Stellungnahme der Bundesärztekammer

zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz - ITSiG)

Berlin, 05.04.2013

Korrespondenzadresse:

Bundesärztekammer
Herbert-Lewin-Platz 1
10623 Berlin

Die Bundesärztekammer wurde mit Schreiben vom 05.03.2013 vom Bundesministerium des Inneren (BMI) um Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz - ITSiG) im Stadium eines Gesetzentwurfs, der innerhalb der Bundesregierung noch nicht abgestimmt ist, gebeten. Gegenstand des Entwurfs sind Änderungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz), das Bundeskriminalamtgesetz (BKA-Gesetz), das Telemediengesetz sowie das Telekommunikationsgesetz. Demnach werden Pflichten zur Erfüllung von Mindestanforderungen an IT-Sicherheit für Betreiber kritischer Infrastrukturen (inklusive Telekommunikationsanbieter), Meldepflichten bei erheblichen Sicherheitsvorfällen sowie Meldepflichten an das BSI definiert. Außerdem wird die Zuständigkeit des BKA im Bereich der Internetkriminalität erweitert.

Die Bundesärztekammer nimmt zum Entwurf des Gesetzes wie folgt Stellung:

Die Bundesärztekammer begrüßt grundsätzlich die Intention des Referentenentwurfs für ein IT-Sicherheitsgesetz, den Schutz kritischer IT-Infrastrukturen zu verbessern.
Die Bundesärztekammer bezieht ihre Stellungnahme auf IT-Infrastrukturen im Gesundheitswesen. Hierbei stellt sich insbesondere die Frage, welche Infrastrukturen im Gesundheitswesen aus IT-Sicherheitsaspekten als kritisch einzustufen sind.

Die geplante Telematik-Infrastruktur, die auf Grundlage des § 291a SGB V realisiert werden soll, wird viele Akteure im Gesundheitswesen vernetzen und Anwendungen für Ärzte und Patienten bereitstellen. Perspektivisch sollen über diese Infrastruktur auch Anwendungen wie die elektronische Verordnung (eRezept) oder elektronische Patientenakten aufgebaut werden, die dann einen bedeutenden Einfluss auf die medizinische Versorgung der Bevölkerung haben könnten, wenn sie flächendeckend etabliert sind. Die Telematik-Infrastruktur im Gesundheitswesen wird aktuell von der verantwortlichen Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) mit besonderem Blick auf die IT-Sicherheit entwickelt und dürfte unserer Einschätzung nach alle Anforderungen des Entwurfs des IT-Sicherheitsgesetzes erfüllen. Bereits in der Konzeption werden wesentliche IT-Sicherheitsanforderungen mit dem BSI abgestimmt. Ärzte und Patienten müssen auf die Sicherheit in einer künftigen Telematik-Infrastruktur vertrauen können.

Die IT-Infrastruktur der Arztpraxen fällt dagegen nicht unter die Definition der „kritischen Infrastrukturen“ im Sinne des § 2 Absatz 9 BSI-Gesetz neu. Die Bundesärztekammer hat zusammen mit der Kassenärztlichen Bundesvereinigung Empfehlungen zur IT-Sicherheit in den Arztpraxen in Abstimmung mit dem BSI veröffentlicht. Aus medizinischer Sicht betrachten diese die IT der Arztpraxis nicht als kritische Infrastruktur. Informationstechnologie wird hauptsächlich für die Verwaltung, Abrechnung und die medizinische Dokumentation in einer Arztpraxis eingesetzt. Auch komplexe technisch-medizinische Geräte, die für die Diagnose und Therapie eingesetzt werden, sind in der Regel autonome Geräte und können ihre Aufgabe unabhängig und ohne jegliche Vernetzung erfüllen. Ein Ausfall der IT in einer Arztpraxis wird daher die medizinische Versorgung weder der eigenen Patienten noch der Bevölkerung insgesamt beeinträchtigen. Die verpflichtende Zertifizierung der IT-Sicherheit sowie die Belegung der Arztpraxen mit Meldepflichten sind daher unnötig, unverhältnismäßig und würden die Arztpraxen in hohem Maße wirtschaftlich und zeitlich belasten, ohne einen konkreten Effekt im Sinne des Gesetzgebers zu erzielen. Dies muss in der Erarbeitung der geplanten Verordnung nach § 2 Absatz 10 (neu) des künftigen BSI-Gesetzes berücksichtigt werden.

Zu den Regelungen im Einzelnen:

Zu Artikel 1 Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik, Nummer 5 a:

Arztpraxen fallen nicht unter die Legaldefinition der „kritischen Infrastrukturen“. Grund dafür ist die Tatsache, dass eine Arztpraxis auch ohne funktionierende Praxis-IT Patienten medizinisch versorgen kann. Zudem ist der mögliche Ausfall einer einzelnen Praxis ohne nennenswerte Auswirkung auf die gesamte medizinische Versorgung der Bevölkerung. Sollten Arztpraxen als „kritische Infrastrukturen“ betrachtet werden, würde dies zu unverhältnismäßig hohen finanziellen und zeitlichen Belastungen führen.
Diese Regelungen beziehen auf Artikel 1, Nummer 4:

- **§ 8a (neu):**

  Zu Absatz 1:
  Die Umsetzung von Maßnahmen nach dem Stand der Technik zur unbedingten Wahrung der Funktionsfähigkeit der IT einer Arztpraxis ist unverhältnismäßig aufwändig und teuer. Die Definition der Angemessenheit für die Maßnahmen gibt dem Arzt keinen hinreichenden Anhaltspunkt, ob eine konkrete Maßnahme tatsächlich realisiert werden muss oder nicht.
  Zu Absatz 4:
  Die Durchführung von Sicherheitsaudits in zweijährigen Zeitabständen ist für eine Arztpraxis unverhältnismäßig aufwändig und teuer.

- **§ 8b (neu):**

  Zu Absatz 3:
  Die Anforderung, für das BSI jederzeit erreichbar zu sein, ist für eine Arztpraxis personell in der Regel nicht umsetzbar und für den Praxisinhaber unzumutbar.

  Zu Absatz 4:
  Die Meldung von Beeinträchtigungen der IT-Systeme wäre für eine Arztpraxis und auch für das BSI sehr aufwändig, da diese z. B. auch Fälle wie Stromausfall, Virenbefall oder den Ausfall einer Festplatte umfassen würde.

Fazit:
Die Bundesärztekammer begrüßt den Entwurf des IT-Sicherheitsgesetzes. Ärzte und Patienten müssen auf die IT-Sicherheit kritischer Infrastrukturen im Gesundheitswesen, wie z. B. einer künftigen Telematik-Infrastruktur vertrauen können. Es muss aber betont werden, dass Arztpraxen aus IT-Sicherheitssicht objektiv keine „kritischen Infrastrukturen“ im Sinne des § 2 Absatz 9 BSI-Gesetz neu darstellen. Daher sollte aus Gründen der Klarstellung zu Artikel 1 Nr. 1 (§ 2 Begriffsbestimmungen) in die Gesetzesbegründung aufgenommen werden, dass die IT in Arztpraxen nicht unter die Definition „kritische Infrastrukturen“ fällt.