GMDS - Deutsche Gesellschaft für Medizinische Informatik,
Biometrie und Epidemiologie e.V.
Industriestraße 154
D-50996 Köln

Tel.: +49 (2236) 3319958
Fax: +49 (2236) 3319959
Email: info@gmds.de
http://www.gmds.de

Vereinsregister: VR 16225 Amtsgericht Köln

Umsatzsteuer-Identifikationsnummer:
27.07.02 DE 182645846

# Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme („IT-Sicherheitsgesetz“, ITSiG) - Bedeutung für das Gesundheitswesen

## 1 Einführung

### 1.1 Zielsetzung

Deutschland soll besser vor „Cyber-Angriffen“ geschützt werden. Dazu sollen kritische Infrastrukturen des Landes ein entsprechend hohes Schutzniveau gegenüber derartigen Angriffen aufweisen.

### 1.2 Wesentliche Inhalte bzw. Forderungen des Entwurfs

Das IT-Sicherheitsgesetz beinhaltet Änderungen bzw. Ergänzungen von vier Gesetzen:

- Dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz),
- dem Bundeskriminalamtgesetz,
- dem Telemediengesetz (TMG) sowie
- dem Telekommunikationsgesetz (TKG).

Hierbei werden im ITSiG Anforderungen an „kritische Infrastrukturen“ gestellt, die

- in **Einrichtungen**, **Anlagen** oder **Teilen** davon
- in den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, **Gesundheit**, Wasser, Ernährung sowie Finanz- und Versicherungswesen,

- die von hoher Bedeutung für das **Funktionieren des Gemeinwesens** sind und
- durch deren **Ausfall** oder **Beeinträchtigung** nachhaltig wirkende **Versorgungsengpässe** oder **erhebliche Störungen** der öffentlichen Sicherheit eintreten würden,

eingesetzt werden. Zu diesen Anforderungen gehören:

1) Pflicht zur Erfüllung von Mindestanforderungen an IT-Sicherheit nach dem Stand der Technik (§8a abs. 1)
2) Zur Überprüfung der organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen sind spätestens 2 Jahre nach Inkrafttreten der Verordnung sowie anschließend mindestens alle zwei Jahre Sicherheitsaudits durch anerkannte Auditoren durchzuführen.
3) Mindestens alle 2 Jahre sind dem BSI eine Aufstellung der durchgeführten Sicherheitsaudits einschließlich der aufgedeckten Sicherheitsmängel zu übermitteln. (§8a Abs. 4)
    a. Das Bundesamt kann bei Sicherheitsmängeln eine Übermittlung der gesamten Ergebnisse des Sicherheitsaudits verlangen. (§8a Abs. 4)
    b. Bei Sicherheitsmängeln kann das Bundesamt deren unverzügliche Beseitigung verlangen. (§8a Abs. 4)
4) Es besteht eine Meldepflicht bzgl. „erheblicher“ Sicherheitsmängel an das BSI. (§8b Abs. 4)
5) Dem BSI sind binnen eines Jahres nach Inkrafttreten der Rechtsverordnung Warn- und Alarmierungskontakte zu benennen. Der Betreiber hat sicherzustellen, dass er hierüber jederzeit erreichbar ist. (§8b Abs.3)
6) Branchen können brancheninterne Standards entwickeln, die das Bundesamt für die Sicherheit in der Informationstechnik (BSI) als Konkretisierung der gesetzlichen Verpflichtung anerkennt. (§8a Abs. 3)

Alle diese Anforderungen finden sich im allgemeinen Teil des Entwurfs, d.h. in dem Änderungsvorschlag zum BSI-Gesetz. Im Änderungsvorschlag zum TKG finden sich für TK-Anbieter weitere Forderungen, insbesondere eine Meldepflicht:

7) Beeinträchtigungen von Telekommunikationsnetzen und -diensten, die zu einer Störung der Verfügbarkeit der über diese Netze erbrachten Dienste oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssystemen der Nutzer oder Teilnehmer führen können und von denen der Netzbetreiber oder der Telekommunikationsdiensteanbieter Kenntnis erlangt, sind der Bundesnetzagentur unverzüglich mitzuteilen. (§109 Abs. 4)
8) Werden Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, sind diese vom Diensteanbieter unverzüglich zu benachrichtigen. (§109a Abs. 4)
9) Soweit technisch möglich und zumutbar, müssen die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hingewiesen werden, mit deren Hilfe die Nutzer Störungen, die von ihren Datenverarbeitungssystemen ausgehen, erkennen und beseitigen können. (§109a Abs. 4)

Sowohl im TMG wie auch im TKG ist ein „technisch und zumutbar“ Schutz der Dienste verankert, der dem „Stand der Technik“ entspricht.

## 2 Erfolgte Kommentierungen

Folgende Organisationen kommentierten den Entwurf:

1) Bundesverband der Deutschen Industrie (BDI); Kritikpunkte:
    a. Grundsätzliche Gefahr der Überregulierung
    b. Anwendungsbereich nicht präzise bestimmt
    c. Unklare Definition von Tatbeständen
    d. Doppelregulierung durch nationale und EU-Gesetzgebung
    e. Erheblicher finanzieller und bürokratischer Mehraufwand
    f. Datenschutz nicht ausreichend sichergestellt
    g. Umsetzungsfrist zu knapp bemessen
2) Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM); Kritikpunkte
    a. Grundsätzliche Gefahr der Überregulierung und Überschneidung von Kompetenzen
    b. Anwendungsbereich nicht präzise bestimmt
    c. Unklare Definition von Tatbeständen
    d. Umsetzungsfrist zu knapp bemessen
    e. Doppelregulierung durch nationale und EU-Gesetzgebung
3) Bundesverband IT-Sicherheit e.V. (TeleTrusT);
    a. Meldepflicht sinnvoller als ein auf Freiwilligkeit basierendes Meldesystem
    b. Harmonisierung mit Vorschlag zu einer EU-Richtlinie der EU-Kommission
4) Bundesärztekammer
    a. Arztpraxen fallen nicht unter die Definition einer „kritischen Infrastruktur“
5) Deutsches Institut für Normung e.V. (DIN);
    a. Bei Definition „Stand der Technik“ einschlägige internationale , europäische und nationale Normen heranziehen
    b. DIN bei der Erstellung branchenspezifischer Normen hinzuziehen
6) Verband der deutschen Internetwirtschaft eV. (eco); Positionen:
    a. Nationale Alleingänge vermeiden, Verantwortlichkeiten beachten, europäische und internationale Standards schaffen.
    b. Notwendig sind klare gesetzliche Definitionen, damit Rechtsicherheit gewährleistet ist.
    c. Risikobasierte Festlegung des Adressatenkreises bei Beachtung schon bestehender branchenspezifischer Verpflichtungen.
    d. Keine Erweiterung der bestehenden Meldepflichten für Betreiber von TK-Netzen und TK-Diensten.
    e. Keine Erweiterung der Haftung von Telemediendiensteanbietern.
    f. Freiwillige, verschlüsselte und anonymisierte Meldungen auf Grundlage des bestehenden Informationsaustausches.
    g. Hinweise an Kunden von Internetprovidern bei Hinweisen auf Schadprogramme können sinnvoll sein, wenn sie freiwillig erfolgen, starre bürokratische Hinweispflichten lehnt die Internetwirtschaft als ineffektiv und nicht praxistauglich ab.
    h. Gesetzliche Verpflichtungen für ein regionales Routing auf ihren Nutzen eingehend und kritisch prüfen.
    i. Branchenspezifische Mindestanforderungen im Wege der Selbstregulierung festlegen.
    j. Ende-zu-Ende-Verschlüsselung fördern.

7) Verband Deutscher Kabelnetzbetreiber (ANGA); Forderungen
    a. Telekommunikationsunternehmen aus allgemeinen Teil (BSI-Gesetz) herausnehmen
    b. Umsetzungsfrist angemessen gestalten (im Vorschlag 2 Jahre)
    c. Stand der Technik konkretisieren
    d. Beschränkung auf eine Meldestelle pro Branche (d.h. für TK die BNetzA)
    e. Konkretisierung, welche IT-Sicherheitsvorfälle Meldepflicht auslösen
    f. Neue Meldepflicht im TKG auf schwerwiegende Vorfälle beschränken

Die hier genannten Inhalte der jeweiligen Kommentierung stellen lediglich eine Zusammenfassung dar. Um die Zielrichtung der Kommentierung der jeweiligen Organisation bzw. des jeweiligen Verbandes zu erfassen, wird darum gebeten, die vollständige Kommentierung zu lesen. Die Internet-Links zu den jeweiligen Kommentierungen sind in Abschnitt 4 auf Seite 7 angegeben.

# 3 Fragestellungen

## 3.1 Definitionsfragen

| | |
|---|---|
| Mindestanforderungen an IT-Sicherheit | |
| Stand der Technik | §8a Abs. 2:<br>„Stand der Technik im Sinne dieses Gesetzes ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität und Vertraulichkeit gesichert erscheinen lässt.<br>Bei der Bestimmung des Standes der Technik sind insbesondere vergleichbare Verfahren, Einrichtungen und Betriebsweisen heranzuziehen, die mit Erfolg in der Praxis erprobt wurden.“ |
| Erhebliche Sicherheitsmängel | |

## 3.2 Abgrenzungsfrage

Die EU-Kommission stellte am 7. Februar 2013 die „Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit“ (Cybersicherheitsrichtlinie) als Entwurf vor [siehe Abschnitt 6 Ziffer 9) und 10)]. Auch diese Richtlinie sieht eine Reihe von Maßnahmen zur Gewährleistung einer Netz- und Informationssicherheit vor, desgleichen eine Meldepflicht.

Sollte dieser Vorschlag verabschiedet werden, muss die dann verabschiedete Richtlinie in nationales Gesetz umgesetzt werden. Es ist als jetzt schon absehbar, dass eine Änderung des ITSiG in absehbarer Zeit ansteht.

Da die Einführung des ITSiG für die vom Gesetz adressierten Institutionen und Unternehmen einen erheblichen finanziellen und bürokratischen Aufwand bedeutet, stellt sich hier die Frage nach der Angemessenheit des Gesetzes.

## 3.3 Für wen gilt das Gesetz?

Das ITSiG richtet sich an Einrichtungen/Betreiber „kritischer Sicherheitsstrukturen“. Hierbei ist zu Fragen, wo im Gesundheitswesen IT-Systeme als kritische Sicherheitsstruktur, deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Störungen der öffentlichen Sicherheit bedeuten, existieren.

### 3.3.1 Gematik

Als erstes fällt hierzu natürlich die sich in der Einführungsphase befindliche Infrastruktur der gematik ein. Sicherlich kann das damit verbundene System als eine entsprechende kritische Sicherheitsstruktur für die Versorgung angesehen werden.

### 3.3.2 Arztpraxis

In der Regel kann die medizinische Versorgung einer Arztpraxis in Deutschland jedoch von anderen Arztpraxen oder Krankenhäusern übernommen werden, so dass ein Versorgungsengpass nicht zu befürchten ist.

Der Ausfall einer einzelnen Arztpraxis könnte im Einzelfall sicherlich einen lokal begrenzten Versorgungsengpass bedeuten. Dies ist aber nur in einer Region zu befürchten, in welcher die ärztliche Versorgung auch mit dieser Arztpraxis nur notdürftig gewährleistet werden kann. Zudem ist der Ausfall der IT in der Arztpraxis in der Regel nicht Ursache dafür, dass in der Arztpraxis keine medizinische Versorgung mehr stattfinden kann.

Daher muss man davon ausgehen, dass Arztpraxen nicht die Normadressaten des ITSiG sind.

### 3.3.3 Krankenhäuser

Einzelne Versorgungsabläufe im Krankenhaus sind ohne IT heute kaum noch denkbar: diverse Verfahren in der Radiologie, OP-Planung, Planung der Strahlentherapie usw. können mit einem vollständigen Ausfall der Krankenhaus-IT nicht mehr gewährleistet werden.

Daher ist davon auszugehen, dass Krankenhäuser als Normadressaten des ITSiG gelten können.

### 3.3.4 Apotheker

Für die einzelne Apotheke gilt das zu den Arztpraxen gesagte.

Unklar ist, wie das Bestellwesen in den Apotheken organisiert ist. Sollte ein Bestellwesen zentral angreifbar sein und so die Versorgung durch die Apotheken insgesamt oder zumindest für einen Abschnitt des Landes beeinträchtigt werden können, so ist das ITSiG auch für Apotheken anwendbar.

### 3.3.5 Rettungsdienst

Der Rettungsdienst ist heute überwiegend sowohl bei der Einsatzplanung wie auch bei der Einsatzkoordinierung von der IT abhängig. Daher kann durch einen zentralen Ausfall der IT der Rettungsdienst ganzer Städte beeinträchtigt werden. Dahher ist das ITSiG auch auf den rettungsdienst anwendbar.

### 3.3.6 Weitere Leistungserbringer

Bugl. weiterer Leistungserbringer wie

- Ergotherapeuten,
- häuslicher Krankenpflege,
- Hebammen,
- Orthopädieschuhtechniker,
- Orthopädietechniker,
- Physiotherapeuten,
- Psychotherapeuten,
- Stimm-, Sprach-, Sprechtherapeuten (z.B. Logopäden, klin.Sprechwissenschaftler u.a.)

gilt überwiegend das zu den Arztpraxen gesagte, d.h. das ITSiG ist auf sie nicht anzuwenden.

# 4 GMDS: Was ist zu tun

Die Kommentierungsphase ist vorbei. Daher ist eine Kommentierung des Gesetzesentwurfs nicht mehr möglich.

Folgende Vorgehensweisen sind für die GMDS möglich:

1) Man kann jetzt entweder abwarten, ob das Gesetz verabschiedet wird und dann überlegen, was zu tun ist.
2) Man kann proaktiv tätig werden. Proaktiv heißt:
   [1] Definitionsfragen klären
   [2] Brancheninterne Standard bzgl. Mindestanforderungen zur IT-Sicherheit aufstellen
      a. „Branche Gesundheitswesen“ organisieren: neben GMDS
         i. bvitg
         ii. KH-IT
         iii. Krankenhausgesellschaft
         iv. (Hochschule, ggfs. Tool-Programmierung siehe unten)
         v. …?
      b. Kontaktperson BSI herausfinden
      c. Arbeitsgruppe bilden
      d. Standard „Gesundheitswesen“ erstellen, verabschieden und vom BSI anerkennen lassen.
      e. Evtl. Tool programmieren zur Unterstützung bei der Umsetzung (Hochschule als OpenSource-Projekt unter LGPL- oder Apache-Lizenz ?)

# 5 Empfehlung der AG

Vorgehen entsprechend Abschnitt 4 Ziffer 2)

# 6 Internet-Links zu den Textstellen

1) Gesetzesentwurf
   http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf?__blob=publicationFile
2) Bundesverband der Deutschen Industrie (BDI)
   http://www.bdi.eu/images_content/SicherheitUndVerteidigung/BDI_Stellungnahme_IT-Sicherheitsgesetz_final.pdf
3) Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM)
   http://www.bitkom.org/files/documents/BITKOM_Stellungnahme_IT-Sicherheitsgesetz.pdf
4) Bundesverband IT-Sicherheit e.V. (TeleTrusT)
   https://www.teletrust.de/uploads/media/2013-03-09-TeleTrusT-Stellungnahme_zu_Entwurf_IT-Sicherheitsgesetz.pdf
5) Bundesärztekammer
   http://www.bundesaerztekammer.de/downloads/Stellungnahme_der_Bundesaerztekammer_zu_Entwurf_eines_Gesetzes_zur_Erhoehung_der_Sicherheit_informationstechnischer_Systeme.pdf
6) Deutsches Institut für Normung e.V. (DIN)
   http://www.din.de/sixcms_upload/media/2896/KITS_N0149_Stellungnahme_des_DIN_zu_Referentenentwurf_eines_.149199.pdf
7) Verband der deutschen Internetwirtschaft eV. (eco)
   http://www.eco.de/wp-content/blogs.dir/positionspapier-it-sicherheit-in-der-18-wp.pdf
8) Verband Deutscher Kabelnetzbetreiber (ANGA)
   http://www.anga.de/media/file/709.ANGA_Stellungnahme_RefE_IT-Sicherheitsgesetz.pdf
9) EU-Richtlinienentwurf zur Informations- und Netzsicherheit(NIS)
   http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1666
10) Vorläufige Ausgabe der NIS-Direktive mit den jeweiligen Änderungen
    http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0244&language=DE

## 6.1 Weiterführende Links

1) BMI-Zusammenfassung der zentralen Eckpunkte des Gesetzentwurfs
   http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/eckpunkte_itsicherheitsgesetz.pdf;jsessionid=7D3AFA13CB9758142930547268414684.2_cid295?__blob=publicationFile