Kenntnisse und Kompetenzen der IT-Abteilungen der Krankenhäuser

IT-Sicherheit im Krankenhaus – neue Herausforderungen managen

Die Bewältigung der zunehmenden Anforderungen in Bezug auf den Datenschutz und die Informationssicherheit stellt viele Krankenhäuser vor große Herausforderungen. Es gilt nicht nur, eine durchgehende Betriebsfähigkeit aufrecht zu erhalten, die zunehmend von der Unterstützung durch die IT-Systeme abhängt, sondern dabei auch den Schutz der sensiblen Patientendaten sowohl in rechtlicher als auch technischer und organisatorischer Hinsicht zu gewährleisten. Dafür bedarf es in den IT-Abteilungen der Krankenhäuser umfangreicher fachlicher Kenntnisse und methodischer Kompetenzen, um die IT-Sicherheit aktuell und auch künftig aufrecht zu erhalten. Hierbei müssen verschiedene Anforderungen berücksichtigt werden, ohne dabei die Bedürfnisse eines performanten Klinikbetriebs außer Acht zu lassen. Von Dipl. Wirtschaftsinformatiker Rüdiger Giebichenstein und Dipl.-Kaufmann Karsten Thomas, PwC AG Wirtschaftsprüfungsgesellschaft

Aktuelle Herausforderungen

Krankenhäuser stellen eine der wesentlichen Säulen des Gesundheitssektors dar und gehören damit zu dem Teil der Infrastruktur unserer Volkswirtschaft, die einem hohen Schutzbedarf unterliegt und deren Verfügbarkeit für die Gesellschaft von hoher Bedeutung ist. Der Gesetzgeber trägt diesem Umstand Rechnung und versucht, das Risiko des Ausfalls dieser sogenannten „kritischen Infrastrukturen" zu minimieren, indem die Betreiber verpflichtet werden, eine IT-Sicherheit nach dem aktuellen Stand der Technik zu gewährleisten.

Zudem wurde Ende 2015 mit der EU-Datenschutzgrundverordnung (EU-DS-GVO) ein in der Europäischen Union einheitliches Recht geschaffen, welches den Schutz der Vertraulichkeit von personenbezogenen Daten zum Ziel hat und bei Verstößen mit bis zu 4 % des Jahresumsatzes empfindliche Strafen vorsieht.

Dem gegenüber stehen die realen Bedrohungen, denen Krankenhäuser permanent ausgesetzt sind. Im Jahr 2015 war der Healthcare-Sektor der am häufigsten aus dem Internet heraus angegriffene Bereich überhaupt.[1] Welche verheerenden Auswirkungen ein Cyberangriff auf den Krankenhausbetrieb haben kann, zeigen bspw. die Fälle der Krankenhäuser, die sich Anfang 2016 mit Ransomware infiziert haben.[2]

Der Schutz sensibler Daten wird grundsätzlich zunehmend schwerer, da sich Daten heute physikalisch oft nicht mehr nur auf den eigenen Servern befinden, sondern mitunter an Software- und Geräteanbieter übertragen werden oder – bei der Nutzung von Cloud-Diensten wie z.B. zur Spracherkennung, zum Datenaustausch oder zur Gerätesynchronisation – an weitere Dienstleister außerhalb der eigenen Infrastruktur.[3]

Rüdiger Giebichenstein, Dipl.-Wirtschaftsinformatiker/ISO 27001 Lead Auditor, ist als Partner bei der PwC AG Wirtschaftsprüfungsgesellschaft mit den Beratungsschwerpunkten Cyber Risk & Security, Informationssicherheit, (IT-)Compliance und (IT-) Governance, (IT-)Risikomanagement und Datenschutz tätig.

Viele Anwender von IT-Systemen und mobilen Endgeräten nutzen solche Dienste in ihrem privaten Umfeld und erwarten vergleichbare Funktionalitäten auch in ihrer Arbeitsumgebung. IT-Bereiche sehen sich häufig in der Situation, die gewünschten Dienste entweder selbst anzubieten oder aber Anbieter zu finden, welche die Dienste rechtskonform mit entsprechenden Sicherheitsvorkehrungen betreiben – anderenfalls besteht die Gefahr, dass die Anwender mit Blick auf die Praktikabilität mitunter ohne Kenntnis der rechtlichen Anforderungen und des Schutzbedarfs eigenmächtig entspre-

chende Cloud-Dienste nutzen und so eine „Schatten-IT" aufbauen, die für das Krankenhaus ein hohes Risiko darstellt.

Werden Daten unautorisiert an fremde Server übertragen, auf welche der IT-Bereich des Krankenhauses keinen Einfluss bzw. Zugriff mehr hat, birgt dies hohe Risiken. Wenn Mitarbeiter private Benutzerkonten bei Cloud-Anbietern nutzen, liegen die Daten außerhalb der Hoheit des Krankenhauses, könnten einem fremden Zugriff unterliegen - und wenn der Mitarbeiter das Unternehmen verlässt, sind diese Daten für den Arbeitgeber nicht mehr verfügbar Somit ist die Nutzung von Cloud-Diensten weder mit den Datenschutzgesetzen oder anderen rechtlichen Anforderungen, noch mit den Interessen der Krankenhausorganisation in Einklang zu bringen, sofern nicht technische, organisatorische und prozessuale Vorkehrungen getroffen werden, die z.B. eine rechtskonforme Auftragsdatenverarbeitung sicherstellen.
Dass die Datensammlung durch Hersteller von Anwendungssoftware und Betriebssystemen zunimmt und Information zur verwertbaren Ware wird, ist nicht neu. Sich davor zu schützen, bekommt allerdings eine neue Dimension. Die Auswirkungen der Cyberangriffe gerade auch auf Krankenhäuser in den letzten Monaten haben gezeigt, dass noch ein erheblicher Nachholbedarf bezüglich des Sicherheitsverhaltens der Nutzer sowie des Einsatzes hinreichend sicherer prozessualen, organisatorischen und technologischen Maßnahmen besteht.
Um diesen Risiken mit strukturierten Maßnahmen zu begegnen und die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit sicherzustellen, stehen verschiedene prozessuale, organisatorische und technische Maßnahmen bereit, die über die IT-Abteilung hinaus die gesamte Organisation des Krankenhauses einbeziehen und ein offizielles und nachhaltiges Committment des Managements voraussetzen.

Ein Informationssicherheits-Managementsystem (ISMS) bietet den geeigneten Rahmen, um alle Aspekte rund um die Informationssicherheit nachhaltig steuern und kontrollieren zu können.

Wie bei den meisten Managementsystemen besteht auch für die Informationssicherheit die Möglichkeit der Ausrichtung an einem internationalen Standard, in diesem Falle der ISO/IEC 27001. Nach diesem Standard ist auch eine Zertifizierung des ISMS möglich, um den Nachweis angemessener und funktionaler Prozesse in Bezug auf die Informationssicherheit zu erbringen. Die genannte ISO-Norm spezifiziert die Anforderungen für die Konzeption, Implementierung, Betrieb, Überwachung und Verbesserung eines dokumentierten ISMS unter Berücksichtigung der identifizierten IT-Risiken innerhalb der gesamten Organisation. Außerdem spezifiziert sie konkrete Sicherheitsmechanismen, welche an die Gegebenheiten der jeweiligen Organisationen zu adaptieren sind (vgl. Abbildung 1).

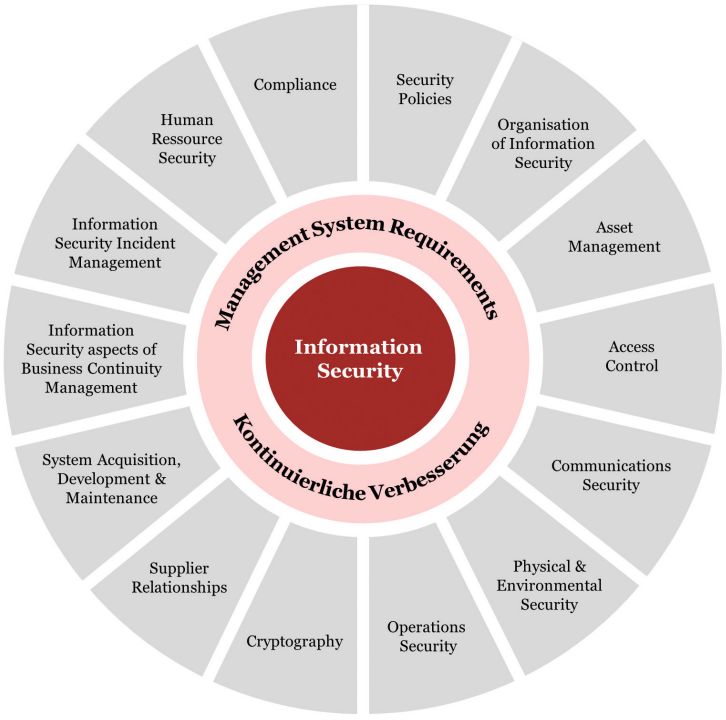

Abbildung 1: Informationssicherheits-Managementsystem (ISMS) nach ISO 27001

Es handelt sich bei der ISO/IEC 27001 grundsätzlich um einen branchenneutralen Standard. Allerdings gibt es branchenspezifische Abwandlungen und Ergänzungen wie z.B. die ISO/IEC 27799 für das Gesundheitswesen[4], durch die eine weitere Spezifizierung z.B. anhand von branchenspezifischen Best-Practice-Ansätzen erfolgt und Pflichtmaßnahmen vorgegeben werden.

Die für die Einführung eines ISMS erforderlichen Schritte werden anhand eines Phasenmodells (vgl. Abbildung 2) nachfolgend beispielhaft dargestellt.

Phase 1: Kontext der Organisation und Geltungsbereich des ISMS festlegen

Die Maßnahmen zur Einhaltung der Schutzziele müssen sich immer in einem ökonomisch angemessenen Rahmen bewegen und an der gegebenen Risikosituation orientieren.

Daher muss zunächst der Geltungsbereich (Scope) festgelegt werden, um bei Bedarf solche (Verwaltungs-)Bereiche des Krankenhausbetriebs aus dem Scope des Informationssicherheitsmanagements auszuklammern, die weder Träger schutzbedürftiger Daten noch für die Aufrechterhaltung der Versorgungsdienstleistung notwendig sind (vgl. Abbildung 3).

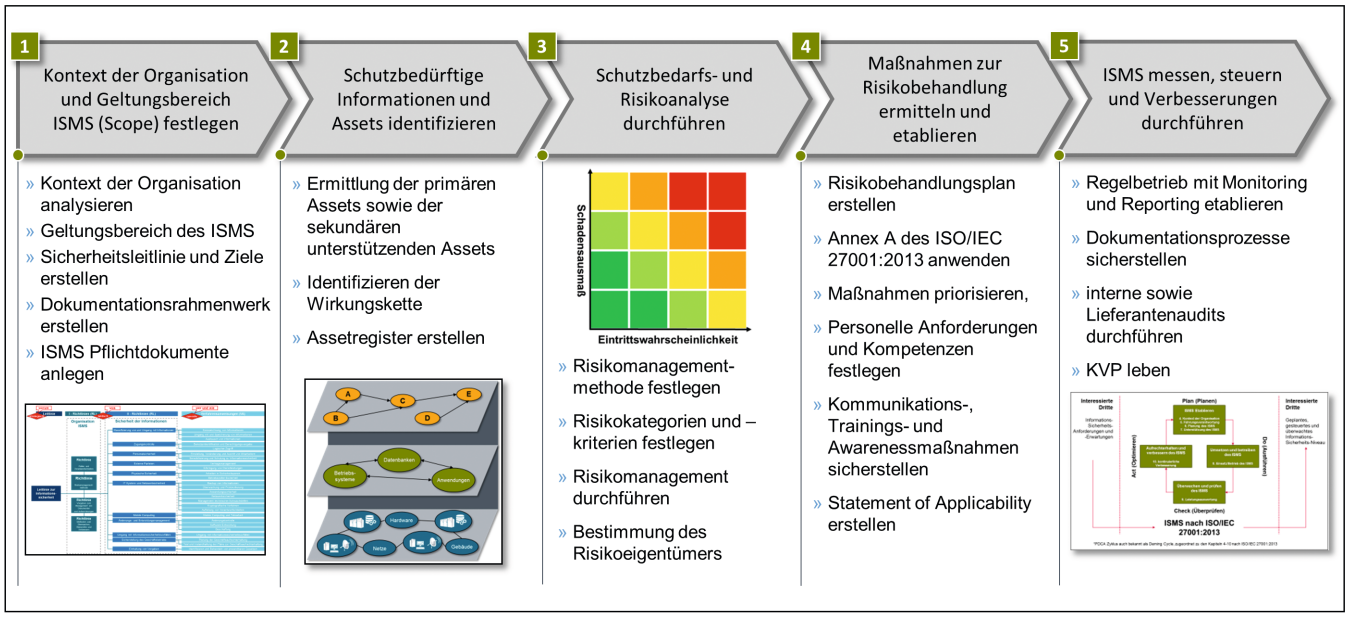

Abbildung 2: Phasenmodell zur ISMS-Implementierung[5]

Dabei müssen insbesondere auch die rechtlichen und vertraglichen Anforderungen sowie Schnittstellen zu externen beteiligten Parteien beachtet werden.

Die folgenden Fragestellungen können bei der Festlegung des Scopes unterstützen:

- Welche Organisationseinheiten im Unternehmen sollen vom ISMS künftig abgedeckt werden und welche nicht (Grenzen)?
- Welches sind die (informationsverarbeitenden) Prozesse und die dazu gehörigen Datenflüsse? Wo liegen diese?
- Welche externen Parteien („Dritte“) sind zu berücksichtigen (Patienten, Mitarbeiter, Dienstleister, Lieferanten, Behörden etc.)?
- Welche expliziten und impliziten Anforderungen und Erwartungen stellen diese „Dritten“ an die Organisation bzw. das ISMS?

Welche externen Einflussfaktoren (u. a. rechtlich-regulatorische Vorgaben, Wettbewerbssituation, Marktstellung, Branchenspezifika) sind zu berücksichtigen?

Zusätzlich sollte frühzeitig ein integriertes und aufeinander abgestimmtes Dokumentationsrahmenwerk erstellt werden, welches eine Leitlinie der Informationssicherheit, entsprechende Richtlinien und weitere Dokumente enthält, die insbesondere bei einer beabsichtigten Zertifizierung obligatorische Voraussetzung sind.

Phase 2: Schutzbedürftige Informationen und Assets identifizieren

Damit durch die Maßnahmen in Bezug auf die Informationssicherheit ein effizienter und umfassender Schutz gewährleistet werden kann, ist es notwendig, zunächst die Informationswerte zu inventarisieren. Informationswerte beschreiben sowohl alle Arten von Informationen (z.B. Patientenstammdaten, Behandlungsdaten oder Befunde einschließlich digitaler Bilddaten etc.), als auch die IT-Anwendungen (z.B. Krankenhausinformationssystem, Archivsystem und deren Vorsysteme) und IT-Infrastrukturkomponenten (z.B. Server, Clients, Netzwerkkomponenten, aber auch Medizintechnik), die für den Klinikbetrieb notwendig sind. Es hat sich bewährt, anhand des in Abbildung 4 dargestellten Schichtenmodels vorzugehen.

Demnach sollten zuerst alle Prozesse des festgelegten Geltungsbereichs einschließlich des dabei aufkommenden Datenflusses erfasst werden, um die verarbeiteten Informationen zu identifizieren. Hierbei sind auch ggf. in die Prozessdurchführung einbezogene externe Dienstleister zu berücksichtigen. Darauf aufbauend werden die für die Prozessdurchführung eingesetzten IT-Anwendungen sowie deren untereinander existierenden Schnittstellenbeziehungen ermittelt. Aus diesen Informationen lassen sich letztendlich die genauen IT-Infrastrukturkomponenten, die für den Betrieb der Anwendung notwendig sind, ableiten. Wichtig dabei ist, dass für alle Informationswerte eine Wirkungskette nachgezeichnet werden kann. Die Erfahrung zeigt, dass diese Erfas-

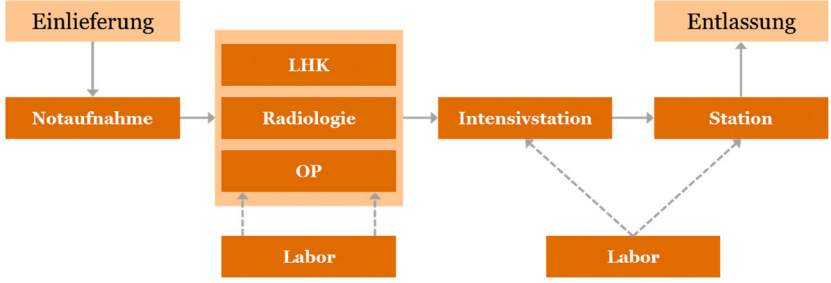

Abbildung 3: Beispielhaftes Ablaufschema Krankenhausbereiche[6]

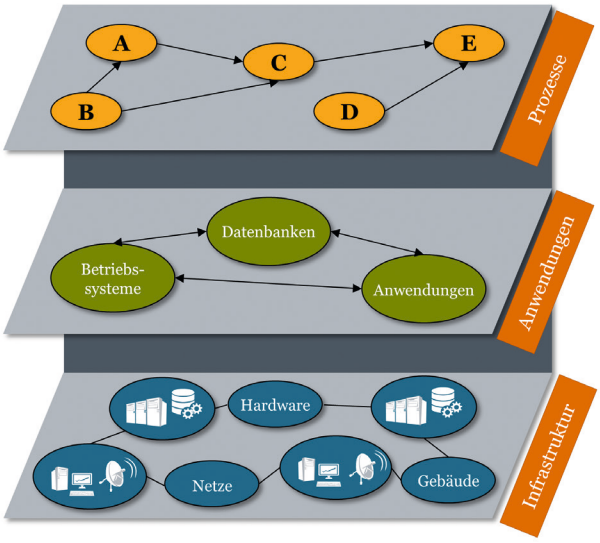

Abbildung 4: Schichtenmodell

sung idealerweise in Form eines Asset-Registers dokumentiert wird. Aus diesem lässt sich nachfolgend die Risiko- bzw. Kritikalitäts- und Schutzbedarfsanalyse aufbauen.

Phase 3: Schutzbedarfs- und Risikoanalyse durchführen

Um zu bestimmen, welches Schutzniveau für einen bestimmten Betriebsablauf inklusive seiner zugehörigen IT-Services und sekundären Assets angemessen ist, müssen Prozesse und Assets zunächst bewertet werden. Ein anerkanntes Instrument hierfür ist die Business Impact Analyse (BIA) (vgl. BSI-Standard 100-4: Notfallmanagement). Sie beinhaltet in der Praxis ein strukturiertes Interview auf Basis eines standardisierten und strukturierten Fragenkataloges, welches mit den vom Scope eingeschlossenen Fachbereichen geführt wird.
Die Zielsetzung der BIA ist, die maximale Schadenshöhe durch Verletzungen der Schutzziele der Informationssicherheit innerhalb der einzelnen Prozesse aus fachlicher Sicht zu identifizieren. Gleichzeitig wird auch die allgemeine Risikotoleranz ermittelt. Daraus können später die individuellen Schutzbedarfsanforderungen abgeleitet werden. Die Schadenspotentiale müssen für jedes der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) konkretisiert und in Kategorien eingeteilt werden. Hierbei gilt es darauf zu achten, dass mit wenigen unternehmensindividuellen Kategorien gearbeitet wird.

Eine strukturierte Gefährdungsanalyse ermöglicht eine umfassende Sicht auf Bedrohungen und Schwachstellen (in Kombination als Gefährdungen bezeichnet) von Assets und deren Eintrittswahrscheinlichkeit. Ausgewählte Bedrohungen und Schwachstellen werden zu Gefährdungen zusammengeführt, um eine vereinfachte Bewertungsmöglichkeit zu schaden. Eine umfangreiche Gefährdungsliste liefert bspw. das BSI (vgl. BSI-Gefährdungskataloge) oder die ISO 27005. Bei der Beurteilung der Gefährdungen hinsichtlich ihrer Eintrittswahrscheinlichkeit sollen bereits vorhandene oder geplante Maßnahmen berücksichtigt werden. Für eine fundierte Gefährdungsanalyse empfiehlt es sich, diese im Rahmen einer Expertenrunde durchzuführen, um die Fragestellung durch auskunftsfähige Experten klären zu können.

Die eigentliche Risikobeurteilung kommt zustande, indem die durch die BIA ermittelten Schadensauswirkungen je Prozess nun mit der ermittelten Eintrittswahrscheinlichkeit einer Gefährdung zusammengeführt werden, was dann ein bewertetes Risiko als Ergebnis liefert.
Aus den ermittelten Werten für Ausmaß und Eintrittswahrscheinlichkeit ergibt sich eine Einordnung in Form einer Matrix, der sog. Risikomatrix. Wenn dies für jede relevante Gefährdung erfolgt ist, ist die Risikoanalyse abgeschlossen. Anhand der Liste können die bewerteten Risiken priorisiert werden und ein Risiko-Eigentümer festgelegt werden.

Phase 4: Maßnahmen zur Risikobehandlung ermitteln und etablieren

Im Anschluss an die Risikoanalyse wird festgelegt, wie diese Risiken behandelt werden sollen. Grundsätzlich sind für die Risikobehandlung folgende Maßnahmen denkbar: Vermeiden, Verringern, Transferieren oder Akzeptieren.

Vermieden werden können Risiken meist dadurch, dass entweder auf eine risikobehaftete Technik oder aber die Speicherung einer bestimmten Information grundsätzlich verzichtet wird. Aufgrund der durch den Klinikbetrieb bedingten Vorgaben besteht diese Option in der Praxis in vielen Fällen nicht. Meist bietet es sich an, das Risiko zu verringern, indem auf wirksame Maßnahmen bzw. Kontrollmechanismen zurückgegriffen wird, um z.B. Schwachstellen zu beheben oder zumin-

Karsten Thomas, Dipl.-Kaufmann, CISA/CRISC, ist als Senior Manager und Prokurist bei der PwC AG Wirtschaftsprüfungsgesellschaft mit den Beratungsschwerpunkten Cyber Risk & Security, (IT-) Risikomanagement, (IT-) Governance, (IT-) Compliance, Datenschutz tätig.

dest den Aufwand, um diese auszunutzen, soweit zu erhöhen, dass ein Angriff unattraktiv wird.

Die Option, Risiken zu transferieren, z.B. indem sie versichert werden, ist i.d.R. nur dann sinnvoll, wenn ein Sicherheitsvorfall überwiegend monetäre Auswirkungen hat. Für Krankenhäuser, die einen Versorgungsauftrag wahrnehmen u.a. die durchgehende Verfügbarkeit gewährleisten müssen, kann dies demnach nur eine nachrangige Option darstellen, die ergänzend wirkt und die monetäre Schadenhöhe verringert. Da nicht alle Risiken in einem ökonomisch vertretbaren Maße minimiert werden können, bedingt dies auch, dass einige Risiken bzw. Restrisiken nach der Umsetzung von Maßnahmen schlicht akzeptiert werden müssen.

Es erfolgt die Zuordnung der Maßnahmen für jede Gefährdung (1:n-Beziehung von Gefährdungen zu Maßnahmen). Es entsteht somit ein Risikobehandlungsplan. Dieser umfasst die noch zu erledigenden Maßnahmen, um das ISMS zu etablieren. Jede Maßnahme wird dann priorisiert, ausgearbeitet und einem Verantwortlichen zur Umsetzung übertragen. Dieser steuert und überwacht die Durchführung bis zur Fertigstellung.

Zeitgleich müssen die Monitoring- und Reportingprozesse etabliert sowie entsprechende Kennzahlen (KPI) entwickelt werden. Mess- und Kontrollpunkte sind zu aktivieren, welche zur Überprüfung der ISMS-Performance und Wirksamkeit herangezogen werden. Eventuelle Dienstleister (externe Parteien) sind hierbei ebenfalls mit zu berücksichtigen.

Phase 5: ISMS messen, steuern und Verbesserungen durchführen

Da Prozesse, eingesetzte Technologien und damit verbundene Schwachstellen sowie die vorliegende Bedrohungslage einem stetigen Wandel unterliegen, ist es notwendig, die Risikobewertung und die daraus resultierenden Maßnahmen regelmäßig neu zu evaluieren. Zudem ist das zielgerichtete Behandeln von Risiken regelmäßig dann erfolgreich, wenn im Anschluss an die Umsetzung von Maßnahmen eine Überprüfung der Wirksamkeit erfolgt und ggf. eine Adjustierung an veränderte Anforderungen oder von nicht optimalen Maßnahmen vorgenommen kann.

Als ein kontinuierlicher Verbesserungsprozess wird von dem Standard der PDCA- oder Deming-Zyklus vorgeschlagen (vgl. Abbildung 5). Damit wird ein vierstufiger iterativer Prozess beschrieben, nachdem umzusetzende Maßnahmen geplant (PLAN), implementiert (DO), anschließend auf ihre Wirksamkeit und Effizienz hin überprüft (CHECK) und dementsprechend verbessert werden (ACT).

Fazit

Aktuell ist zu beobachten, dass durch die Verabschiedung der EU-Datenschutzgrundverordnung und der für Anfang 2017 erwarteten zweiten Verordnung zum Geltungsbereich des IT-Sicherheitsgesetzes bei gleichzeitig stattfindenden medienwirksamen Cyberangriffen der Druck auf die Krankenhaus-IT,

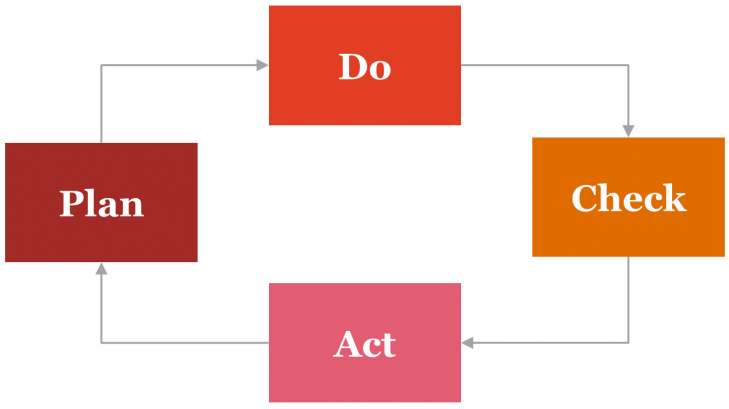

Abbildung 5: PDCA-Zyklus

ein an den aktuellen Anforderungen ausgerichtetes Sicherheitsniveau herzustellen und zu erhalten, so hoch wie noch nie ist. Um diesen Anforderungen gerecht zu werden, ist es für Krankenhäuser zwingend notwendig, die für das aktive Management der Risiken erforderlichen Kompetenzen aufzubauen und vorzuhalten. Aufgrund der Bedrohungslage und der zeitlichen Vorgaben der EU-Datenschutzgrundverordnung und des IT-Sicherheitsgesetzes erscheint es sinnvoll, diese Schritte sehr zeitnah anzugehen. Erfahrungsgemäß ist die vom Gesetzgeber jeweils vorgegebene Zeit bis 2018 für die Umsetzung eines adäquaten ISMS relativ knapp bemessen.

Die Einrichtung eines Informationssicherheits-Management-Systems stellt eine strukturierte und nachhaltige Vorgehensweise sicher. Des Weiteren verspricht die adäquate Anwendung, unter Berücksichtigung der branchenspezifischen Anforderungen im Gesundheitswesen, ein angemessenes Schutzniveau für die kritischen Daten herzustellen und aufrechtzuerhalten sowie den wachsenden Bedrohungen langfristig die richtigen Maßnahmen entgegen zu setzen.

Datenschutz und die Nutzung von Windows 10

Risiken bei sensiblen Patientendaten?

Ohne weiteres ist eine Datenübermittlung schutzbedürftiger Daten wie Patientendaten zu Microsoft oder anderen Anbietern in der Regel unzulässig und birgt einige Risiken. Doch ein Verzicht auf Windows 10 ist nicht erforderlich. Durch gezieltes Management der Risiken lässt sich Windows rechtskonform nutzen und an den Schutzbedarf der Daten anpassen. Im Krankenhaus-IT Journal Ausgabe 5/2016 veröffentlichten Rüdiger Giebichenstein und Karsten Thomas, PwC AG Wirtschaftsprüfungsgesellschaft, einen Beitrag über Datenschutz und die Nutzung von Windows 10.