DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

30.06.2017

IT-Sicherheitsgesetz: Schutz Kritischer Infrastrukturen
- 1. Änderungsverordnung zur BSI-KritisV („Korb 2“)

Das Bundesministerium des Innern hat den vom Bundeskabinett am 31.5.2017 verabschiedeten Referentenentwurf einer 1. Änderungsverordnung zur BSI-Kritisverordnung veröffentlicht. Die Verordnung enthält u. a. Kriterien zur Identifizierung von Krankenhäusern, die als kritische Infrastrukturen i. S. d. § 2 Abs. 10 BSI-Gesetz gelten. Krankenhäuser, die jährlich mindestens 30.000 vollstationäre Fälle/Jahr an einem Standort i. S. d. Landeskrankenhausplanung behandeln, haben künftig eine Kontaktstelle für das Bundesamt für Sicherheit in der Informationstechnik (BSI) einzurichten, dem BSI kritische Sicherheitsvorfälle zu melden und alle zwei Jahre geeignete Maßnahmen für das Aufrechterhalten der Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme nachzuweisen.

Am 29.6.2017 wurde der vom Bundeskabinett am 31.5.2017 gebilligte Referentenentwurf einer 1. Änderungsverordnung zur BSI-Kritisverordnung im Bundesanzeiger veröffentlicht. Die Änderungsverordnung tritt damit am heutigen Tag, dem 30.6.2017, in Kraft. Sie ergänzt die bisherigen Vorgaben zur Identifizierung kritischer Infrastrukturen um die notwendigen Anlagenkategorien, Bemessungskriterien und Schwellenwerte in den Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr.

Gegenüber dem am 3.4.2017 übermittelten Beratungsstand zur Verordnung sind für die Branche „Medizinische Versorgung“ keine weiteren Änderungen vorgenommen worden, neu ist jedoch die Aufnahme identifizierender Kriterien für den Bereich der gesetzlichen Krankenversicherung.

Krankenhäuser gelten ab Inkrafttreten der Verordnung am **30.6.2017** als kritische Infrastruktur i. S. d. § 2 Abs. 10 BSI-Gesetz, wenn sie im Jahr 2016 den festgelegten Schwellenwert von 30.000 vollstationären Behandlungsfällen pro Jahr überschritten haben. Die Betrachtung erfolgt dabei je Standort im Sinne der Landeskrankenhausplanung. Für die Folgejahre erfolgt die Feststellung einer Schwellwertüberschreitung jeweils am 31.3. für das Vorjahr.

Aus Sicht der Deutschen Krankenhausgesellschaft sollte das Ziel der Verbesserung der IT-Sicherheit kritischer Infrastrukturen von **allen** Krankenhäusern in Deutschland nachhaltig verfolgt werden. Die Auswirkungen bei Störungen oder Ausfall der informationstechnischen Systeme mit Blick auf die hohe Durchdringung des

Klinikalltags können gravierende Folgen für das Krankenhaus, den Betreiber und nicht zuletzt die zu versorgenden Patienten haben.

Der Umfang möglicher prozessualer und finanzieller Auswirkungen für Krankenhäuser, die künftig den Anforderungen des BSI-Gesetzes hinsichtlich des Schutzes ihrer informationstechnischen Systeme unterfallen, wird schon heute als erheblich eingeschätzt. Dabei ist die konkrete Ausgestaltung entsprechender Maßnahmen und Nachweise, die auch den Stand der Technik berücksichtigen sollen, heute noch nicht klar umrissen. Auch hinsichtlich der Ausgestaltung der Meldeprozesse besteht noch Klärungsbedarf, der jedoch nicht Gegenstand der Änderungsverordnung ist, da diese lediglich identifizierende Kriterien beschreibt.

Im Folgenden werden die Anforderungen an Betreiber kritischer Infrastrukturen dargestellt, soweit diese heute schon als gesichert gelten können.

Identifizierung kritischer Infrastrukturen

Mit dem IT-Sicherheitsgesetz wurde bereits 2015 der legislative Rahmen zum Schutz kritischer Infrastrukturen in Deutschland geschaffen. Ziel der Bundesregierung war dabei die Vermeidung des Ausfalls oder der Beeinträchtigung von Einrichtungen („Anlagen“), die wesentlich für das Allgemeinwohl in Deutschland sind. Die Identifizierung kritischer Infrastrukturen folgt einem methodischen Ansatz, der – ausgehend von der Definition abstrakter **Anlagenkategorien** – konkrete „Anlagen“ innerhalb jeder Branche der Sektoren des sog. Umsetzungsplans „kritische Infrastrukturen“ (UP KRITIS) beschreibt. Branchenspezifisch werden diejenigen „kritischen Dienstleistungen“ und Prozesse identifiziert, die für die Funktionsfähigkeit der Anlagen als maßgeblich angesehen werden können. Zur Quantifizierung wurde mit der Festlegung von 500.000 betroffenen Personen ein „Regelschwellenwert“ definiert, der diesem Ansatz Rechnung trägt. Je Branche wurden **Bemessungskriterien** identifiziert, welche die kritische Dienstleistung charakterisieren. Die Verordnung definiert zu diesen Bemessungskriterien **Schwellenwerte**, die dem Betreiber einer potenziell kritischen Infrastruktur die Identifizierung ermöglicht.

Festlegungen für den Sektor Gesundheitsversorgung (betroffene Krankenhäuser)

Im Sektor Gesundheitsversorgung des UP KRITIS wurde in der für Krankenhäuser maßgeblichen Branche „Medizinische Versorgung“ ausschließlich die **stationäre Krankenversorgung** als sog. „kritische Dienstleistung“ identifiziert. Diese wird bei Aufnahme, Diagnose, Therapie, Unterbringung/Pflege und Entlassung erbracht. Als „Anlage“ gelten „**Standort oder Betriebsstätten** eines nach § 108 SGB V zugelassenen Krankenhauses, die für die Erbringung stationärer Versorgungsleistungen notwendig sind.“ Als Bemessungskriterium wurde die **Anzahl vollstationärer Krankenhausbehandlungen** festgelegt. Ein Krankenhaus ist dann als kritische Infrastruktur gemäß BSI-Gesetz einzustufen, wenn an diesem planungsrechtlich ausgewiesenen Standort mehr als **30.000 vollstationäre Behandlungsfälle pro Jahr** erbracht werden.

Der jahresbezogenen Betrachtung folgend kann es bei Krankenhäusern mit Fallzahlschwankungen zu jährlich wechselnden Einstufungen kommen. Die Identifizierung erfolgt dabei grundsätzlich nicht als Verwaltungsakt des Bundesamtes

für Sicherheit in der Informationstechnik (BSI) sondern durch den Betreiber entlang der Kriterien der Verordnung. Es ist jedoch davon auszugehen, dass seitens des BSI eine Evaluierung der Meldungen erfolgen wird. Die hierzu maßgeblichen Kennzahlen sind i. d. R. auf Basis der öffentlich zugänglichen Qualitätsberichte der Krankenhäuser frei verfügbar.

Verpflichtungen für Betreiber kritischer Infrastrukturen

Die Verpflichtungen für Betreiber kritischer Infrastrukturen folgen aus § 8a und 8b BSI-Gesetz. Die abstrakt definierten Anforderungen müssen im Weiteren noch konkret ausgestaltet werden.

Einrichtung einer Kontaktstelle für das BSI

Betreiber von Krankenhäusern, die als kritische Infrastrukturen gelten, haben dem BSI **spätestens 6 Monate** nach Inkrafttreten der 1. Änderungsverordnung (30.12.2017) gemäß § 8b Abs. 3 BSIG eine Kontaktstelle zu benennen, die zur Krisenfrüherkennung, Krisenreaktion und -bewältigung sowie zu Koordinierungszwecken jederzeit erreichbar sein muss. Dabei ist zu beachten, dass mit dem Zeitpunkt der Benennung einer Kontaktstelle die nachfolgend dargestellten Meldepflichten entstehen. Das BSI informiert kritische Infrastrukturen über die Kontaktstelle über aktuelle Warnmeldungen oder Hinweise, die sich aus dem Lagebild ergeben und bittet um frühzeitige Benennung der Kontaktstelle, um einen „Meldestau“ am Jahresende zu vermeiden.

Meldepflichten

Mit der Benennung einer Kontaktstelle entsteht gemäß § 8b Abs. 4 BSIG auch die Verpflichtung zur Meldung von „erheblichen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit“ der eingesetzten informationstechnischen Systeme, Komponenten und Prozesse, wenn diese den Ausfall oder die Beeinträchtigung der Funktionsfähigkeit der betriebenen kritischen Infrastruktur zur Folge hatten oder hätten haben können. Dabei unterscheidet das BSI grundsätzlich zwischen „gewöhnlichen“ und „außergewöhnlichen“ IT-Störungen. Meldepflichtig sind grundsätzlich nur außergewöhnliche Störungen, die zu einem Ausfall oder der Beeinträchtigung der kritischen Dienstleistung hätten führen können (pseudonymisierte Meldung) oder geführt haben (Meldung muss namentlich erfolgen).

Eine Meldung muss unverzüglich (ohne schuldhaftes Zögern) erfolgen; dabei kann zwischen einer „Erstmeldung“, der ggf. noch wesentliche Informationen fehlen, und einer „Abschlussmeldung“ unterschieden werden. Das BSI formuliert hier den Grundsatz „Schnelligkeit vor Vollständigkeit“ für die Erstmeldung. Wann eine Beeinträchtigung der kritischen Dienstleistung vorliegt, ist dabei nicht je Sektor bzw. Branche festgelegt. Die Geschäftsstelle wird sich im Weiteren für eine branchenspezifische Konkretisierung dieser Kriterien einsetzen, um Meldefehler, die ggf. auch als Ordnungswidrigkeit geahndet werden können, zu vermeiden. Das BSI fasst die Kriterien für das Melden einer IT-Störung in der in Abb. 1 wiedergegeben Grafik zusammen:

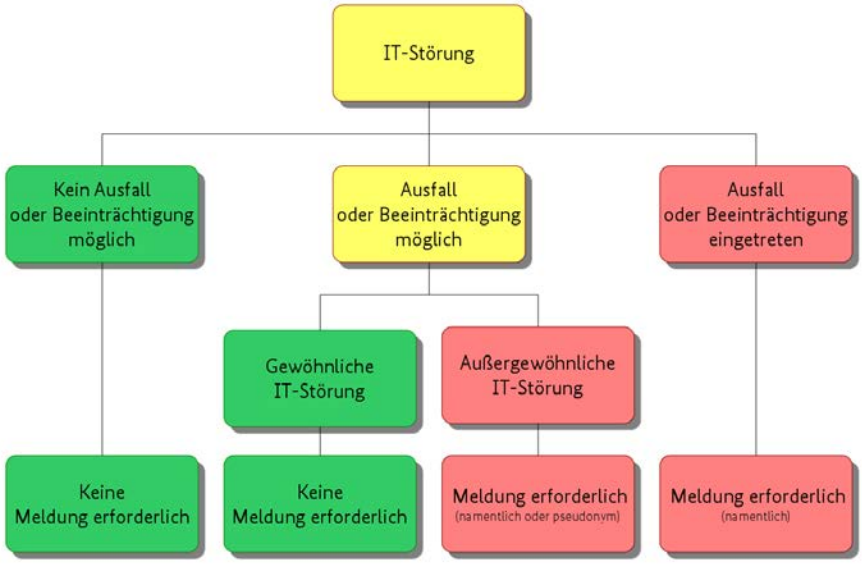

Abbildung 1 Meldekriterien für IT-Störungen (Quelle: Bundesamt für Sicherheit in der Informationstechnik)

Um Krankenhäusern im Falle einer Störung oder eines Vorfalls die Informationssicherheit betreffend einen Überblick über notwendige Meldepflichten, -fristen und ggf. Ansprechpartner zu geben, erarbeitet die Geschäftsstelle derzeit eine Übersicht, die neben den Anforderungen des BSI-Gesetzes voraussichtlich auch datenschutzrechtliche Anforderungen aufgreifen sowie Ansprechpartner im Falle eines Angriffs auf die informationstechnischen Systeme des Krankenhauses (z. B. „Ransom-Ware“) bei den zuständigen Behörden auflisten wird. Hierzu wird die Geschäftsstelle gesondert informieren.

Nachweispflichten („Branchenspezifischer Sicherheitsstandard“)

Überschreitet ein Krankenhaus den Schwellenwert für zwei Jahre in Folge, hat es gemäß § 8a Abs. 1 BSIG angemessene organisatorische und technische Vorkehrungen und Maßnahmen zum Erreichen der im BSIG definierten Schutzziele (Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität) zu treffen und dies nach Abs. 4 alle zwei Jahre geeignet nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Dabei können auch sogenannte „branchenspezifische Sicherheitsstandards“ (B3S) zum Nachweis herangezogen werden. Diese können von Betreibern oder Branchenverbänden selbst erarbeitet und dem BSI zur Eignungsprüfung vorgelegt werden. Dabei ist schon heute absehbar, dass die Umsetzung eines Informationssicherheits-Managementsystems (ISMS) für diejenigen Prozesse notwendig wird, die für die Funktionsfähigkeit der kritischen Infrastruktur benötigt werden.

Der Umfang der für die Etablierung eines ISMS umzusetzenden Maßnahmen kann heute noch nicht realistisch eingeschätzt werden und wird maßgeblich davon abhängen, welche Prozesse und Systeme zur Aufrechterhaltung der kritischen Dienstleistung im einzelnen Krankenhaus vonnöten sind. Trotz immer weiter zunehmender Digitalisierung auch im Gesundheitswesen gestaltet sich der Grad der IT-Durchdringung in den Krankenhäusern sehr heterogen. Die Geschäftsstelle bringt sich in den Umsetzungsprozess der Nachweispflichten auf verschiedenen Ebenen ein, sei

es bei der Erarbeitung geeigneter Sicherheitsstandards, der Diskussion zum „Stand der Technik“ oder der Frage der Verfügbarkeit der notwendigen Prüfungskompetenz.

Zeitlicher Rahmen der Umsetzung

Die Prüfung auf Überschreiten des Schwellenwertes erfolgt zum **31.3.** eines jeden Jahres für die vollstationären Fallzahlen des Vorjahres. Erreicht ein Krankenhaus („Anlage“) den Schwellenwert, ist es **ab dem 1.4.** desselben Jahres als kritische Infrastruktur zu betrachten. Es entsteht damit sofort die Pflicht zur Meldung einer Kontaktstelle sowie zur Meldung sicherheitsrelevanter Vorfälle an das BSI. Unterschreitet ein Krankenhaus, das im Vorjahr als kritische Infrastruktur galt, den Schwellenwert bei der Prüfung am 31.3., verliert es diesen Status am Folgetag. Damit entfallen sowohl Melde- als auch Nachweispflichten gemäß BSI-Gesetz. Es wird jedoch empfohlen, die umgesetzten Maßnahmen zur Verbesserung der Informationssicherheit aufrecht zu erhalten.

Für 2017 erfolgt die Prüfung auf Überschreiten des Schwellenwertes anhand der Fallzahlen des Jahres 2016 mit dem Tag des Inkrafttretens der Änderungsverordnung am 30.6.2017. Krankenhäuser, die den Schwellenwert in 2016 überschritten haben, gelten dann **ab diesem Tag** als kritische Infrastrukturen. Die Pflicht zur Meldung einer Kontaktstelle entsteht in 2017 einmalig mit einer Umsetzungsfrist von höchstens 6 Monaten ab dem Datum des Inkrafttretens.

Mit der Meldung der Kontaktstelle entsteht **gleichzeitig** die Pflicht zur Meldung sicherheitsrelevanter Vorfälle an das BSI, spätestens jedoch 6 Monate nach Inkrafttreten der Änderungsverordnung zur BSI-KritisV. Die nachfolgende Grafik verdeutlicht den zeitlichen Rahmen der Umsetzung noch einmal:

Abbildung 2 Zeitplan zur Umsetzung der BSI-KritisVO

Hinweis zum „Anlagenbegriff“

„Anlage“ sind Krankenhäuser bzw. Standorte im Sinne der Landeskrankenhausplanung, „*welche die zugelassenen Krankenhäuser, teilweise differenziert nach Betriebsstätten oder Standorten, ausweist. Dabei sind räumlich getrennte Standorte oder Betriebsstätten eines Krankenhauses als eine Anlage anzusehen, wenn sie aus planungsrechtlicher Sicht, etwa aus organisatorischen, technischen, medizinischen oder sicherheitsbezogenen Aspekten als Einheit betrachtet werden.*“

Der Verordnungsgeber trägt damit der föderal organisierten Krankenhausplanung Rechnung. Aufgrund heterogener Differenzierungsgrade und Aggregationsebenen zum „Standortbegriff“ auf Landesebene wird sich die DKG im Rahmen der Vereinbarungen zu § 2a KHG bzw. § 293 Abs. 6 SGB V (Standortverzeichnis für Krankenhäuser) auch für die Berücksichtigung der Anforderungen des IT-Sicherheitsgesetzes einsetzen, um perspektivisch eine einheitliche Grundlage für die Definition von Standorten auch im Kontext kritischer Infrastrukturen zu schaffen.

Vorbereitende Maßnahmen

Krankenhäusern, die sich als kritische Infrastruktur identifizieren, wird zunächst geraten, die Etablierung einer Kontaktstelle sowie die Vorbereitung der notwendigen Meldewege umzusetzen. Darüber hinaus sollte eine Erhebung des IST-Zustands der eingesetzten informationstechnischen Systeme, Prozesse und Dienstleistungen erfolgen, soweit dies nicht schon erfolgt ist. Über den Fortgang der Beratungen zu einem branchenspezifischen Sicherheitsstandard wird die Geschäftsstelle mit Blick auf die zeitlich knapp bemessene Umsetzungsfrist (Juni 2019) für entsprechende Nachweise möglichst frühzeitig informieren.

Finanzierung möglicher Aufwände

Krankenhäuser nehmen schon heute ihre Verantwortung für Patientensicherheit wahr, die aufgrund der wachsenden Digitalisierung im Gesundheitswesen in Teilen auch von der Informationstechnik im Krankenhaus abhängt. Dabei wirkt sich die mangelnde Investitionsbereitschaft der Bundesländer, besonders bei IT-Investitionen, hemmend aus. Ein Umsetzen von Maßnahmen auf dem „Stand der Technik“, wie ihn das BSI-Gesetz fordert, wird voraussichtlich sowohl bei den Personalkosten, den Betriebskosten als auch notwendigen Investitionsmitteln erheblichen Mehrbedarf erzeugen. Die Geschäftsstelle sieht hier den Gesetzgeber in der Pflicht, sich der Herausforderung der Finanzierung entstehender Aufwände für die Umsetzung von Maßnahmen zur Verbesserung der IT-Sicherheit in Krankenhäusern zu stellen und wird sich für eine adäquate Refinanzierung entstehender Aufwände einsetzen. Die Erhebung der bei den Krankenhäusern entstehenden Aufwände wird dabei maßgeblich für das Ergebnis dieser Verhandlungen sein.