MSzert 2019

IT-Sicherheitsgesetz

Anforderungen für das Gesundheitswesen

© MSzert GmbH
28.03.2019

Einleitung

Infrastrukturen im Allgemeinen und Kritische Infrastrukturen im Besonderen sind die unverzichtbaren Lebensadern moderner, leistungsfähiger Gesellschaften. In Deutschland existieren im Rahmen der nationalen Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) sowie der aktuellen Gesetzgebung für Einrichtungen und Institutionen im Gesundheitswesen viele neue Herausforderungen.

Am 30. Juni 2017 ist die Umsetzungsverordnung auch für das Gesundheitswesen in Kraft getreten. Mit dieser Ergänzung der Kritis-Verordnung (BSI-KritisV) wurden auch ganz konkrete Kriterien und Schwellenwerte für das Gesundheitswesen formuliert. Jetzt sind die Betreiber dieser Kritischen Infrastrukturen verpflichtet technische und organisatorische Maßnahmen zu ergreifen, um ihre Systeme nach dem „Stand der Technik“ abzusichern. Doch wer ist genau betroffen, wer nicht? Und welche Maßnahmen müssen getroffen werden?

Der „Nationale Plan zum Schutz der Informationsinfrastrukturen - Umsetzungsplan KRITIS“ (UP KRITIS) bildet seit 2007 im Wege einer „Public-private-Partnership“ die Basis für übergreifende Maßnahmen zum Schutz der kritischen Infrastrukturen. Bund und Länder unterscheiden 9 Sektoren Kritischer Infrastrukturen. Davon sind acht in der Plattform UP KRITIS organisiert, die jeweils noch einmal in einzelne Branchen unterteilt werden. Im Sektor Gesundheit werden nach den Vorgaben der BSI-KritisV drei Branchen unterschieden:

- Medizinische Versorgung
- Arzneimittel und Impfstoffe
- Labore

Schwellenwerte zur verpflichtenden Umsetzung:
Die BSI-KritisV regelt nicht nur für Krankenhäuser, sondern untern anderem auch für Laboratorien, Apotheken und Herstellern von Medizinprodukten, wer unter das IT-Sicherheitsgesetz fällt. Bei Krankenhäusern sind das alle Einrichtungen, die mindestens 30.000 vollstationäre Fälle pro Jahr dokumentieren. Damit sind in Deutschland rund 100 Krankenhäuser betroffen. Bei Herstellen bzw. Abgabestellen für Medizinprodukte liegt der Schwellenwert bei einem Umsatz von mindestens 90,6 Mio. Euro. Apotheken sind ab 4,65 Mio. abgegebene Packungen und Labore ab 1,5 Mio. Aufträge betroffen.

Chancen durch Etablierung eines ISMS:

- ✓ **Erfüllung gesetzlicher Anforderungen**
- ✓ **Erhöhung der Patientensicherheit unter Berücksichtigung der Behandlungseffektivität**
- ✓ **BSI-konformer Nachweis über die Erfüllung der Anforderungen aus dem IT-Sicherheitsgesetz**
- ✓ **erhöhte Sicherheit Ihrer IT-Systeme, -Prozesse und -Komponenten durch Absicherung nach dem Stand der Technik**
- ✓ **verbesserte Versorgungssicherheit Ihrer kritischen Dienstleistung**
- ✓ **gute Verknüpfungsmöglichkeit mit einer Zertifizierung nach ISO 27001 und dem damit verbundenen, international anerkannten Zertifikat**

Ansprechpartner

Wirt.-Ing. Thomas Welsch
Leiter der Zertifizierungsstelle

Dipl.-Ing. Stefan Oehm
Geschäftsführung

Telefon: +49 (0)6833 900 895-0

Telefax: +49 (0)6833 900 895-19

E-Mail: mszert@mszert.de

Stichtag für die Umsetzung

Seit dem 30. Juni 2017 ist mit der Änderungsverordnung (oder: dem „2. Korb“) nun auch für die Gesundheitsbranche die Umsetzung des IT-Sicherheitsgesetzes konkret formuliert. Die betroffenen Unternehmen und Organisationen haben zwei Jahre Zeit, die vom Gesetz definierten Anforderungen (IT-Systeme, -Komponenten und -Prozesse für ihre kritischen Dienstleistungen angemessen, nach dem Stand der Technik zu schützen) zu erfüllen. Stichtag für die Umsetzung ist der 30. Juni 2019.

Ergänzende Anforderungen

Zusätzlich zu diesen Anforderungen treten im Mai 2018 die Vorgaben der Datenschutz-Grundverordnung (DS-GVO) in Kraft. Diese Vorgaben betreffen zwar nicht ausschließlich das Gesundheitswesen, aufgrund der Verarbeitung hoch sensibler, personenbezogener Informationen steht dieses jedoch besonders im Fokus. Im Artikel 32 der DS-GVO wird wie bei den bisher dargestellten Anforderungen von der Umsetzung technischer und organisatorischer Maßnahmen auf Basis des „aktuellen Stand der Technik“ gesprochen.

Prüfgrundlage

Nachweise können durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Als Kriterienwerke hierfür sind entweder anerkannte Normen und Standards wie ein **Informationssicherheitsmanagementsystem nach ISO/IEC 27001** oder alternativ vom Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannte **branchenspezifische Standards (B3S)** zugelassen.

Davon ausgenommen ist das Einrichten der Meldestelle und deren Benennung beim BSI. Diese muss bereits bis zum 31. Dezember 2017 eingerichtet sein. Bei einer Nichterfüllung der definierten Anforderungen sind Bußgelder bis zu einer Höhe von 100.000 Euro für das verantwortliche Management möglich.

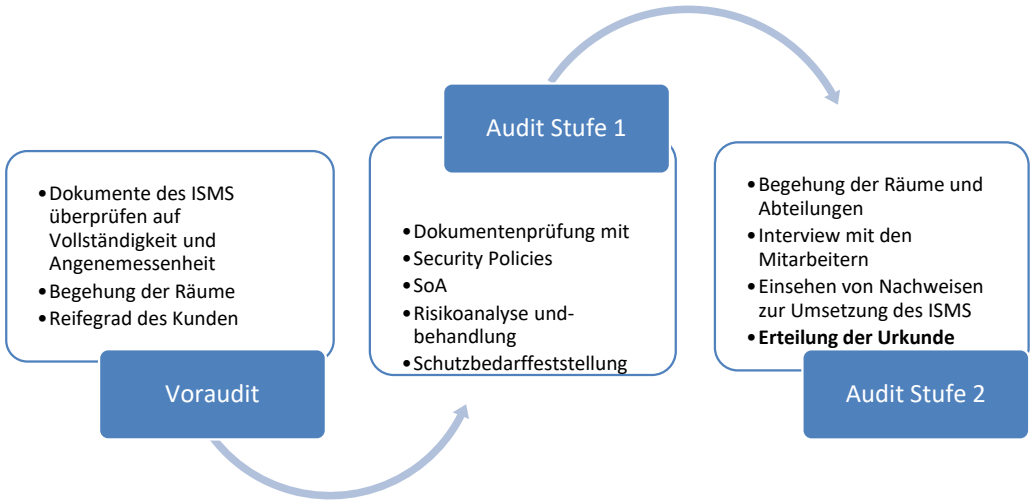
Was ist der richtige Weg?

Ein entscheidender und zielführender Lösungsansatz kann daher die sofortige Auseinandersetzung mit der ISO/IEC 27001 sowie dem veröffentlichten Branchenstandard sein, um diese verschiedenen gesetzlichen und behördlichen Anforderungen zu erfüllen und sich frühzeitig mit dieser komplexen Thematik auseinanderzusetzen. Das gilt auch dann, wenn die Organisationen nicht über den Schwellenwerten liegen und noch keine Branchenstandards vorliegen.

Ablauf der Prüfung

Für die „prüfende Stelle“ und deren Auditoren empfiehlt das BSI eine sogenannte „Spezielle Prüfverfahrenskompetenz“ als Qualifikationsnachweis. Die MSzert GmbH ist anerkannte Prüfstelle und akkreditierte Zertifizierungsstelle, u.a. für ISO 27001. Gerne stellen wir Ihnen alle geforderten Kompetenzen für einen BSI-konformen Nachweis zur Verfügung.

Der Ablauf der KRITIS-Prüfung basiert auf der BSI-Orientierungshilfe. Unser Angebot wird entsprechend diesen Vorgaben aufgebaut und mit Auditaufwänden versehen. Aufgrund unserer Erfahrungen bieten wir Ihnen eine KRITIS-Prüfung im Rahmen eines zweistufigen Verfahrens.



Aufwand und Ablauf der Auditierung

Der Umfang der Auditierung orientiert sich an der für alle akkreditierten Zertifizierungsstellen bindenden Norm ISO/IEC 17021-1. Hier werden in Abhängigkeit der Größe des QMS (Anzahl der Mitarbeiter im Geltungsbereich) folgende Vorgaben genannt.

Die Durchführung der Prüfung wird auf Basis einer Dokumentenprüfung als auch Vor-Ort Begutachtung organisiert.

Es ist davon auszugehen, dass von dem gesamt angesetzten Prüfaufwand mindestens 70% beim Kunden vor Ort erbracht werden.

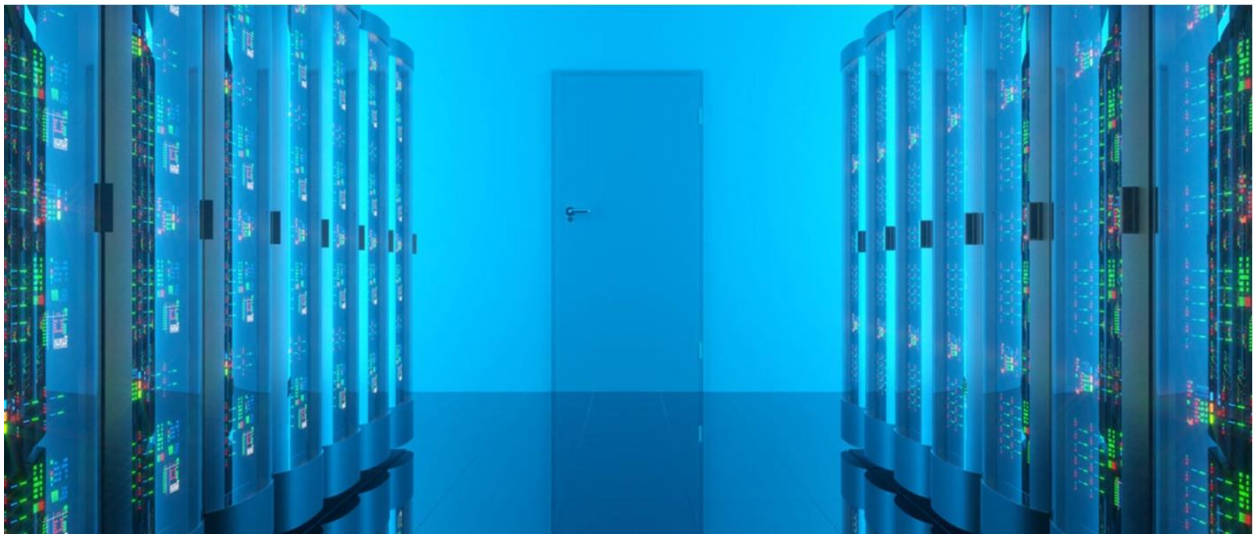
Tabelle zur Ermittlung des Prüftage-kontingentes nach Betreiberkomplexität:	Vollstationäre Fälle					
	Anzahl Fachabteilung	**30001-40000**	**40001-50000**	**50001-60000**	**60001-70000**	**>70000**
Fachabteilungen nach §301-Datenübermittlung	**<=20**	10	10	11	11	12
	<=30	11	11	12	12	13
	<=40	12	12	13	13	14
	<=50	13	13	14	14	15
	<=60	14	14	15	15	16
	>60	15	15	16	16	25
	Hebefaktor Normalkrankenhaus	1,0	1,0	1,1	1,2	1,3
	Hebefaktor Universitätsklinika	1,2	1,2	1,3	1,4	1,6

Pre-Check-Up

Die folgende Checkliste hilft Ihnen einen Überblick über die wesentlichen geforderten dokumentieren Informationen zu erhalten. Bitte beachten Sie, dass es sich um mindestens geforderte Referenzdokumente handelt und in der Regel deutlich mehr dokumentierte Informationen vorgehalten werden müssen.

2.1	Organisation der Informationssicherheit	☐
2.1.1	Geschäftsführung/Leitung	☐
2.1.2	Manager Informationssicherheit (ISO, CISO, IT-SiBe)	☐
2.1.3	Prozess-/Anwendungsverantwortlicher	☐
3	Meldepflichten nach §8b (4) BSI-Gesetz	☐
4	Fortführungsmanagement für kDL	☐
5	Asset Management	☐
6	Robuste/Resilente Architektur	☐
7	Physische Sicherheit	☐
8	Personelle und organisatorische Sicherheit	☐
9	Vorfallerkennung und Behandlung	☐
10	Überprüfung im laufenden Betrieb	☐
11	Externe Informationsversorgung und Unterstützung	☐
12	Lieferanten, Dienstleister und Dritte	☐
13	Technische Informationssicherheit	☐
13.1	Netz- und Systemmanagement (Netztrennung und Segmentierung)	☐
13.2	Absicherung Fernzugriff	☐
13.3	Härtung und sichere Basiskonfiguration der Systeme und Anwendungen	☐
13.4	Schutz vor Schadsoftware	☐
13.5	Intrusion Detection/Prevention	☐
13.6	Identitäs- und Rechtemanagement	☐
13.7	Sichere Authentisierung	☐
13.8	Kryptographische Absicherung (data in rest, data in motion)	☐
13.9	Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit (ggf. BYOD)	☐
13.10	Datensicherung, Datenwiederherstellung und Archivierung	☐
13.11	ordnungsgemäße IT-Administration	☐
13.12	Patch- und Änderungsmanagement	☐
13.13	Beschaffungsprozesse	☐
13.14	Protokollierung	☐
13.15	Umgang mit Datenträgern, Austausch von Datenträgern	☐
13.16	Sicheres Löschen und Entsorgen von Datenträgern	☐
13.17	Softwaretests und Freigaben	☐
13.18	Datenschutz	☐

KONTAKT



Zum Nollenberg 16
66780 Rehlingen-Siersburg
www.mszert.de

Ihre Ansprechpartner

Wirt.-Ing. Thomas Welsch
Leiter der Zertifizierungsstelle

Dipl.-Ing. Stefan Oehm
Geschäftsführung

Telefon: +49 (0)6833 900 895-0

Telefax: +49 (0)6833 900 895-19

E-Mail: mszert@mszert.de