DEUTSCHE KRANKENHAUS GESELLSCHAFT

Bundesverband der Krankenhausträger in der Bundesrepublik Deutschland

Stellungnahme

der Deutschen Krankenhausgesellschaft

zum Referentenentwurf eines

Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

(IT-Sicherheitsgesetz – ITSiG)

11. November 2014

I. Allgemeiner Teil

Die DKG teilt die Einschätzung, dass mit zunehmender informationstechnischer Vernetzung der Bereiche Energie-, IT- und Transportdienstleistungen, Gesundheits- und Finanzwesen sowie Trinkwasser und Ernährung, die Verwundbarkeit des staatlichen Gemeinwesens durch gezielte Angriffe aus dem Cyberraum ansteigt und dass ein Ausfall kritischer Infrastrukturen zu einer Gefährdung der gesellschaftlichen Lebensgrundlagen der Bundesrepublik Deutschland führen kann. Umso mehr ist es Aufgabe der gerade zur Abwehr derartiger Gefahren berufenen Sicherheitsorgane, die Lebensgrundlagen des staatlichen Gemeinwesens aktiv zu schützen. Die Partner der Selbstverwaltung haben im Dialog mit dem Bundesministerium des Innern ihre Bereitschaft bekundet, die staatlichen Sicherheitsorgane bei der Erfüllung von deren Aufgaben durch Bereitstellung von branchenspezifischem Know-how zu unterstützen.

Die DKG begrüßt, dass der Begriff „kritische Infrastrukturen“ jetzt verbindlich im Gesetz definiert ist und dass die notwenige Konkretisierung durch Rechtsverordnung nach Maßgabe des Grundsatzes der Verhältnismäßigkeit unter Einbindung des spezifischen Branchenwissens vorgenommen werden soll. **Die DKG setzt voraus, dass sie in die Entwicklung von angemessenen Branchenstandards eingebunden wird.**

Problematisch und unklar bleiben aber weiterhin der **Umfang** der den Betreibern kritischer Infrastrukturen auferlegten Pflichten **sowie das Fehlen von Regelungen zur Refinanzierung** der mit zusätzlichen Investitionen in die Cybersicherheit verbundenen Kosten. Der Gesetzentwurf differenziert nicht hinreichend nach den branchenspezifisch zu bewertenden Risiken eines Ausfalls informationstechnischer Systeme und den daraus resultierenden Folgen für die Arbeitsfähigkeit der kritischen Infrastruktur. Die Funktionsfähigkeit eines Krankenhauses kann bei einem Cyberangriff auf die Krankenhaus-IT zwar beeinträchtigt werden, sie bleibt aber im Großen und Ganzen erhalten. Mögliche Abwehrmaßnahmen müssen auf die Risiken fokussiert sein, die für die Funktionsfähigkeit der Infrastruktur tatsächlich relevant sind.

Es ist weder erkennbar, welche unternehmenskritischen Bereiche besonders abzusichern sind, noch an welchen Erfolgskriterien sich die auferlegten regelmäßigen Sicherheitsaudits zu orientieren haben. Der Gesetzentwurf strebt explizit eine „Erhöhung“ der Sicherheitsstandards informationstechnischer Systeme an und bewertet das Sicherheitsniveau der gegenwärtigen Systeme als nicht hinreichend und fordert deren Anpassungen. Die hierfür erforderlichen Finanzmittel hängen stark von der Anzahl der betroffenen Einrichtungen und dem Niveau der gestellten Anforderungen ab. Angesichts der im Krankenhausbereich bekannten Defizite bei der Investitionsförderung der Länder muss sichergestellt werden, dass die erforderlichen Investitionen für eine weitere Anhebung der Sicherheitsstandards durch den Bund übernommen werden. Die kritische Situation der Investitionsfinanzierung der Krankenhäuser ist bekannt und darf nicht über zusätzliche Anforderungen des Bundes weiter verschärft werden.

Die DKG nimmt das Ziel zur Kenntnis, durch Bündelung aller über Cyberrisiken verfügbaren Informationen beim Bundesamt für die Sicherheit in der Informationstechnik (BSI) ein bedrohungsspezifisches Lagebild zu erhalten. Bislang fehlten belastbare Informationen zur Abschätzung des Bedrohungspotentials und Ausmaßes der durch Cyber-Angriffe möglichen Beeinträchtigungen und Risiken, um hieraus eine aus der Bedrohungslage objektiv ableitbare Abwehrstrategie zu entwickeln. Der Gesetzentwurf zeigt die Perspektive auf, dieses Informationsdefizit zu beseitigen. Die Zentralisierung schafft aber umgekehrt **die neue Gefahr eines single point of failure**, wenn die zur Cyberabwehr zuständigen Zentralinstanzen ihrerseits Ziel eines erfolgreichen Cyberangriffs werden. Insbesondere die zentrale Sammlung von Schwachpunkten, die automatisch bei der Übermittlung von Auditergebnissen anfallen, stellt einen Angriffspunkt dar, der die Unterwanderung der entsprechenden Organisation durch interessierte Gruppierungen lohnenswert machen könnte. Hier fehlen der DKG Aussagen zu den Maßnahmen einer Risikoabwendung.

II. Besonderer Teil

Zu Artikel 1 (Änderung des BSI-Gesetzes)

Zu Artikel 1 Nr. 1 und 2

Beabsichtigte Neuregelung

Die Neuregelung statuiert die künftige Verankerung des BSI als zentrale Stelle für die Sicherheit der Informationstechnik kritischer Infrastrukturen und macht dieses zum zentralen Ansprechpartner für Krankenhäuser.

Stellungnahme

Die DKG begrüßt die grundsätzliche Intention, alle verfügbaren Erkenntnisse zu Ursachen und Ausmaß von Bedrohungen aus dem Cyberraum zu sammeln und auch den Betreibern kritischer Infrastrukturen auf Ersuchen zur Verfügung zu stellen. Nur ein objektives Bedrohungslagebild kann als Grundlage für die Ableitung von geeigneten und erforderlichen Abwehrmaßnahmen dienen.

Mit dem Gesetzentwurf werden aber zentralistische Kontrollstrukturen beim BSI eingeführt, die über das anzustrebende Ziel deutlich hinausgehen und z.T. sogar riskant und kontraproduktiv sind. Durch die verbindlichen Meldungen von Störungen von informationstechnischen Systemen, Komponenten oder Prozessen gegenüber dem BSI wird ein zentrales Register über die informationstechnischen Schwachstellen der gesamten deutschen Volkswirtschaft geschaffen. Wer dieses Register erfolgreich angreift, besitzt alle erforderlichen Informationen für flächendeckende Angriffe auf die deutsche Volkswirtschaft.

Die Erforderlichkeit einer zentralen, unternehmendbezogenen Sammlung von Informationen beim BSI sollte nochmals grundsätzlich überdacht werden, oder es sollten Mechanismen entwickelt werden, der neu geschaffenen Bedrohungssituation zu begegnen, insbesondere mit dem Blick auf das sehr konkret gewordene Risiko der Unterwanderung auch von öffentlichen Einrichtungen.

Zu Artikel 1 Nr. 3

Beabsichtigte Neuregelung

Die Neuregelung schafft sowohl auf gesetzlicher Ebene als auch über eine Verordnungsermächtigung für das Bundesministerium des Innern die Grundlage zur Definition kritischer Infrastrukturen.

Stellungnahme

Angesichts der nicht überschaubaren Menge potentieller Ziele von Cyberangriffen war es ein Erfordernis der gesetzlichen Bestimmtheit, „kritische Infrastrukturen“ im Sinne des ITSiG näher zu definieren. Die DKG begrüßt, dass dieser Ansatz im Ge-

setz aufgenommen worden ist. Gerade der Bereich „Gesundheit“ ist durch eine Vielzahl von medizinischen Leistungserbringern unterschiedlichster Ausrichtung in Regionen mit differenzierter Versorgungsdichte geprägt, deren möglicher Ausfall nicht pauschal „erhebliche Versorgungsengpässe“ oder eine „Gefährdung für die öffentliche Sicherheit“ nach sich zieht. In ländlichen Regionen kann beispielsweise der Ausfall der einzigen ortsansässigen Allgemeinarztpraxis weiterreichende Versorgungsengpässe nach sich ziehen, als der Ausfall einer großen kritischen Infrastruktur in einer Großstadt.

Der gewählte Weg, über eine gesetzliche Definition der kritischen Infrastrukturen und eine ergänzende gesetzeskonkretisiere Verordnung Normenklarheit über den Anwendungsbereich des weite Teile des öffentlichen Lebens erfassenden ITSiG zu schaffen, kann die geeignete Grundlage für branchenspezifische Differenzierungen darstellen. Insbesondere über die Rechtsverordnung muss aber die noch sehr weite Definition potentiell gefährdeter Infrastrukturen an der Versorgungskritikalität orientiert auf diejenigen Organisationseinheiten und Anwendungen fokussiert und eingegrenzt werden, deren Ausfall tatsächlich zu schwerwiegenden Beeinträchtigungen für das Gemeinwohl führen können.

Die DKG ist bereit, sich in den entsprechenden Prozess einzubringen und sich an der Arbeitsgruppe des BSI zu beteiligen.

Zu Artikel 1 Nr. 6 und 7

Beabsichtigte Neuregelung

Die Neuregelung konkretisiert die Handlungsmöglichkeiten des BSI zur Warnung und Information der Öffentlichkeit zu Sicherheitslücken oder Schadprogrammen etc. sowie zur Untersuchung der am Markt bereitgestellten informationstechnischen Produkte, Systeme und Dienste.

Stellungnahme

Die DKG begrüßt die erweiterten Untersuchungs- und Informationsrechte des BSI. Nur durch belastbare Informationen zur Abschätzung des Bedrohungspotentials und Ausmaßes der durch Cyber-Angriffe möglichen Beeinträchtigungen und Risiken werden die Betreiber kritischer Infrastrukturen in die Lage versetzt, eine aus der tatsächlichen Bedrohungslage objektiv ableitbare Abwehrstrategie zu entwickeln. Dies setzt unmittelbar bei den verwendeten informationstechnischen Produkten, Systemen und Dienste an und zeigt konkrete Handlungsmöglichkeiten auf.

Zu Artikel 1 Nr. 8

Beabsichtigte Neuregelung

Die Neuregelung beschreibt die Verpflichtung der Betreiber kritischer Infrastrukturen, am „Stand der Technik“ orientierte Vorkehrungen zur Gefahrenabwehr zu treffen und

verpflichtet diese, innerhalb definierter Zeitabstände regelmäßig wiederkehrende externen Sicherheitsaudits durchführen zu lassen. Ergänzend wird die Funktion des BSI als zentrale Meldestelle für die Betreiber kritischer Infrastrukturen bei Beeinträchtigungen von informationstechnischen Systemen festgeschrieben.

Stellungnahme

1. Bestimmtheit der Anforderungen

Die gesetzliche Vorgabe für Betreiber kritischer Infrastrukturen, „angemessene organisatorischen und technischen Vorkehrungen“ zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, beinhaltet für die kritische Infrastruktur weder konkrete noch hinreichend bestimmte Anforderungen und ist äußerst interpretationsfähig. Auch wenn die Bewertung einzuführender Schutzmaßnahmen zu Recht unter den Grundsatz der Verhältnismäßigkeit gestellt wird, orientiert sich die Bewertung nur an den möglichen Ausfallfolgen und daraus resultierenden Beeinträchtigungen als Kriterien. Unberücksichtigt bleiben die Eintrittswahrscheinlichkeit eines Ausfalls sowie die verbleibende Arbeitsfähigkeit der Infrastruktur.

Bei falscher Bewertung des Kontextes durch externe Auditoren oder das BSI kann dies zu einem Aufwands-Overhead oder zu einer Lähmung der Arbeitsfähigkeit der Infrastruktur durch überschießende IT-Sicherheitsmaßnahmen führen. Letztlich legt damit der Auditor bei seiner Prüfung die Maßstäbe selbst fest. Dies wirft hinsichtlich der Einheitlichkeit der Prüfungsergebnisse Fragezeichen auf und kann zu interessensgesteuerten Ergebnissen führen.

Der geforderte „Stand der Technik“ ist zu weitreichend, da dies auf fortschrittliche Verfahren referenziert, die nicht hinreichend und langjährig erprobt sind, was gerade in der Medizin aber zwingend erforderlich ist. Angemessen wäre lediglich ein Verweis auf die „allgemein anerkannten Regeln der Technik“, die auch in der Medizin durch hinreichende Erprobung ihre Tauglichkeit bewiesen haben.

Dies muss in den vorgesehenen Branchenstandards berücksichtigt werden und die DKG ist bereit, sich an den dafür notwendigen Arbeiten zu beteiligen.

2. Konkretisierung der abzusichernden Risiken

Ergänzend bedarf es einer Konkretisierung der abzusichernden Risiken, weil die medizinische Versorgung im Krankenhaus nicht mit den vollautomatisierten IT-gestützten Produktionsprozessen anderer Branchen vergleichbar ist. Es muss danach unterschieden werden, ob die IT zum Kern der Aufgabenerfüllung der Einrichtung gehört, oder nur eines von vielen Instrumentarien bei der Verfolgung des Unternehmenszwecks darstellt. Gerade im Krankenhausbereich liegt die Kritikalität als Infrastruktur weniger in der IT-Sicherheit, als vielmehr in den Abhängigkeiten von anderen kritischen Infrastrukturen.

Ohne Zweifel nehmen Krankenhäuser eine wesentliche Funktion in der Daseinsvorsorge ein. Gerade in Großschadenslagen haben Krankenhäuser unverzichtbare Aufgaben zur Krisenbewältigung. Dazu gehört insbesondere

- Menschenleben zu retten und die Gesundheit von Mitarbeitern und Patienten sowie des ggf. unterstützenden Rettungsdienstpersonals zu erhalten,

- die Funktionsfähigkeit der Einrichtung, mindestens in ihren kardinalen Funktionsbereichen, zu erhalten, sowie

- materielle und ggf. immaterielle Schäden zu minimieren.

Die Krankenhäuser nehmen diese Aufgaben bereits heute z.B. im Rahmen ihrer Einbindung in den Katastrophenschutz wahr und orientieren sich hierbei eng an dem mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe abgestimmten Leitfaden „Schutz kritischer Infrastrukturen: Risikomanagement im Krankenhaus“.

Der zur Identifikation und Reduzierung von Ausfallrisiken in Krankenhäusern dienende Leitfaden zeigt aber deutlich, dass die eigentlichen Risiken für die Aufrechterhaltung eines Krankenhausbetriebes in Krisenszenarien primär vom Fortbestand der Funktionsfähigkeit anderer kritischer Basisinfrastrukturen abhängen. Ausgehend von dem gebräuchlichen All-Gefahren-Ansatz bei der Bewertung einer Gefährdung kritischer Infrastrukturen sind Krankenhäuser grundsätzlich von Domino- und Kaskadeneffekten bei einem Ausfall mehrerer eng vernetzter technischer Basisinfrastrukturen betroffen. Insbesondere die dauerhafte und zuverlässige Verfügbarkeit der öffentlichen Wasserversorgung, der Telefonverbindungen, der Lebensmittel- und Energieversorgung sowie der Banken ist in Extremsituationen nicht verzichtbar.

Maßgeblich für die adäquate Handhabung derartiger Schadenslagen ist die Krankenhausalarmplanung. Die z.T. landesrechtlich vorgeschriebenen Krankenhausalarmpläne enthalten Verhaltensanweisungen und Checklisten z.B. für Bombendrohungen, den Massenanfall Verletzter und Sterbender (Triage), oder die Kontamination von Patienten mit chemischen, biologischen oder radiologischen Substanzen.

In Krankenhäusern ist gerade die Verfügbarkeit von Trinkwasser eine Überlebensnotwendigkeit. Beeinträchtigungen der Trinkwasserversorgung entweder durch fehlendes Wasser im System (Bruch von Transportleitungen oder Ausfall von Pumpen), oder durch Qualitätsdefizite z.B. aufgrund einer Kontamination mit Mikroorganismen oder Chemikalien führen unmittelbar zum Zusammenbruch einer geordneten Krankenhausversorgung.

Weiterhin ist das Krankenhaus auf eine reibungslose Kooperation mit der Vielzahl der übrigen hoch spezialisierten Organisationen und Akteure der Gesundheitsbranche angewiesen, wie z.B. dem Rettungsdienst, der Medikamentenversorgung, externer Laborleistungen, niedergelassener Ärzte und dem öffentlichen Gesundheitsdienst.

Innerhalb des Krankenhauses selbst muss im Wesentlichen die Funktionsfähigkeit der medizinischen Fachabteilungen, die Sterilgutversorgung, die Küche, der Krisenstab und die IT nur in den Teilen, in denen die Nutzung von Medizinprodukten über das IT-Netzwerk erfolgt, sichergestellt werden, nicht jedoch aber die Nutzung netz-

werkunabhängiger Medizinprodukte. Auf deren Ausfallsicherheit hat das Krankenhaus aufgrund der strikten Zulassungsvorgaben des MPG ohnehin keinen Einfluss.

Neben der Wasserversorgung ist die Stromversorgung existentiell für die Funktionsfähigkeit der Krankenhäuser. Alle Geräte zur Diagnostik bis hin zu Geräten mit lebenserhaltenden Funktionen sind von einer dauerhaften und zuverlässigen Stromversorgung abhängig. Die Ausstattung mit Geräten zur Notstromversorgung bzw. mit Sicherheitsstromversorgungsanlagen ist bereits heute in den Bundesländern im Krankenhausrecht geregelt und wird von den Häusern umgesetzt. In längerfristigen Schadensszenarien ist die unterbrechungsfreie Treibstoffversorgung dieser Aggregate allerdings von der Funktionsfähigkeit der kritischen Infrastruktur Transport abhängig.

Die Versorgung mit Arzneimitteln und Lebensmitteln, die Sterilisation von medizinischen Instrumenten, die Reinigung der Wäsche und die Versorgung mit sonstigen Gütern ist ebenfalls fundamentale Voraussetzung für das Aufrechterhalten eines Krankenhausbetriebes. Besonders der Krankenhausapotheke kommt hierbei eine herausragende Bedeutung bei der Sicherung der Arzneimittelversorgung zu. Sofern die allgemein übliche Bevorratungslagerung von Arzneimitteln für ca. 14. Tage überschritten werden muss, tritt ebenfalls die Abhängigkeit des Krankenhauses von anderen kooperierenden kritischen Infrastrukturen zu Tage.

Die in den Einrichtungen erstellten Gefährdungs- und Verwundbarkeitsanalysen umfassen auch spezifisch standortbezogene Risiken, wie z.B. eine erhöhte Hochwassergefährdung, Erdbebengefahr in Regionen erhöhter seismischer Aktivität und sonstige Naturgefahren.

Die Sicherung der Informations- und Telekommunikationstechnik im Krankenhaus ist differenziert zu betrachten. Soweit es um die einrichtungsübergreifende fallbezogene Kommunikation zwischen Versorgungseinrichtungen (Krankenhäusern, Vertragsärzten, Reha-Einrichtungen etc.) geht, hat der Gesetzgeber die Verantwortung für Datensicherheit und Datenschutz auch der Gesellschaft für Telematikanwendungen der Gesundheitskarte (gematik) übertragen. Die gematik spezifiziert gegenwärtig ein hochsicheres Netz zur Kommunikation der Einrichtungen untereinander und schützt die Einrichtungen vor Cyber-Angriffen durch den Einsatz spezifischer Hochsicherheitskomponenten.

Für die IT-Sicherheit innerhalb der Krankenhäuser soll die internationale Norm IEC 80001-1:2010 „Application of risk management for IT- networks incorporating medical devices“ helfen, die Aktivitäten in diesem Bereich zu systematisieren und die Effektivität des Risikomanagements im Krankenhaus zu erhöhen. Mit der deutschen Veröffentlichung der internationalen IEC-Norm als DIN EN 80001-1:2011 „Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten“ wird ein Normenwerk zur Verfügung gestellt, welches für die Beherrschung grundlegender Risiken, die aus dem Betrieb eines medizinischen IT-Netzwerkes erwachsen können, einen Risikomanagementprozess nach dem aktuellen Stand der Technik beschrieben. Die Deutsche Krankenhausgesellschaft hat hierzu explizit Umsetzungshinweise für die Krankenhäuser veröffentlicht.

Weitergehende Sicherheitsmechanismen sind z.T. gar nicht umsetzbar. Zahlreiche medizinische Systeme dürfen nach den Vorgaben der Hersteller nicht modifiziert und etwa gegen Hackerangriffe oder Vireninfektionen geschützt werden. Damit besteht keine Möglichkeit, auf den medizinischen Systemen installierte Betriebssysteme und Anwendungssoftware durch Patches oder Updates zu schützen; selbst bekannte Schwachstellen dürfen nicht beseitigt werden. Ein darüber hinausgehender individueller Schutz eines jeden einzelnen Medizinprodukts sowohl vor Angriffen aus dem Internet als auch, wegen der wechselseitigen Kommunikation der Systeme untereinander, vor Gefahren aus dem internen Netz würde einen immensen technischen Aufwand (Firewall für jedes einzelne medizinische System) und einen extrem hohen organisatorischen Aufwand nach sich ziehen, da den Herstellern der medizinischen Systeme oft die Kommunikationsbeziehungen zwischen den Systemen innerhalb des Krankenhausnetzes gar nicht bekannt sind.

Die „übrige“ Krankenhaus-IT, die häufig der Leistungsdokumentation, Absicherung von Fallprüfungen, Gewährleistung einer ordnungsgemäßen Abrechnung und weiterer administrativer Verpflichtungen des Krankenhauses dient, dürfte unter dem Blickwinkel einer kritischen Infrastruktur nicht relevant sein. In für den Fortbestand des staatlichen Gemeinwohls bedrohlichen Krisenszenarien, in denen die Rettung und Lebenserhaltung einer Vielzahl von Verletzten absolut prioritär ist, wäre ein Ausfall oder ein Nicht-Bedienen administrativer Verpflichtungen für die Patientenversorgung nicht substantiell und temporär akzeptabel.

Die entsprechenden Erkenntnisse wird die DKG in die Erstellung des Branchenstandards einbringen.

Änderungsvorschlag

Aufnahme einer Verpflichtung zur Identifizierung und Ausweisung der für den Betrieb der kritischen Infrastruktur maßgeblichen informationstechnischen Systeme, Komponenten oder Prozesse sowie Fokussierung der erforderlichen Abwehrmaßnahmen ausschließlich auf diese unternehmenskritischen Bereiche:

„§ 8a

Sicherheit der Informationstechnik kritischer Infrastrukturen

(1) Betreiber kritischer Infrastrukturen sind verpflichtet, binnen … Jahren nach Inkrafttreten der Rechtsverordnung nach § 10 Abs. 1 diejenigen informationstechnischen Systeme, Komponenten oder Prozesse zu identifizieren und auszuweisen, die für den Erhalt der Funktionsfähigkeit der Einrichtung als kritische Infrastruktur unverzichtbar sind. Für die so ausgewiesenen unternehmenskritischen Bereiche sind angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen …“

3. Branchenspezifische Sicherheitsstandards

Die im Gesetzentwurf als § 8a Abs. 2 eröffnete Option zur Etablierung branchenspezifischer Sicherheitsstandards, deren Eignung durch das BSI zu bestätigen ist, muss ebenfalls differenziert betrachtet werden.

Erst nach Identifikation der tatsächlich für die Funktionsfähigkeit der Unternehmen kritischen IT-Anwendungen kann eine Diskussion über heranzuziehende Standards und deren Bewertung als ggf. geeignetes Instrument zur Beurteilung der Sicherheit von informationstechnischen Systemen erfolgen. Die Diskussion über die Notwendigkeit ggf. branchenspezifischer Sicherheitsstandards ist erst ein zweiter Schritt bei der Bewertung. Die bisherigen Erfahrungen mit dem BSI stimmen allerdings skeptisch, ob hier wirklich realistische und an der Praxis orientierte Lösungen für den Krankenhausbereich abgestimmt werden können.

4. Durchführung von Audits

Bei der in 8a Abs. 3 geregelten Verpflichtung zur Durchführung regelmäßiger Sicherheitsaudits ist zu berücksichtigen, dass schon jetzt jährliche Audits im Bereich der Krankenhaus-IT durchgeführt werden, deren Ergebnisse und Zertifikate auch im Rahmen der Diskussion um kritische Infrastrukturen anerkannt werden sollten.

Die verpflichtende Einführung zusätzlicher spezieller IT-Sicherheitsaudits mindestens alle zwei Jahre auf Grundlage nicht hinreichend konkretisierter Bedrohungen und Bewertungskriterien etabliert lediglich neue Geschäftsfelder. Neben den Auditorkosten und Zertifikatskosten sind auch personelle Mehrkosten in den Einrichtungen durch den Auditierungsprozess an sich und die Erstellung der jeweils auditspezifischen Dokumentensammlungen zu verzeichnen.

Vorzugswürdig sind interne Audits durch ein (meist ohnehin vorhandenes) Qualitätsmanagement anhand von Kriterienkatalogen, damit nicht immer teure externe Auditoren eingeschaltet werden müssen. Zudem ist der vorgesehene Zwei-Jahres-Zeitraum als Prüfturnus zu belastend, weshalb auf mindestens 4 oder 5 Jahre abgestellt werden sollte.

5. Finanzierung der erforderlichen Aufwendungen

Dem Gesetzentwurf fehlt jegliche Regelung zur Refinanzierung der geforderten Investitionen in die IT-Sicherheit kritischer Infrastrukturen. Der Entwurf beschreibt eine notwendige Anhebung der Sicherheitsstandards in allen Bereichen und impliziert damit notwendige Investitionen in noch nicht abzuschätzender Höhe und eine evtl. notwendige personelle Aufstockung in den IT-Bereichen, um insbesondere weitere Überwachungspflichten umzusetzen.

Speziell die deutschen Krankenhäuser kämpfen seit Jahren mit einer chronischen investiven Unterfinanzierung. Cyberangriffe gehören nicht zu den die Existenz von Krankenhäusern gegenwärtig primär bedrohenden Risiken. Angesichts des noch vollständigen Fehlens von belastbaren Informationen zu Bedrohungspotential und Ausmaß derartiger Angriffe sind erhebliche Investitionen in die Steigerung der Resilienz gegen Cyberangriffe nicht vermittelbar. Dies gilt insbesondere, da die IT im Krankenhaus nur eines von vielen Instrumentarien bei der Verfolgung des Unternehmenszwecks darstellt und die Kritikalität als Infrastruktur weniger in der IT-Sicherheit, als vielmehr in der Abhängigkeit von anderen kritischen Infrastrukturen liegt. Deutliche Steigerungen der IT-Sicherheit würden finanziell direkt zu Lasten der direkten Patientenversorgung gehen.

Hiervon unberührt bleibt selbstverständlich die Bereitschaft zur Fortsetzung des begonnenen Dialogs zur Unterstützung der staatlichen Sicherheitsorgane bei der Erfüllung von deren Aufgaben zur Abwehr von Bedrohungen aus dem Cyberraum durch ein Zur-Verfügung-Stellung von branchenspezifischen Know-how.

6. BSI als zentrale Meldestelle

DKG begrüßt die grundsätzliche Intention, alle verfügbaren Erkenntnisse zu Ursachen und Ausmaß von Bedrohungen aus dem Cyberraum zu sammeln und auch den Betreibern kritischer Infrastrukturen auf Ersuchen zur Verfügung zu stellen. Nur ein objektives Bedrohungslagebild kann als Grundlage für die Ableitung von geeigneten und erforderlichen Abwehrmaßnahmen dienen.

Mit dem Gesetzentwurf werden aber zentralistische Kontrollstrukturen beim BSI eingeführt, die über das anzustrebende Ziel deutlich hinausgehen und z.T. sogar riskant und kontraproduktiv sind. Durch die verbindlichen Meldungen von Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozessen gegenüber dem BSI wird ein zentrales Register über die informationstechnischen Schwachstellen der gesamten deutschen Volkswirtschaft geschaffen. Wer dieses Register erfolgreich angreift, besitzt alle erforderlichen Informationen für flächendeckende Angriffe auf die deutsche Volkswirtschaft.

Die Erforderlichkeit einer zentralen, unternehmendbezogenen Sammlung von Informationen aus Sicherheitsaudits beim BSI sollte nochmals grundsätzlich überdacht werden, oder es sollten Mechanismen entwickelt werden, der neu geschaffenen Bedrohungssituation zu begegnen, insbesondere mit dem Blick auf das sehr konkret gewordene Risiko der Unterwanderung auch von öffentlichen Einrichtungen.

Soweit § 8b des Entwurfs die Funktion des BSI als zentrale Meldestelle für die Sicherheit in der Informationstechnik für die Betreiber kritischer Infrastrukturen festschreibt, bedarf es Anpassungen:

- Es ist definitiv nicht sinnvoll, eine Störung noch vor der Ursachenanalyse zu melden.

- Die Schwelle für die Meldepflicht muss erhöht werden. Eine bedeutende Störung könnte z.B. schon die momentane Fehlfunktion des Virenscanners sein. Eine Meldepflicht sollte sich auf Fälle fundamentaler Störungen beschränken, die Beeinträchtigungen von erheblichem Umfang für Dritte bedeuten oder als sehr wahrscheinlich erscheinen lassen.

- Das Erfordernis der „Unverzüglichkeit“ darf den internen Problembehehebungsprozess nicht beeinträchtigen. Besonders in kleinen Krankenhäusern sind oft alle Mitarbeiter mit der Störungsursachensuche und -beseitigung gefordert, so dass sich eine Pflicht zur unverzüglichen Kommunikation kontraproduktiv auswirken kann. Es sollte zumindest im Rahmen der Begründung darauf hingewiesen werden, dass ein kurzfristiges Zurückstellen der erforderlichen Meldung zugunsten der akuten Problembehebung nicht als schuldhaftes Zögern zu werten ist.

- Es bedarf einer Harmonisierung mit anderen Meldepflichten, um erhöhte Verwaltungsaufwände durch Doppelmeldungen und ggf. unterschiedliche, nicht kompatible Verschlüsselungstechniken zu den einzelnen Behörden bzw. dem BSI zu vermeiden. Insbesondere die Fortführung der bisherige Meldepflicht aus § 42a BDSG (Informationspflicht bei unrechtmäßiger Kenntniserlangung von Daten) muss kritisch hinterfragt werden.

- Auf das grundsätzliche Risiko der Etablierung einer zentralen Institution mit umfassender Kenntnis der informationstechnischen Schwachstellen der gesamten deutschen Volkswirtschaft ist bereits hingewiesen worden.

Zu Artikel 1 Nr. 9

Beabsichtigte Neuregelung

Die Neuregelung beschreibt die Voraussetzungen, unter denen eine Einrichtung oder Anlage als kritische Infrastruktur klassifiziert wird.

Stellungnahme

Die DKG begrüßt den Weg, über eine gesetzeskonkretisiere Verordnung Normenklarheit über den Anwendungsbereich des weite Teile des öffentlichen Lebens erfassenden ITSiG zu schaffen. Die Rechtsverordnung muss aber die noch sehr weite Definition potentiell gefährdeter Infrastrukturen an der Versorgungskritikalität orientieren und auf diejenigen Organisationseinheiten und Anwendungen fokussieren und eingrenzen, deren Ausfall tatsächlich zu schwerwiegenden Beeinträchtigungen für das Gemeinwohl führen können. Entsprechende Vorgaben für das Verordnungsgebungsverfahren fehlen. Auch der explizite Ausschluss eines Zugangs zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, schafft nicht die erforderliche Transparenz und das Vertrauen in diesen Prozess.

Zu Artikel 2 (Änderung des Telemediengesetzes)

Zu Artikel 2 Nr. 2

Beabsichtigte Neuregelung

Die Neuregelung ermächtigt die Anbieter von Telemedien zur Speicherung von Nutzungsdaten für den Zeitraum von 6 Monaten auf Vorrat.

Stellungnahme

Mit Urteil vom 2. März 2010 hat das Bundesverfassungsgericht das deutsche Gesetz zur Vorratsdatenspeicherung für ungültig erklärt. Mit Urteil vom 8. April 2014 hat der Europäische Gerichtshof die EU-Richtlinie zur Vorratsdatenspeicherung für ungültig erklärt.

Die beabsichtigte Neuregelung wird vom Arbeitskreis Vorratsdatenspeicherung als „verdachtslose Aufzeichnung des Surfverhaltens“ gewertet, bei der sogar Inhalte sechs Monate archiviert und ausgewertet werden dürften. Dies gehe noch über die

frühere Speicherung von Verbindungs- und Standortdaten hinaus, die das Bundesverfassungsgericht für ungültig erklärt hat.

Die DKG sieht vor diesem Hintergrund in der beabsichtigten Neuregelung kein dem Grundsatz der Verhältnismäßigkeit entsprechendes Mittel zu Steigerung der IT-Sicherheit, sondern vielmehr eine Steigerung der Risiken einer Überwachung des Internetverkehrs.

Zu Artikel 3 (Änderung des Telekommunikationsgesetzes)

Zu Artikel 3 Nr. 2

Beabsichtigte Neuregelung

Die Neuregelung ermächtigt die Anbieter von Telekommunikationsdiensten zur Nutzung von Bestandsdaten und Verkehrsdaten zur Eingrenzung und Beseitigung von Störungen der Telekommunikationsdienste.

Stellungnahme

Auch diese Neuregelung wird unter dem Gesichtspunkt einer verbotenen Vorratsdatenspeicherung als Nicht-Verhältnismäßig zur Erreichung des gesetzgeberischen Ziels abgelehnt.

Zu Artikel 3 Nr. 4

Beabsichtigte Neuregelung

Die Neuregelung beschreibt die Information und Unterstützung der Verbraucher bei der Prävention und der Beseitigung von IT-Sicherheitsvorfällen.

Stellungnahme

Nach Einschätzung der DKG fallen Patiententelefone nicht unter öffentlich zugängliche Telekommunikationsdienste. Entsprechendes muss gelten, wenn Krankenhäuser ihren Patienten die inzwischen als selbstverständliche Informationsquelle angesehene Nutzung von LAN oder WLAN anbieten.

Es muss gewährleistet sein, dass Krankenhäuser als Telekommunikationsanbieter generell nicht unter die erweiterten Pflichten nach §§ 109, 109a TKG fallen. Andernfalls wären sie zu einer technischen Unterstützung der IT-Endgeräte der Patienten verpflichtet, was zwangsläufig dazu führen müsste, derartige Angebote mit Inkrafttreten des Gesetzes abzuschaffen.

Änderungsvorschlag

Klarstellung, dass die erweiterten Pflichten nach §§ 109, 109a TKG nicht auf Krankenhäuser als Telekommunikationsanbieter zutreffen.

Zu Artikel 5 (Änderung des Bundeskriminalamtgesetzes)

Beabsichtigte Neuregelung

Die Neuregelung erweitert die Zuständigkeit des Bundeskriminalamtes für Straftaten nach § 303b StGB (Computersabotage), wenn sich die Tat gegen Bundeseinrichtungen richtet.

Stellungnahme

Die DKG begrüßt ausdrücklich die Ausweitung der Zuständigkeit des Bundeskriminalamtes.

Die Ausweitung der Befugnisse einer sowohl zur Gefahrenabwehr als auch zur Strafverfolgung zuständigen Bundesbehörde stellt nach Auffassung der DKG den ordnungspolitisch richtigen Weg dar, die Gefahrenabwehrkompetenz der staatlichen Sicherheitsorgane auch im Bereich von Cyberrisiken zu stärken. Dies weckt die Erwartung, dass der Schutz der für das staatliche Gemeinwesen als notwendig angesehenen Infrastrukturen nicht auf deren Betreiber abgewälzt wird, sondern durch die zuständigen staatlichen Instanzen künftig wahrgenommen wird.

Leider verfolgt der Gesetzentwurf diesen Weg nicht konsequent und dehnt die Zuständigkeit des BKA nicht auch auf die §§ 202a (Ausspähen von Daten), 202b (Abfangen von Daten), 202c (Vorbereiten des Ausspähens und Abfangens von Daten), 263a (Computerbetrug) und 303a StGB (Datenveränderung) aus, wie dies Vorentwürfe zum ITSiG vorgesehen hatten.

Fehlende Übergangsfristen

Der Gesetzentwurf enthält keine Übergangsfristen. Angesichts des Erfordernisses einer umfassenden Bestandsaufnahme und Risikobewertung in den als kritisch eingestuften Infrastrukturen und der Einführung von aus der konkreten Bedrohungslage ableitbaren erforderlichen Schutzmaßnahmen bedarf es – neben der erforderlichen Finanzierung – mindestens eines 4-jährigen Übergangszeitraums zur Einstellung auf die neue Situation.