

Stellungnahme

der Deutschen Krankenhausgesellschaft

zum

Referentenentwurf

einer

**Ersten Verordnung zur Änderung der
BSI-Kritisverordnung**

vom 15. März 2017

Inhaltsverzeichnis

Allgemeiner Teil	3
Besonderer Teil	5
Zu Artikel 1 Nr. 2.....	5
Zu Artikel 1 Nr. 8 a).....	6
Zu Artikel 1 Nr. 8 h).....	7
Zu Artikel 1 Nr. 8 k).....	8

Allgemeiner Teil

Mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 25. Juli 2015 hat der Gesetzgeber die Grundlage für eine Verbesserung der IT-Sicherheit kritischer Infrastrukturen geschaffen. Die Methodik zur Identifizierung kritischer Infrastrukturen wurde in der BSI-Kritisverordnung vom 3. Mai 2016 zunächst für die Sektoren Energie, Wasser, Informationstechnik und Telekommunikation sowie Ernährung festgelegt. Die vorliegende Änderungsverordnung ergänzt die BSI-Kritisverordnung nun um Festlegungen zu den noch ausstehenden Sektoren Transport und Verkehr, Gesundheit sowie Finanz- und Versicherungswesen, insbesondere zur Identifizierung der dortigen kritischen Infrastrukturen.

Die DKG begrüßt ausdrücklich den gewählten kooperativen Ansatz des UP KRITIS, schon im Vorfeld der Verordnung die betroffenen Branchen und Verbände frühzeitig einzubeziehen. Der Verordnungsentwurf greift viele der hieraus gewonnenen Erkenntnisse zur Identifizierung kritischer Infrastrukturen auf.

Die medizinische Versorgung wird wegen ihrer besonderen Bedeutung für die Funktionsfähigkeit des staatlichen Gemeinwesens als kritische Dienstleistung angesehen. Dabei bilden die Krankenhäuser das Rückgrat der medizinischen Versorgung. Der Schutz ihrer informationstechnischen Systeme wird im Rahmen des KRITIS-Umsetzungsprozesses – im Gegensatz zur vertragsärztlichen Versorgung – besonders betrachtet.

Die Identifizierung der künftig als Kritische Infrastruktur geltenden Krankenhäuser erfolgt durch Definition eines „Anlagenbegriffs“, der im Wesentlichen auf den „Krankenhaus-Standort“ abstellt, insbesondere den Standort „im Sinne der Landeskrankenhausplanung“. Die DKG gibt zu bedenken, dass die bis Mitte 2017 gem. § 2a Abs. 1 KHG zu vereinbarende bundeseinheitliche Standortdefinition **künftig eine weniger föderal zersplitterte und einheitlichere Grundlage** für den Anlagenbegriff bereitstellen könnte.

Als „Bemessungskriterium“ für die Kritikalität der betroffenen Anlagen wurde die **Anzahl vollstationärer Behandlungsfälle** gewählt. Der Schwellenwert (30.000 Fälle/Jahr) soll sicherstellen, dass nur Einrichtungen einer bestimmten Größe und Versorgungsrelevanz unter den Anwendungsbereich der Verordnung fallen. Für diese Krankenhäuser sind geeignete Maßnahmen zur Sicherung der für die Funktionsfähigkeit der Kritischen Infrastruktur maßgeblichen informationstechnischen Systeme einzuführen. Darüber hinaus sind dem Bundesamt für Sicherheit in der Informationstechnik (BSI) erhebliche IT-Sicherheits-Vorfälle zu melden und es ist eine Kontaktstelle zur Entgegennahme von Informationen des BSI einzurichten.

Der Entwurf misst der Sicherheit der Patienten im Krankenhaus höchste Priorität zu. Auch für die DKG ist die Patientensicherheit die erste und grundlegende Bedingung einer erfolgreichen Krankenhausbehandlung. In den heutigen hochtechnisierten Krankenhäusern lässt sich die Sicherheit informationstechnischer Systeme nicht mehr von der Patientensicherheit trennen. Informationstechnische Systeme sind unmittelbar in den Behandlungsprozess eingebunden; sie liefern und koordinieren maßgebliche

Behandlungsdaten und schaffen damit die Grundlage eines erfolgreichen ärztlichen Handelns.

Die geforderte Stärkung des Schutzes der informationstechnischen Systeme verursacht zwingend **deutliche Mehrbelastungen** bei den Krankenhäusern im investiven Bereich und bei den Betriebskosten, deren Refinanzierungsnotwendigkeit bislang leider ignoriert wird. Der Verordnungsgeber geht von ca. 80 – 110 betroffenen Krankenhäusern in Deutschland aus. Mindestens für diese Einrichtungen werden absehbar deutliche Mehrkosten durch Investitionen in die IT-Sicherheit und im Bereich Personal entstehen. Während die Betriebskosten im Rahmen der Budgetvereinbarungen mit den Krankenkassen verhandelt werden, ist die seit Jahren bestehende Lücke bei den Investitionskosten, welche die Bundesländer verantworten, ein ernstzunehmendes Hemmnis bei der Umsetzung zusätzlicher Sicherheitsmaßnahmen in der Krankenhaus-Informationstechnik.

Die DKG bekennt sich ausdrücklich zu dem Ziel, die IT-Sicherheit möglichst in allen Krankenhäusern zu verbessern, fordert aber gleichzeitig die hierfür notwendige finanzielle Unterstützung ein, insbesondere, weil Krankenhäuser – anders als klassisch marktwirtschaftlich geprägte Sektoren – entstehende Mehrkosten gerade nicht auf die Endnutzerpreise umlegen können. Allen Krankenhäusern, die Maßnahmen zur Verbesserung der IT-Sicherheit (z. B. durch Anwendung branchenspezifischer Sicherheitsstandards) umsetzen, muss eine gesicherte Refinanzierung der hierfür erforderlichen Aufwände gewährleistet werden – unabhängig davon, ob diese Krankenhäuser kritische Infrastrukturen im Sinne dieser Verordnung sind, oder nicht. Dies hebt das Niveau der IT-Sicherheit im gesamten Krankenhaussektor und nicht nur bei den explizit benannten kritischen Infrastrukturen.

Die DKG wird sich aktiv in den Prozess der Konkretisierung der umzusetzenden Maßnahmen zur Verbesserung der Sicherheit informationstechnischer Systeme einbringen und das im Verbandsbereich verfügbare Expertenwissen hierzu beisteuern. Zu betonen ist aber auch, dass dem Grundsatz der Verhältnismäßigkeit sowie der bereits im IT-Sicherheitsgesetz angelegten Wirtschaftlichkeitsbetrachtung ebenfalls Rechnung getragen werden muss.

Aus Sicht der DKG ist die Ausgestaltung der Meldeverpflichtungen noch nicht hinreichend belastbar; hier wird sich zeigen, ob die getroffenen Annahmen (sieben meldepflichtige Vorfälle je Anlage und Jahr) in der Praxis tatsächlich zutreffen.

Besonderer Teil

Zu Artikel 1 Nr. 2

Beabsichtigte Neuregelung

Es werden die nach Maßgabe des § 10 Absatz 1 Satz 1 BSI-Gesetz im Sektor Gesundheit als kritisch anzusehenden Dienstleistungen definiert.

Stellungnahme

Die gewählte Definition der kritischen Dienstleistungen greift die Ansätze der vorangegangenen Sektorstudie des BSI auf. Für Krankenhäuser ist primär die Dienstleistung „medizinische Versorgung“ relevant.

Die daneben definierte Dienstleistung „Versorgung mit Medizinprodukten, die Verbrauchsgüter sind“ fokussiert auf Medizinprodukte, denen z. T. eine unmittelbar lebenserhaltende Funktion zukommt (z. B. Verbrauchsgüter zur Beatmung/Tracheostomie, parenteralen Ernährung, enteralen Ernährung, zur ableitenden Inkontinenz und zur Behandlung von Diabetes Typ I).

Krankenhäuser sind jedoch auch auf Medizinprodukte angewiesen, die nicht Verbrauchsgüter sind (sog. Gebrauchsgüter). Auch die Hersteller dieser Medizinprodukte müssen die technischen Voraussetzungen erbringen, ihre Produkte in das IT-Sicherheitsmanagement der Krankenhäuser einzugliedern (z. B. Patchmanagement).

Zu Artikel 1 Nr. 8 a)

Beabsichtigte Neuregelung

Die Neuregelung beschreibt die Anlagenkategorien und Schwellenwerte in den verschiedenen Sektoren und legt die jeweils kritische Dienstleistung fest. Für Krankenhäuser wird auf Standorte oder Betriebsstätten abgestellt, sofern diese für die Erbringung der stationären Versorgungsleistung notwendig sind.

Stellungnahme

Der gewählte Anlagenbegriff orientiert sich maßgeblich an der Krankenhausplanung und möglichen Standortdefinition der einzelnen Bundesländer. Es wird abgestellt auf einen

„Krankenhausbegriff [...] im Sinne der Landeskrankenhauspläne [...], 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.“

Diese Definition könnte wegen der in den verschiedenen Bundesländern sehr heterogen ausgestalteten Planungstiefe der Krankenhauspläne zu Problemen in der praktischen Auslegung und Umsetzung führen.

In dem Gesetz zur Weiterentwicklung der Versorgung und der Vergütung für psychiatrische und psychosomatische Leistungen (PsychVVG) vom 23.12.2016 wurden die DKG und der GKV-Spitzenverband beauftragt, bis zum 30.6.2017 im Benehmen mit den Ländern, der KBV/KZBV und der PKV, eine bundeseinheitliche Definition zu vereinbaren, welche die Kriterien für den Standort oder die Standorte eines Krankenhauses und dessen Ambulanzen festlegt. Die Definition soll insbesondere für Qualitätssicherung, Abrechnung, Krankenhausplanung und Krankenhausstatistik geeignet sein. Darüber hinaus wurden die Vereinbarungspartner beauftragt, bis zum 30.6.2017 ein bundesweites Verzeichnis der Standorte der nach § 108 zugelassenen Krankenhäuser und ihrer Ambulanzen zu führen und im Internet zu veröffentlichen.

Die DKG regt an, in der BSI-Kritisverordnung einen Mechanismus vorzusehen, sich bei der Festlegung der als eine „Anlage“ zu betrachtenden Krankenhausstandorte an diesem künftigen bundesweiten Verzeichnis der Krankenhäuser nach § 293 Abs. 6 SGB V zu orientieren. Sie ist bereit, die Anforderungen an den Standortbegriff im Kontext der BSI-Kritisverordnung in die Verhandlung zur Etablierung dieses bundesweiten Krankenhaus- und Standortverzeichnisses einzubringen.

Zu Artikel 1 Nr. 8 h)

Beabsichtigte Neuregelung

Es wird die Anlagenkategorie „Apotheke“ definiert.

Stellungnahme

Eine nicht unerhebliche Anzahl von Krankenhäusern verfügt über eine eigene Krankenhausapotheke, ohne dass all diese Krankenhäuser zwingend den KRITIS-relevanten Schwellenwert von 30.000 Fällen pro Jahr erreichen. Es muss sichergestellt sein, dass ein solches – den Schwellenwert unterschreitendes – Krankenhaus nicht wegen des bloßen Vorhandenseins einer Krankenhausapotheke zur kritischen Infrastruktur erklärt wird. Der Fokus muss weiterhin auf der für das Krankenhaus definierten kritischen Dienstleistung „medizinische Versorgung“ liegen und nicht auf der Dienstleistung, die ein Teilbereich (die Apotheke) des Krankenhauses erbringt.

Die DKG begrüßt, dass mit dem Verweis auf den ersten Abschnitt des Apothekengesetzes diesem Ansatz offenbar Rechnung getragen werden soll, indem die Krankenhausapotheke – die als inhärenter Bestandteil des Krankenhauses zur Sicherstellung der medizinischen Versorgung notwendig ist – ausdrücklich nicht der Dienstleistung „Versorgung mit verschreibungspflichtigen Medikamenten“ zugerechnet wird.

Allerdings sollte eher grundsätzlich klargestellt werden, dass einem Krankenhaus assoziierte „Begleitinfrastrukturen“ (z. B. Krankenhausapotheke, Labor, Rechenzentrum des Krankenhauses) nicht als eigenständiger Erbringer einer kritischen Dienstleistung anzusehen sind, sondern vielmehr als *conditio sine qua non* für die Erbringung der eigentlichen Dienstleistung des Krankenhauses, die „medizinische Versorgung“, so dass die Einstufung als kritische Infrastruktur von der Fallzahl des Krankenhauses abhängt und nicht von den Aktivitäten assoziierter „Begleitinfrastrukturen“.

Änderungsvorschlag

Aufnahme einer Klarstellung, dass Einrichtungen des Krankenhauses, die der Sicherstellung der medizinischen Versorgung dienen, nicht zur Identifizierung als kritische Infrastruktur herangezogen werden:

6. Soweit die in Teil 3 Nummer 2 - 4 aufgeführten Anlagenkategorien Bestandteil einer Anlage sind, die der in Teil 3 Nummer 1.1 genannten Anlagenkategorie zuzuordnen ist, wird für die Identifizierung der Anlage insgesamt das in Teil 3 Nummer 1.1 Spalte C genannte Bemessungskriterium sowie der in Spalte D genannte Schwellenwert herangezogen.

Zu Artikel 1 Nr. 8 k)

Beabsichtigte Neuregelung

Es wird die Anlagenkategorie „Labor“ definiert.

Stellungnahme

Analog der Feststellung zu Artikel 1 Nr. 8 lit. h) ist aus Sicht der DKG auch für Labore an Krankenhäusern festzustellen, dass diese nicht etwa den unter Buchstabe k) aufgeführten Anlagenkategorien unterfallen.