führen und wirtschaften im Krankenhaus

f&W

4|18

April 2018 | 35. Jahrgang

H 5162 | ISSN 0175–4548

Offizielles Organ des BDPK,
des BVBG und des DVKC sowie
Medienpartner der Entscheiderfabrik

Sonderdruck

Abwarten ist keine Strategie

Umsetzung des IT-Sicherheitsgesetzes

Umsetzung des IT-Sicherheitsgesetzes

Abwarten ist keine Strategie

Noch läuft die Frist zur Umsetzung des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG). Betroffen sind Krankenhäuser mit mehr als 30.000 stationären jährlichen Behandlungsfällen. Sie sollten sich bereits jetzt mit den neuen Anforderungen auseinandersetzen.

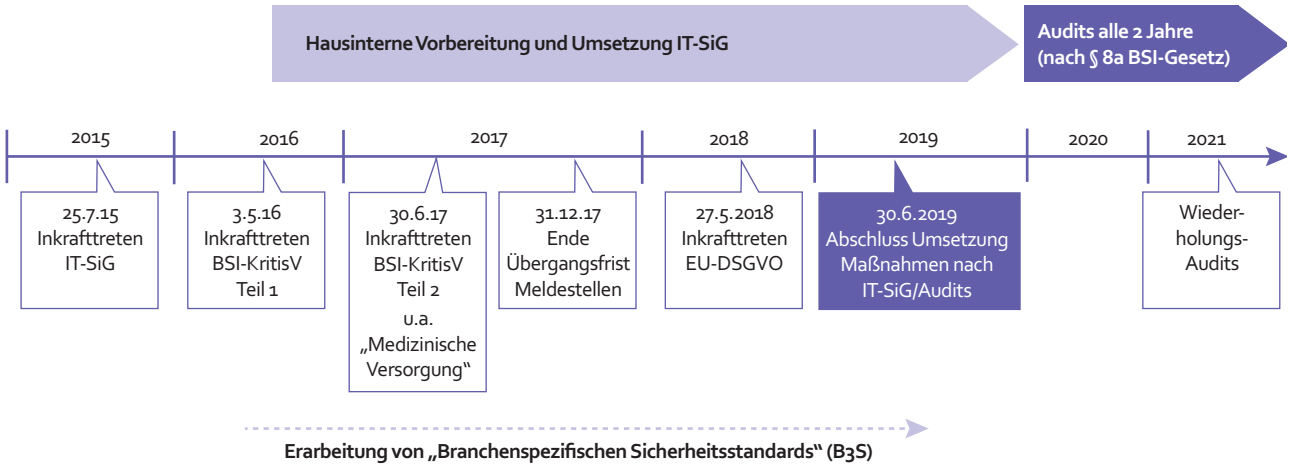
Von Michael Thoss, Prof. Dr. Thomas Kersting

Mit dem seit Juli 2015 gültigen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, IT-SiG) will die Bundesregierung dazu beitragen „die IT-Systeme und digitalen Infrastrukturen Deutschlands zu den sichersten weltweit zu machen“. Dabei geht es um die sogenannten „Kritischen Infrastrukturen“ (Kritis) wie Strom- und Wasserversorgung, Finanzen oder Ernährung, aber eben auch Gesundheit. Ein Ausfall oder eine Beeinträchtigung der Versorgungsdienstleistungen dieser Systeme hätte vermutlich dramatische Folgen für Wirtschaft, Staat und Gesellschaft in Deutschland. Ihre IT-Systeme sollen daher abgesichert werden.

Im Mai 2016 ist bereits der erste Teil der Kritis-Verordnung des Bundesamtes für Sicherheit und Informationstechnik, BSI (BSI-KritisV gemäß § 10 BSI-Gesetz), zur Umsetzung des IT-SiG in Kraft getreten. Er betraf zunächst die Unternehmen aus den Sektoren Energie, Informationstechnik und Telekommunikation, Wasser sowie Ernährung. Aber: Mit der ersten Verordnung zur Änderung der BSI-KritisV, die seit 30. Juni 2017 gilt,

Foto: GettyImages.de/ValeryBrozhinsky

Ablauf und Fristen der Umsetzung des IT-SiG



Quelle: IMC clinicon
Abb. 1

kommen die Sektoren Finanz- und Versicherungswesen, Transport und Verkehr sowie Gesundheit hinzu. In § 6 ist der Bereich Gesundheit detailliert beschrieben. Krankenhäuser müssen geeignete Schutzmaßnahmen ab einer Fallzahl von jährlich 30.000 vollstationären Fällen nachweisen.

Potenziell vom IT-SiG betroffene Krankenhäuser (Hochrechnung)

Fallzahl 2015	Anzahl Häuser	Teilnahme ab 2018/2019
> 29.999	133	verpflichtend
> 29.000	14	wahrscheinlich
> 28.000	20	vermutlich

Anmerkung: Verbünde und Klinikgruppenzugehörigkeit noch nicht berücksichtigt
Quelle: IMC clinicon, eigene Berechnungen auf Basis der Qualitätsbericht der Krankenhäuser 2015
Tab. 1

Unklare Anforderungen

Doch die Anforderungen für die betroffenen Krankenhäuser sind bisher nicht klar definiert. Und sie werden vermutlich auch in Zukunft wegen der dramatischen Geschwindigkeit der Veränderungsprozesse der IT sehr schwierig zu handhaben sein. Helfen könnte der sogenannte „Branchenspezifische Sicherheitsstandard", kurz B3S. So schreibt § 8a des IT-SiG vor, dass Betreiber von Kritis bis 30. Juni 2019 Vorkehrungen nach dem Stand der Technik „gegen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit" ihrer Systeme treffen müssen. Um dieser Anforderung zu genügen, können oder besser sollen Kritis-Betreiber und ihre Verbände „Branchenspezifische Sicherheitsstandards" erarbeiten, die das BSI dann prüfen kann.

Der B3S soll also dabei helfen, einen Orientierungsrahmen für die Anforderungen des IT-SiG zu schaffen. An diesem könnten sich betroffene Kliniken theoretisch orientieren. Dies ist in der Tat nur theoretisch zu sehen, denn der Standard steht zum einen mehr als acht Monate nach Beginn des zweijährigen Zertifizierungszeitraums Anfang Juli 2017 noch gar nicht zur Verfügung. Zum anderen ist die Verabschiedung des Standards keine zwingende Voraussetzung, den gesetzten Rechtspflichten nachzukommen. Die Maßgaben des IT-SiG müssen auch ohne eine branchenspezifische Regelung oder eine allgemeine Vorlage erfüllt werden. Daher ist abwarten keine Lösung.

Hausspezifische Standards entwickeln

Betroffene Krankenhäuser müssen jetzt beginnen zu handeln. Dabei ist ihnen die Wahl der Werkzeuge grundsätzlich freigestellt. Da es nicht sinnvoll ist, das Rad neu zu erfinden, sollten sie sich an vorhandenen Standards orientieren.

Interview

"Gerüstet sein"

Drei Fragen an Jens Schulze, Leiter Abteilung Informationstechnologie, Klinikum Leverkusen Service GmbH

Was sind derzeit die größten Hürden bei der Umsetzung des IT-SiG?

In NRW hat die landeseigene Krankenhausgesellschaft eine Arbeitsgruppe für die von Kritis betroffenen Krankenhäuser initiiert. Allein aus dieser Gruppe ist zu entnehmen, dass sich die überwiegenden Häuser bei der Herangehensweise sehr schwer tun.
Das beginnt bei der Aufklärung oder beim Commitment der Geschäftsführung zu Kritis im eigenen Haus, geht über die Einführung eines IT-Sicherheitsbeauftragten im Unternehmen bis zum Etablieren einer Meldestelle nach § 8b BSIG und tangiert ebenso die Definition des Geltungsbereichs im eigenen Krankenhaus.

Welchen Lösungsansatz verfolgt Ihr Haus?

Um die Einführung eines Information Security Management Systems (ISMS) werden wir nicht herumkommen. Diesbezüglich gibt es aktuell Gespräche mit der Geschäftsführung. Sobald wir die Unterstützung der Geschäftsführung in puncto ISMS haben, werden wir uns in Richtung ISO/IEC 27001 Zertifizierung bewegen, dabei den IT-Grundschutz des BSI berücksichtigen und somit gut für den zukünftigen branchenspezifischen Sicherheitsstandard (B3S) gerüstet sein. Auf fertige Lösungen warten oder Eigendefinitionen kreieren, das ist bei den wenigen verfügbaren Ressourcen verschenkte Zeit.

Wie geht man mit dem Thema „Audit" und Anpassungsbedarf um?

Mit der Einführung eines Information Security Management Systems und zur Vorbereitung auf die ISO/IEC 27001 Zertifizierung werden sicher Prozessanpassungen im Unternehmen vorgenommen werden müssen. Man hat also so die Chance oder sogar Verpflichtung, veraltete und schlechte Prozesse zu aktualisieren. Es empfiehlt sich bei den resultierenden Prozessanpassungen existierende Normen und Standards zu berücksichtigen, sodass man für Audits eine gute Ausgangssituation hat.

Grundsätzlich ist es dabei zulässig – und wegen des fehlenden „Branchenspezifischen Sicherheitsstandards" vermutlich sinnvoll –, einen eigenen Standard für das jeweilige Unternehmen zu definieren: Dieser muss lediglich qualitativ den aktuellen Stand der Technik definieren und die Schutzmaßnahmen darstellen. Als Grundlage kann unter anderem der IT-Grundschutz des BSI dienen.

Dieses Werk dürfte allerdings in seiner Gesamtheit die meisten Organisationen im Gesundheitswesen überfordern. Mögliche weitere Lösungsansätze leiten sich aus der Kombination vorhandener Normen ab: Das kann als Grundlage die DIN ISO/IEC 27001 (Anforderungen für das Einrichten, Realisieren, Betreiben und Optimieren eines dokumentierten Informationssicherheits-Managementsystems) mit Ergänzungen beispielsweise aus der DIN 50600 (Rechenzentrumsbau) liefern.

Informationssicherheits-Managementsystem nötig

Unverzichtbar ist in jedem Fall der Aufbau eines Informationssicherheits-Managementsystems (ISMS). Das stellt eine dauerhaft zu leistende Arbeit dar, weil sich beteiligte Technologiegruppen des Krankenhauses kontinuierlich stark wandeln. Das klassische Risikomanagement des Unternehmens im Sinne einer Früherkennung etwa nach dem Gesetz zur Kontrolle und Transparenz (KonTraG) ist für diese Zwecke ungeeignet oder benötigt eine Revision. Denn es geht nicht nur darum, bestimmte Risiken lediglich zu erkennen, sondern im Bereich der IT grundsätzlich zu vermeiden. Das bedeutet ebenfalls, dass verschiedene Prozesse des Unternehmens umgestaltet werden müssen. Ein Beispiel für solche Anpassungen liefert der Einsatz von Elementen der DIN 80001 im Rahmen der Beschaffung von Anlagen mit informationstechnischen Komponenten, egal ob Informationstechnik, Medizintechnik oder Versorgungstechnik des Krankenhauses betroffen sind.

Die Ausrichtung des IT-SiG auf spezifische Gefährdungen und deren

Vermeidung macht es neben der Einrichtung eines IT-Sicherheitsbeauftragten – meist als neue und zusätzliche Ressource – auch erforderlich, verbindliche Veto-Rechte der Sicherheit in Beschaffungsprozessen zu definieren. Im Klartext bedeutet ein derartiges Veto-Recht, dass unter Umständen nicht die billigste Beschaffung umgesetzt werden kann, weil sie die notwendigen Mindestanforderungen an die Sicherheit nicht erfüllt. Alle diese Arbeitsschritte erfordern einen umsichtigen zeitlichen Vorlauf, wobei der Zeitrahmen insgesamt durch die gesetzlichen Vorgaben bereits gesetzt ist (Abbildung 1).

Die Umsetzung des IT-SiG erfordert (neben der EU-Datenschutz-Grundverordnung, EU-DSGVO) zusätzliche personelle und finanzielle Kapazitäten. Sie benötigt nachhaltige, neue oder zumindest angepasste Prozesse und wird dauerhaft Ressourcen in Personal, Sach- und Finanzmitteln binden, die vermutlich in der Regel nicht aus dem Bestand bereitgestellt werden können. In den zwei Jahren zwischen den zukünftig vorgeschriebenen Audits erfordert das laufende und dynamische Veränderungsmanagement im Rahmen der digitalen Transformation der Krankenhäuser eine ständige Präsenz und Aufmerksamkeit der Verantwortlichen.

Checkliste: Kritis-Vorbereitung Audits

Ansatz	Maßnahmen
Entscheidung	✓ Start der Maßnahmen ✓ Entscheidung zum Lösungsansatz „Aktueller Stand der Technik" (Norm, Selbstverwaltung) ✓ Budgetierung ✓ Managementführung des Projektes
Organisation	✓ Anpassung der Beschaffungsverfahren (z. B. angelehnt an DIN 80001) zur Etablierung künftiger Sicherheitsstandards ✓ Vorgabe von Rahmenbedingungen für IT-vernetzte Güter ✓ Definition der Kommunikationsregelungen bei Störfällen (Pflicht: BSI, Kür: Öffentlichkeit)
Personal	✓ Auseinandersetzung mit dem entstehenden Aufwand der IT ✓ Schaffung und Ausbildung eines IT-Sicherheitsbeauftragten (IT-SiB) ✓ Klärung weiterer benötigter Ressourcen für das Projekt und den laufenden Betrieb
Dokumentation	✓ Anpassung der technischen Dokumentation zur Identifizierung kritischer Systeme z. B. angelehnt an OBASHI (1). ✓ Betrachtung nicht nur der IT, sondern auch der Medizintechnik und anderer integrierter Systeme (Hintergrund: Diese Überlegungen sind auch sinnvoll im Rahmen der Umsetzung der DSGVO und der erforderlichen Datenschutz-Folgenabschätzung.)
IT-Sicherheits-management	✓ Aufbau eines Informationssicherheits-Managementsystems (ISMS). ✓ Verinnerlichung des Aufwandes an Dokumentation, Fortschreibung und Umsetzung im eigenen Haus ✓ Vermittlung und Stärkung der Funktion des IT-SiB
Audit	✓ Auswahl möglicher Auditoren ✓ Abstimmung möglicher Verfahrensansätze ✓ Entscheidung eigene Qualifizierung vs. Dienstleistungspartner (alle 2 Jahre)

Quelle: IMC clinicon; (1) OBASHI: Im Prinzip stellt OBASHI ein Regelwerk dar, wie die Abhängigkeiten und Datenflüsse zwischen Geschäftsprozessen und IT dargestellt werden können. OBASHI steht für Ownership, Business Process, Application, System, Hardware, Infrastructure. Mit dem Blick auf die Sicht des BSI im Sinne Versorgungssicherheit steht hier der Versorgungsprozess des Patienten mit klinischen Leistungen der Diagnose, Therapie und Pflege im Mittelpunkt.

Tab. 2

Mehr als 160 Kliniken ab sofort betroffen

Tabelle 1 auf Basis von Auswertungen der Qualitätsbericht der Krankenhäuser (2015) zeigt die Anzahl betroffener Krankenhäuser. Würde ein Fallwachstum von zwei bis vier Prozent pro Jahr unterstellt und würden zudem die Fallzahlen von in Gruppen oder Verbünden organisierter Krankenhäuser zusammengezählt, könnte die Anzahl betroffener Einrichtungen 2018 tatsächlich bereits deutlich über 160 liegen.

Möglicherweise betroffene Einrichtungen sollten daher mit Blick auf die laufenden Fristen frühzeitig ihre Leistungsentwicklung bewerten. Dazu gehören potenziell auch Verbünde mit gemeinsam genutzten Anlagen. Bis 30. Juni 2019 müssen in allen relevanten Fällen die Audits erfolgt sein. Dies macht im Vorfeld eine eigene Unternehmensentscheidung zum Prüfungsstandard erforderlich. Krankenhäuser können bereits jetzt eine Reihe von Punkten erledigen, um gut vorbereitet zu sein.

Bereits Anfang Dezember 2017 wies das BSI im Rahmen einer Tagung des Deutschen Krankenhausinstituts (DKI) in Düsseldorf erneut darauf hin, dass die Erfüllung der gesetzlichen Auflagen nicht von der Verfügbarkeit des angestrebten B3S abhängig ist. Zudem könnten Bußgelder nach dem IT-SiG prinzipiell schon heute verhängt werden, denn auch die Einrichtung einer durchgehend erreichbaren Kontaktstelle und Verstöße gegen die Meldepflicht stellen bußgeldfähige Verstöße dar. Sämtliche Übergangsfristen dafür sind bereits abgelaufen. Die potenziellen Bußgelder bewegen sich zwischen 50.000 und 100.000 Euro (§ 14 IT-SiG). Eine Anwendung wäre prinzipiell möglich, ist aber – im Gegensatz zur Versorgungssicherheit – wohl nicht die primäre Intention des BSI.

Prof. Dr. Thomas Kersting
Geschäftsführer
IMC clinicon GmbH
Friedrichstraße 180
10117 Berlin

Michael Thoss
Senior Berater
IMC clinicon GmbH
Friedrichstraße 180
10117 Berlin
E-Mail: michael.thoss@imc-clinicon.de

2018 – Ist Ihr Krankenhaus vorbereitet?

Daten und Budget effektiv schützen

IMC clinicon

T + 49 30 230 809 888
www.imc-clinicon.de | info@imc-clinicon.de