DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

03.04.2017

IT-Sicherheitsgesetz: Schutz Kritischer Infrastrukturen
1. Änderungsverordnung zur BSI-KritisV/Stellungnahme der DKG

Die DKG hat im Rahmen einer Verbändeanhörung am 28.3.2017 ihre Stellungnahme zum Referentenentwurf einer Änderungsverordnung zur BSI-Kritisverordnung (BSI-KritisV - vgl. Rundschreiben vom 24.2.2017) eingebracht. Die Veröffentlichung der Verordnung wird für Anfang Mai 2017 erwartet.

Der Entwurf enthält u. a. Kriterien zur Einstufung von Krankenhäusern als künftige kritische Infrastrukturen nach § 2 Abs. 10 BSI-Gesetz: Krankenhäuser, die jährlich mindestens 30.000 vollstationäre Fälle an einem Standort i. S. d. Landeskrankenhausplanung behandeln, müssen danach eine Kontaktstelle für das Bundesamt für Sicherheit in der Informationstechnik (BSI) einrichten, dem BSI kritische Sicherheitsvorfälle melden und alle zwei Jahre geeignete Maßnahmen für das Aufrechterhalten der Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme nachweisen.

Der Referentenentwurf einer 1. Änderungsverordnung zur BSI-Kritisverordnung (BSI-KritisV) ergänzt die bereits existierenden Vorgaben zur Bestimmung kritischer Infrastrukturen um Definitionen zu Anlagenkategorien, Bemessungskriterien und Schwellenwerte in den Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr („Korb 2“).

Die Geschäftsstelle hat zu dem Verordnungsentwurf eine Stellungnahme gefertigt und fordert darin u. a. Klarstellungen zu Krankenhausapotheken sowie Laboren an Krankenhäusern („interne Dienstleistungen“). Weiter wurde angeregt, bei Definition des „Anlagenbegriffs“ künftig auf das erwartete Standortverzeichnis für Krankenhäuser nach § 293 Abs. 6 SGB V abzustellen. Das für die Änderungsverordnung zuständige Bundesministerium des Innern hat bereits im Rahmen der Verbändeanhörung signalisiert, dass die erhobenen Einwände aufgegriffen und in Gänze berücksichtigt werden.

Die möglichen organisatorischen und finanziellen Auswirkungen für Krankenhäuser, die künftig den Anforderungen des BSI-Gesetzes (BSIG) zum Schutz ihrer informationstechnischen Systeme unterfallen, werden schon heute als erheblich eingeschätzt. Dabei ist die konkrete Ausgestaltung der am „Stand der Technik“ zu orientierenden Maßnahmen und Nachweise noch nicht klar umrissen. Auch zu den Meldeprozessen besteht noch Klärungsbedarf, der jedoch nicht im Rahmen der Änderungsverordnung zu befriedigen ist, da die Verordnung lediglich identifizierende Kriterien beschreibt.

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

Einstufung als kritische Infrastruktur

Mit dem IT-Sicherheitsgesetz wurde bereits 2015 der legislative Rahmen zum Schutz kritischer Infrastrukturen in Deutschland geschaffen. Ziel der Bundesregierung ist dabei die Vermeidung eines Ausfalls oder einer Beeinträchtigung von Einrichtungen („Anlagen“), die wesentlich für das Allgemeinwohl in Deutschland sind. Diesem gesamtgesellschaftlichen Ansatz folgend ist eine Infrastruktur dann als kritisch anzusehen, wenn mehr als 500.000 Personen („Regelschwellenwert“) von deren Ausfall oder einer Beeinträchtigung betroffen sein können.

Die Einstufung als kritische Infrastruktur folgt einem methodischen Ansatz, der – ausgehend von abstrakten Anlagenkategorien – konkrete „Anlagen“ innerhalb der verschiedenen Sektoren des sogenannten Umsetzungsplans „Kritische Infrastrukturen“ (UP KRITIS) beschreibt. Es werden branchenspezifisch alle „kritischen Dienstleistungen“ und Prozesse identifiziert, die für die Funktionsfähigkeit der Anlagen maßgeblich sind. Der Fokus liegt dabei auf der Relevanz der einzelnen Anlage für das Allgemeinwohl. Mit der Festlegung von 500.000 betroffenen Personen ist ein „Regelschwellenwert“ definiert, der diesem Ansatz Rechnung trägt. Für jede Branche wurden Bemessungskriterien definiert, welche die kritische Dienstleistung charakterisieren. Die Verordnung regelt zu diesen Bemessungskriterien Schwellenwerte, die dem Betreiber einer potenziell kritischen Infrastruktur die Einordnung ermöglichen.

Festlegungen für den Sektor Gesundheitsversorgung (betroffene Krankenhäuser)

Für den Sektor Gesundheitsversorgung ist die **stationäre Krankenversorgung** als „kritische Dienstleistung“ beschrieben. Diese wird in den Bereichen 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 dient die **Anzahl vollstationärer Krankenhausbehandlungen.** Ein Krankenhaus als „Anlage“ i. S. d. Verordnung ist dann als kritische Infrastruktur gemäß BSI-Gesetz einzustufen, wenn am planungsrechtlich ausgewiesenen Standort mehr als 3**0.000 vollstationäre Behandlungsfälle pro Jahr** erbracht werden.

Dieser jahresbezogenen Betrachtung folgend kann es insbesondere bei Krankenhäusern mit nahe dem Schwellenwert schwankenden Fallzahlen durchaus zu jährlich wechselnden Einstufungen kommen. Die Einstufung erfolgt dabei grundsätzlich nicht durch Verwaltungsakt des BSI sondern durch den Betreiber des Krankenhauses nach Maßgabe der genannten Kriterien. Es ist aber davon auszugehen, dass das BSI eine Evaluierung der Meldungen vornehmen wird, zumal die hierfür maßgeblichen Kennzahlen in den öffentlich zugänglichen Qualitätsberichten der Krankenhäuser frei verfügbar sind.

Verpflichtungen für Betreiber kritischer Infrastrukturen

Die §§ 8a und 8b BSIG beschreiben die Verpflichtungen der Betreiber kritischer Infrastrukturen. Die dort noch abstrakt gehaltenen Anforderungen müssen noch konkret ausgestaltet werden.

Einrichtung einer Kontaktstelle für das BSI

Betreiber von als kritische Infrastruktur eingestuften Krankenhäusern haben dem BSI **spätestens sechs Monate** nach Inkrafttreten der 1. Änderungsverordnung eine Kontaktstelle zu benennen, die jederzeit erreichbar sein muss zum Zwecke der Krisenfrüherkennung, Krisenreaktion und -bewältigung sowie für Koordinierungszwecke.

Meldepflichten

Ab dem Zeitpunkt der Benennung der Kontaktstelle entsteht für den Betreiber 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 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 hat unverzüglich (ohne schuldhaftes Zögern) zu erfolgen; dabei kann zwischen einer „Erstmeldung“, der ggf. noch wesentliche Informationen fehlen, und einer „Abschlussmeldung“ unterschieden werden. Für die Erstmeldung gilt der Grundsatz „Schnelligkeit vor Vollständigkeit“, um schnelle Reaktionen zu ermöglichen, Die Bewertung, ab wann eine Beeinträchtigung der kritischen Dienstleistung vorliegt, ist dabei nicht pro Sektor bzw. Branche festgelegt. Die Geschäftsstelle der DKG wird sich für eine Klarstellung und Konkretisierung dieser Kriterien einsetzen, um das bei Verstößen drohende Risiko einer Ahndung als Ordnungswidrigkeit zu minimieren. Das BSI fasst die Kriterien für die Meldung einer IT-Störung in der als Abb. 1 wiedergegeben Grafik zusammen.

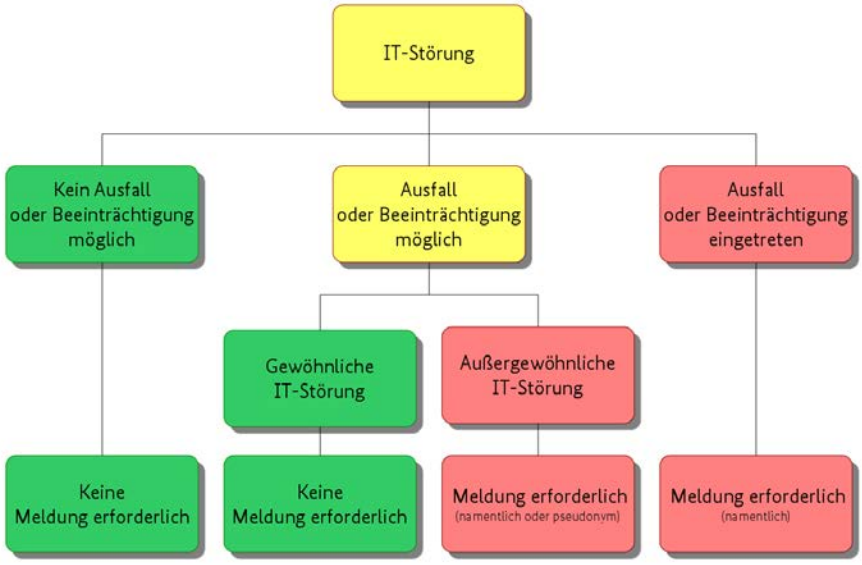

Abbildung 1 Meldekriterien für IT-Störungen (Quelle: Bundesamt für Sicherheit in der Informationstechnik)

Nachweispflichten („Branchenspezifischer Sicherheitsstandard“)

Überschreitet ein Krankenhaus den Schwellenwert für zwei Jahre in Folge, hat es gemäß § 8a BSIG angemessene organisatorische und technische Vorkehrungen und Maßnahmen zum Erreichen der im BSIG definierten Schutzziele (Verfügbarkeit, Vertraulichkeit, Integrität, Authentizität) zu treffen und diese alle zwei Jahre geeignet nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Dabei können auch sog. „branchenspezifische Sicherheitsstandards“ (B3S) 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 sogenannten Informationssicherheits-Managementsystems (ISMS) für die 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 notwendig sind.

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 einer Verfügbarkeit der notwendigen Prüfungskompetenz.

Zeitlicher Rahmen der Umsetzung

Die Prüfung des Überschreitens des Schwellenwertes erfolgt jeweils zum **31.3.** eines jeden Jahres anhand der vollstationären Fallzahlen des Vorjahres. Erreicht ein Krankenhaus („Anlage“) den Schwellenwert, ist es **ab dem 1.4.** als kritische Infrastruktur i. S. d. Verordnung zu betrachten. Es entsteht damit die **sofortige** 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 Folgeprüfung am 31.3., verliert es diesen Status auch unmittelbar am Folgetag. Damit entfallen die aus der Eigenschaft als kritische Infrastruktur resultierenden Pflichten.

Für das Jahr 2017 erfolgt die Prüfung auf Überschreiten des Schwellenwertes anhand der Fallzahlen des Jahres 2016 mit dem Tag des Inkrafttretens der Änderungsverordnung (erwartet für Anfang Mai 2017). Krankenhäuser, die den Schwellenwert im Jahr 2016 überschritten haben, gelten dann **ab diesem Tag** als kritische Infrastrukturen. Die Pflicht zur Meldung einer Kontaktstelle entsteht für 2017 als Ausnahmeregelung mit einer Umsetzungsfrist von höchstens sechs Monaten ab dem Datum des Inkrafttretens.

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

Abbildung 2 voraussichtlicher Zeitplan zur Umsetzung

Hinweis zum „Anlagenbegriff“

Als „Anlage“ im Sinne der Verordnung sind nach der Begründung des Entwurfs Krankenhäuser bzw. Standorte im Sinne der Landeskrankenhausplanung zu verstehen, „*welche die zugelassenen Krankenhäuser, teilweise differenziert nach Betriebsstätten oder Standorten, ausweisen. 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 mit dieser Regelung dem Umstand der föderal organisierten Krankenhausplanung Rechnung. Aufgrund heterogener Differenzierungsgrade und Aggregationsebenen zum „Standortbegriff“ auf Landesebene wird sich die DKG bei der Vereinbarungen zu § 2a KHG bzw. § 293 Abs. 6 SGB V (Standortverzeichnis für Krankenhäuser) auch für die Berücksichtigung der Anforderungen aufgrund des IT-Sicherheitsgesetzes einsetzen, um perspektivisch eine einheitliche Grundlage für die Definition von Standorten auch im Kontext kritischer Infrastrukturen zu schaffen.

Finanzierung möglicher Aufwände

Krankenhäuser nehmen schon heute ihre Verantwortung für Patientensicherheit wahr, die in wachsenden Anteilen auch von der Informationstechnik im Krankenhaus abhängt. Dabei wirkt sich die mangelnde Investitionsbereitschaft der Bundesländer, besonders bei IT-Investitionen, hemmend aus. Eine Umsetzung von Maßnahmen auf dem „Stand der Technik“, wie ihn das BSI-Gesetz fordert, wird voraussichtlich sowohl bei den Personalkosten, den Betriebskosten also 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 Refinanzierung entstehender Aufwände einsetzen.