilft jedoch nicht, wir haben uns auf den Weg gemacht. Mit den uns zur Verfügung stehenden Ressourcen werden wir die gesetzlichen Anforderungen erfüllen und reduzieren gleichzeitig das Risiko, Opfer einer Cyber-Attacke zu werden.

Wie ordnen Sie die neuen Herausforderungen unter den Begriffen Compliance und Risikomanagement ein?

IT-Sicherheit ist nun gesetzlich geregelt. Unter Compliance versteht man unter anderem die Einhaltung gesetzlicher Bestimmungen. Aus diesem Grund ist IT-Sicherheit ein neuer Bestandteil unseres Compliance-Management-Systems geworden

Welche Maßnahmen sollten ergriffen werden, um das Risiko eines Organisationsverschuldens auf ein akzeptables Niveau zu bringen und dort zu halten?

Das Thema IT-Sicherheit war in unserem Klinikum schon vor den bekannt gewordenen Cyber-Angriffen auf deutsche Krankenhäuser ein wichtiges Thema. Aus diesem Grund gibt es in unserem Klinikum gute technische und organisatorische Lösungen, um Viren- oder Trojaner-Angriffe zu verhindern. Wir sind uns dabei im Klaren, dass wir einem gezielten, professionellen Angriff nicht Stand halten können. Wir sind jedoch sehr gut auf IT-Ausfälle vorbereitet. In vielen Funktionsbereichen unseres Klinikums wissen die Mitarbeiter, was zu tun ist, wenn die IT-Systeme nicht zur Verfügung stehen.

Auch in unserer Leitungskonferenz, an der sämtliche Führungskräfte unseres Klinikums teilnehmen, war IT-Sicherheit bereits Thema und wird es auch zukünftig regelmäßig sein. Die Führungskräfte sind aktuell aufgefordert, mit ihren Teams die bestehenden Ausfallkonzepte zu prüfen und bei Erfordernis zu aktualisieren.

Regelmäßig führen wir gemeinsam mit der Feuerwehr Brandschutzübungen durch und Proben den Ernstfall mit Evakuierungsübun- ▶

gen. Zukünftig werden wir auch den Totalausfall unserer IT-Systeme trainieren. Eine Herausforderung wird sein, dies im laufenden Betrieb zu simulieren.

Des Weiteren haben wir einem Mitarbeiter aus der IT-Abteilung das Thema IT-Sicherheit schwerpunktmäßig übertragen. Weil IT-Sicherheit nicht mal so eben nebenbei bearbeitet werden kann, mussten wir die Personalressourcen innerhalb der IT-Abteilung reorganisieren, um damit auch das Themenfeld IT-Sicherheitsmanagement dauerhaft zu besetzen. Im Rahmen einer Revision erfassen wir derzeit auch alle technischen und medizintechnischen Anlagen, die einen IP-Anschluss benötigen und prüfen diese Anlagen unter dem Aspekt der IT-Sicherheit. Dies gehörte in der Vergangenheit aus Sicht der IT nicht zum originären Aufgabengebiet einer IT-Abteilung.

Es finden regelmäßige IT-Sicherheitsmeetings zwischen dem IT-Sicherheitsmanager und dem IT-Leiter statt, die protokolliert werden. Wir reglementieren Fernwartungszugänge und unterbinden, dass im Rahmen von Wartungsarbeiten Softwareupdates eingespielt werden, die nicht durch unsere IT-Abteilung geprüft wurden.

Unsere Mitarbeiter werden regelmäßig zum Thema IT-Sicherheit informiert und sensibilisiert. Zum Beispiel werden IT-Sicherheitshinweise im Intranet veröffentlicht und für die nächste Mitarbeiterversammlung ist ein separater Tagesordnung zum Thema IT-Sicherheit vorgesehen.

Ist die IT-Sicherheit nur ein Thema für die Geschäftsführung oder auch für ihr Aufsichtsgremium?

Die IT-Sicherheit muss ein Thema für das Aufsichtsgremium sein. Dies leitet sich unmittelbar aus den Aufgaben der Aufsichtsräte, der laufenden Aufsicht und Beratung der Geschäftsführung ab. Im Rahmen des Risikofrüherkennungssystems mit einem inhaltlichen Überblick über die Chancen- und Risikoentwicklung gehört das Thema IT-Sicherheit spätestens seit den Cyber-Angriffen auf deutsche Krankenhäuser auf die Agenda. Diese Angriffe haben gezeigt, dass damit erhebliche Einschränkungen in den medizinischen Abläufen und damit in der akuten Patientenversorgung verbunden waren. Der wirtschaftliche Schaden war erheblich. Mindestens einmal im Jahr oder anlassbezogen sollte dem Aufsichtsgremium über den aktuellen Stand der IT-Sicherheit berichtet werden.

Wie gehen Sie in Ihren Kliniken nun konkret vor, um die Anforderungen aus Gesetz und Verordnung umzusetzen? Schließlich müssen Sie bis Juni 2019 gegenüber dem BSI einen geeigneten Nachweis zur Erfüllung der Anforderungen erbringen.

Nach Bekanntwerden der gesetzlichen Anforderungen haben wir uns um externe Kompetenz bemüht, die bereits Erfahrung aus anderen kritischen Dienstleistungsbereichen gesammelt hat. Diese Kompetenz haben wir in einem Unternehmen aus dem Bereich IT-Security-Consulting gefunden, das bereits langjährige und umfangreiche Erfahrungen im Bereich der IT-Sicherheit insbesondere bei Banken vorweisen kann, aber auch über die aus meiner Sicht unbedingt erforderlichen Kenntnisse zu den Versorgungsprozessen und den Besonderheiten des Krankenhausbetriebs verfügt.

Erklärtes Ziel ist, mit der externen Beratung möglichst zeitnah unsere Stärken und Schwächen im Bereich der IT-Sicherheit zu identifizieren und die Schwachstellen zu beseitigen. Hierbei ist uns völlig klar, dass das Projekt IT-Sicherheit auch in unserem Klinikum ein laufender Prozess sein wird, der in unseren täglichen Abläufen zur Selbstverständlichkeit werden muss. Auf jeden Fall werden wir noch in diesem Jahr ein Audit gemäß den Vorgaben der BSI-Kritisverordnung durchführen.

Was werden dabei die größten Herausforderungen sein?

Die größte Herausforderung ist, unsere Mitarbeiter in der täglichen Routine bei hoher Arbeitsbelastung für das Thema IT-Sicherheit zu sensibilisieren. Das fängt bei vermeintlich banalen Dingen an, wie etwa der Umgang mit Passwörtern, und hört bei der Simulation unserer medizinischen Prozesse bei einem IT-Totalausfall auf.

IT-Sicherheit gibt es nicht zum Nulltarif und wird auch nicht zusätzlich über das Krankenhausbudget finanziert. Daher werden wir unsere Personalressourcen anpassen und Investitionsentscheidungen zu Gunsten der IT-Sicherheit priorisieren.

Wie wird sich zukünftig die Zusammenarbeit mit der IT-Leitung gestalten? Wie werden Sie über die weitere technische Entwicklung auf dem Laufenden gehalten?

Die Zusammenarbeit mit der IT-Leitung war schon immer sehr eng, was sicherlich auch an meiner persönlichen Affinität zur IT liegt. Mit unserem IT-Leiter habe ich schon seit längerer Zeit einen monatlichen Jour-Fix organisiert, in deren Rahmen ich über Entwicklungen aus dem Bereich IT informiert werde. Hier geht es aber nicht nur um technische Entwicklungen, sondern sehr häufig auch um die Menschen in unserem Klinikum, die die IT-Technik anwenden. Beispielsweise informiert mich der IT-Leiter, in welchen Bereichen Schulungsbedarf besteht und wie in unserem Klinikum IT-Sicherheit gelebt wird.

Welche Rolle kann bei der IT-Sicherheit ein sogenannter Risikotransfer durch eine entsprechende Versicherung spielen?

Zunächst muss ich feststellen, dass finanzielle Schäden aufgrund von Cyber-Attacken durch bestehende Versicherungsverträge nicht abgedeckt sind. Hier eröffnet sich ein neuer, lukrativer Markt für die Versicherungsbranche im Bereich der Absicherung von Cyber-Risiken zu Lasten der Krankenhäuser. Oftmals werden über diese Versicherungen auch nur Schäden abgesichert, bei denen ein gezielter Angriff auf das Krankenhaus erfolgt ist. Schäden durch einen Massenangriff, wie zum Beispiel beim Krypto-Trojaner Locky, sind zum Teil nicht abgedeckt.

Es ist auch sehr genau zu prüfen, unter welchen Voraussetzungen der

Versicherer im Schadensfall eintritt. Viele Policen setzen eine IT-Infrastruktur voraus, die dem „Stand der Technik“ entspricht. Diese Formulierung ist ein unbestimmter Rechtsbegriff. Meines Erachtens müssten Versicherungspolicen präzisiert werden oder der Versicherer muss sich im Rahmen eines Kurz-Checks selbst vom Stand der Technik überzeugen.

Positiv ist, dass es in der Krankenhausbranche mittlerweile Makler beziehungsweise Versicherungen gibt, die nicht nur ein reines Versicherungsprodukt verkaufen, sondern einen echten Mehrwert, wie zum Beispiel IT-Sicherheitsprüfungen und Notfallübungen, anbieten, um Schäden zu vermeiden oder zu minimieren. Somit können Krankenhäuser von dem gebündelten Know-how eines Versicherers profitieren.

Viele Krankenhäuser fragen sich, wie die Forderung zur Einrichtung einer Kontaktstelle umgesetzt werden soll. Haben Sie hierzu schon einen Plan?

Wir als Betreiber einer kritischen Infrastruktur im Sinne von § 2 Absatz 10 BSIG haben nach § 8b Absatz 3 BSIG innerhalb von sechs Monaten nach Inkrafttreten der BSI-Kritisverordnung dem BSI eine Kontaktstelle zu benennen, über die wir jederzeit erreichbar sind. Diese Kontaktstelle ist ein Funktionspostfach, an das das BSI IT-Sicherheitsinformationen schickt. Problem ist die jederzeitige Erreichbarkeit eines sachkundigen, entscheidungsbefugten Mitarbeiters an 24 Stunden, sieben Tage die Woche zu gewährleisten.

Wir werden nach heutiger Überlegung bei Eingang einer E-Mail automatisch diese Nachricht an den IT-Rufdienst, den IT-Leiter und den Geschäftsführer weiterleiten. Außerhalb der betriebsüblichen Zeiten, insbesondere Nachts, am Wochenende und an Feiertagen wird darüber hinaus bei Eingang einer Sicherheitswarnung durch das BSI ein automatischer Telefonanruf mit dem Hinweis, dass eine IT-Sicherheitswarnung eingegangen ist, an den genannten Personenkreis abgesetzt.

IT-Sicherheit ist ja ein Thema für alle Mitarbeiter. Wie werden Sie die erforderliche Durchdringung des Themas in die Gesamtorganisation fördern?

IT-Sicherheit ist Führungsaufgabe! Wir haben das Thema bereits in unserer regelmäßig stattfindenden Führungskräftekonferenz aufgegriffen. Sämtliche Führungskräfte aus allen Bereichen unseres Klinikums wurden über das IT-Sicherheitsgesetz informiert und dass in diesem Jahr ein IT-Sicherheits-Audit durchgeführt wird. Die Führungskräfte wurden aufgefordert, in ihren Bereichen IT-sicherheitsrelevante Prozesse zu identifizieren und gemeinsam mit den Teams einen Ausfall der IT-Systeme gedanklich durchzuspielen.

Bieten die neuen Anforderungen aus dem BSI-Gesetz und der Kritis-VO für die Geschäftsführung nur Risiken oder auch Chancen?

Die Umsetzung der Anforderungen aus dem BSI-Gesetz und der Kritis-VO Sicherheit bindet zusätzliche Personalressourcen und führen zu einem erhöhten Investitionsbedarf im IT-Bereich. Abweichungen von den gesetzlichen Vorgaben sind zukünftig bußgeldbewährt. Die Chance besteht natürlich darin, dass IT-Sicherheit einen höheren Stellwert innerhalb der Krankenhausorganisation erhält. Letztendlich dienen die gesetzlichen Vorgaben der Schadenabwehr, insbesondere im Kernbereich eines Krankenhauses, der Patientenversorgung. Hinzu kommt natürlich auch, dass die angemessene Umsetzung der Anforderungen aus dem Gesetz und der Verordnung auch das Haftungsrisiko des Geschäftsführers gegenüber dem Träger, also das Risiko der die Innenhaftung, minimiert.

Zum Abschluss des Gespräches. Haben Sie abschließend noch einen Rat für Ihre Kolleginnen und Kollegen?

Da kann ich gerne eine Reihe von Praxis-Tipps geben:

Gehen Sie das Thema IT-Sicherheit unverzüglich an, auch wenn Ihr Krankenhaus noch nicht als kritische Infrastruktur eingestuft ist.

Vereinbaren Sie noch heute einen Termin mit Ihrer IT-Leitung und vertrauen Sie auf deren Sachverstand.

Investitionen für IT-Sicherheit müssen den gleichen Stellenwert erhalten wie Investitionen in die Medizintechnik.

Vergessen Sie nicht die Haustechnik. Es gibt kaum noch Lüftungs- und Lichtsteuerungstechniken, die nicht gegebenenfalls zu Wartungszwecken externe Datenverbindungen benötigen.

Fördern Sie die Kommunikation zwischen dem Technischen Leiter und dem IT-Leiter.

Binden Sie die IT-Leitung bei Investitionsentscheidungen ein. Eine Vielzahl von Medizingeräten ist mit dem Krankenhausnetzwerk und/oder dem Internet verbunden. Hier muss die IT-Sicherheit geklärt werden.

Dokumentieren und Reglementieren Sie externe Online-Wartungs-Zugänge.

Unterbinden Sie, dass bei Wartungsarbeiten bezüglich Haustechnik und Medizintechnik durch den Hersteller Softwareupdates aufgespielt werden, die nicht durch die IT-Abteilung geprüft wurden.

Machen Sie sich bewusst, dass jedes Gerät im Krankenhaus mit einer IP-Adresse ein potenzielles Einfallstor für Cyberattacken sein kann.

Achten Sie schon bei der Ausschreibung und Beschaffung neuer Produkte auf die Einhaltung der Erfordernisse der IT-Sicherheit.

Implementieren Sie ein IT-Sicherheitsmanagement.

Lassen Sie sich die Aktivitäten regelmäßig reporten.

Und zu guter Letzt: Achten Sie bei der Auswahl externer Berater auch auf die Krankenhauskompetenz.

Herr Weinand, vielen Dank für das Gespräch.

Das Interview führte KU-Fachredakteur Marcel Leuschner.