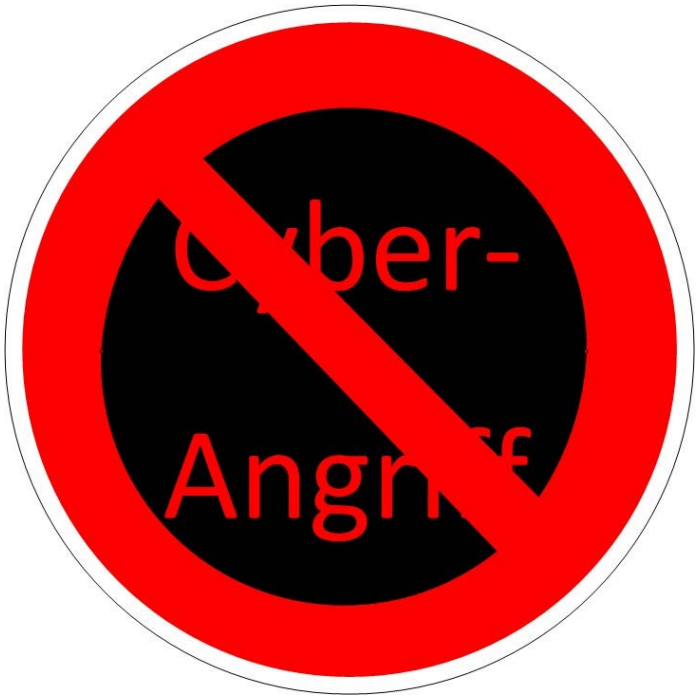


AUSWIRKUNGEN DES IT-SICHERHEITSGESETZES AUF KRANKENHÄUSER

Dr. Bernd Schütze

nrw.uniTS trifft Medizin - IT'S - YOUR RESPONSIBILITY!

22. September 2015

HEALTHCARE SOLUTIONS

DR. BERND SCHÜTZE

Studium

- Studium Informatik (FH-Dortmund)
- Studium Humanmedizin (Uni Düsseldorf / Uni Witten/Herdecke)
- Studium Jura (Fern-Uni Hagen)

Zusatz-Ausbildung

- Zusatzausbildung Datenschutzbeauftragter (Ulmer Akademie für Datenschutz und IT-Sicherheit)
- Zusatzausbildung Datenschutz-Auditor (TüV Süd)
- Zusatzausbildung Medizin-Produkte-Integrator (VDE Prüf- und Zertifizierungsinstitut)

Berufserfahrung

- 10 Jahre klinische Erfahrung
- 20 Jahre IT im Krankenhäusern
- 20 Jahre Datenschutz im Gesundheitswesen

Mitarbeit in wiss. Fachgesellschaften

- Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS)
- Gesellschaft für Datenschutz und Datensicherung e.V. (GDD)
- Gesellschaft für Informatik (GI)

Mitarbeit in Verbänden

- Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD)
- Berufsverband Medizinischer Informatiker e.V. (BVMI)
- Fachverband Biomedizinische Technik e.V. (fbmt)
- HL7 Deutschland e.V.

AGENDA

- (kurze) Historie des Gesetzes
- Was ist das: IT-Sicherheitsgesetz?
- Was ist die Zielsetzung des Gesetzes?
- An wen richtet sich das Gesetz?
- Was fordert das Gesetz?
- Unklarheiten, die durch das Gesetz entstanden sind
- Bin ich als Krankenhaus davon überhaupt betroffen?
- Fazit

HISTORIE DES GESETZES

- Februar 2011: Cyber-Sicherheitsstrategie beschlossen
- 07. 02.2013: EU-Kommission stellt Entwurf der „Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit“ (Cybersicherheitsrichtlinie) vor
- 12.03.2013: Bundesinnenminister Dr. Hans-Peter Friedrich stellt ersten Referentenentwurf vor
- 18.08.2014: Überarbeitung Entwurf vorgestellt
  (http://www.bmi.bund.de/DE/Nachrichten/Dossiers/ITSicherheit/itsicherheit_node.html)
- 17.12.2014: Bundeskabinett beschließt etwas geänderte Fassung
- 29.12.2015: Bundesregierung bringt Entwurf in die parlamentarischen Beratungen ein (Bundesrat Drucksache 643/14)
- 12. Juni 2015: Veröffentlichung Bundesanzeiger
  (http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf)
- 25. Juli 2015: in Kraft getreten

WAS IST DAS: IT-SICHERHEITSGESETZ?

- „Richtiger“ Name: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme
- Auffanggesetz, welches mehrere Gesetze ändert
  - BSI-Gesetz
  - Atomgesetz
  - Energiewirtschaftsgesetz
  - Telemediengesetz
  - Telekommunikationsgesetz
  - Bundesbesoldungsgesetz
    (Anpassung des Gehalts des Präsidenten des BSI)
  - Bundeskriminalamtsgesetz
  - Gesetz zur Strukturreform des Gebührenrechts des Bundes

WAS IST DIE ZIELSETZUNG DES GESETZES?

(QUELLE: DRUCKSACHE 18/5121 BUNDESTAG, GESETZESBEGRÜNDUNG)

- Defizite im Bereich der IT-Sicherheit sind abzubauen, insbesondere bei Betreibern „Kritischer Infrastrukturen“
- Ein Mindestniveau an IT-Sicherheit soll eingehalten werden
- Dem BSI sind IT-Sicherheitsvorfälle zu melden
- Betreiber Kritischer Infrastrukturen müssen branchenspezifische Sicherheitsanforderungen umsetzen

AN WEN RICHTET SICH DAS GESETZ?

- Betreiber Kritischer Infrastrukturen
- Telekommunikationsunternehmen
- Betreiber von Webangeboten
- (Bundesamt für Sicherheit in der Informationstechnik)

☝ Ausgenommen: Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG, d.h.

- es werden weniger als 10 Personen beschäftigt, dabei zählen folgende Personengruppen
  - Lohn- und Gehaltsempfänger
    (keine Azubis, aber Teilzeittätige entsprechend ihres Zeitrahmens)),
  - für das Unternehmen tätige Personen, die in einem Unterordnungsverhältnis zu diesem stehen und nach nationalem Recht Arbeitnehmern gleichgestellt sind,
  - mitarbeitende Eigentümer sowie
  - Teilhaber, die eine regelmäßige Tätigkeit in dem Unternehmen ausüben und finanzielle Vorteile aus dem Unternehmen ziehen
  - Partnerunternehmen sowie „Verbundene Unternehmen“ sind gemeinsam zu zählen
- der Jahresumsatz beträgt höchstens 2 Millionen € oder die Jahresbilanzsumme beträgt höchstens 2 Millionen €

AN WEN RICHTET SICH DAS GESETZ?
BETREIBER KRITISCHER INFRASTRUKTUREN

Bundesministerium des Inneren gliedert kritische Infrastrukturen in neun Sektoren mit entsprechenden Branchen, sieben Sektoren werden vom Gesetz adressiert:

1) Energie: Elektrizität, Gas, Mineralöl
2) Informationstechnik und Telekommunikation: Telekommunikation, Informationstechnik
3) Transport und Verkehr: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik
4) Gesundheit: Medizinische Versorgung, Arzneimittel und Impfstoffe, Labore
5) Wasser: Öffentliche Wasserversorgung, Öffentliche Abwasserbeseitigung
6) Ernährung: Ernährungswirtschaft, Lebensmittelhandel
7) Finanz- und Versicherungswesen: Banken, Börsen, Versicherungen, Finanzdienstleister
8) Medien und Kultur: Rundfunk (Fernsehen und Radio), gedruckte und elektronische Presse, Kulturgut, symbolträchtige Bauwerke
9) Staat und Verwaltung: Regierung und Verwaltung, Parlament, Justizeinrichtungen, Notfall-/ Rettungswesen einschließlich Katastrophenschutz

Quelle: BMI – Definition „Kritische Infrastrukturen“, online, verfügbar unter
http://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/BevoelkerungKrisen/Sektoreneinteilung.pdf?__blob=publicationFile

KRITISCHE INFRASTRUKTUR: GESUNDHEITSWESEN

Wahrscheinlich nicht betroffen

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

Möglicherweise betroffen

- Arztpraxen (Großpraxen)
- Rettungsdienst
- Krankenhäuser
- Pharmaindustrie
- gematik

WAS FORDERT DAS GESETZ?

- Pflicht zur Erfüllung von Mindestanforderungen an IT-Sicherheit nach dem Stand der Technik (§8a Abs.1 BSI-Gesetz)
- Mindestens alle 2 Jahre sind dem BSI eine Aufstellung der durchgeführten Sicherheitsaudits einschließlich der aufgedeckten Sicherheitsmängel zu übermitteln (§8a Abs. 3 BSI-Gesetz)
- Benennung von „Warn- und Alarmierungskontakten“ für das BSI (jederzeit erreichbar: 24 Stunden, 7 Tage, §8b Abs.3 BSI-Gesetz)
- Meldepflicht bzgl. „Beeinträchtigungen der informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der von ihnen betriebenen Kritischen Infrastruktur führen können“ (§8b Abs. 4 BSI-Gesetz)
- Meldepflicht bzgl. „erheblicher“ Sicherheitsmängel (§8b Abs. 4 BSI-Gesetz)

MINDESTANFORDERUNGEN AN IT-SICHERHEIT NACH DEM STAND DER TECHNIK

- Branchen können brancheninterne Standards entwickeln, welche das Bundesamt für die Sicherheit in der Informationstechnik (BSI) als Konkretisierung der gesetzlichen Verpflichtung anerkennen kann (§8a Abs. 2 BSI-Gesetz)
- KRITIS: Bundesamts für Bevölkerungsschutz und Katastrophenhilfe (BBK) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI)
  http://www.kritis.bund.de/
- Eine bei KRITIS genannte „kritische Infrastruktur“ ist das Gesundheitswesen
  - Definiert und analysiert „Schwachpunkte für die IT-Sicherheit im Gesundheitswesen
  - Erstellt Maßnahmenkatalog zur Beseitigung/Verhütung er erkannten Schwachstellen
  - Branchenspezifischer Standard für Gesundheitswesen in Arbeit
- Mitgliedschaft KRITIS
  - Aufnahme bei UP KRITIS erfolgt zunächst als Teilnehmer
  - Bei Wunsch zur aktiveren Mitarbeit kann eine Organisation dann Partner im UP KRITIS werden
  - Zusammenarbeit im UP KRITIS = zwei Formen
    - operativ-technischen Zusammenarbeit zwischen allen Teilnehmern des UP KRITIS
    - strategisch-konzeptionellen Zusammenarbeit in den eingerichteten Gremien

WEITERE REGELUNGEN IM GESETZ

- Diensteanbieter darf „zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen ... die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden“. (§100 Abs. 1 TKG)
- Diensteanbieter haben entspr. § 13 Abs. 7 TMG sicherzustellen (Zumutbarkeitsregelung),
  - Kein unerlaubter Zugriff auf für die Telemedien genutzten technischen Einrichtungen möglich
  - Telemedien sind gegen Verletzungen personenbezogener Daten und gegen Störungen (äußere Angriffe) geschützt
- Änderung BKAG erlaubt Ermittlungen ohne Anzeige betreffend
  - Ausspähen von Daten (§202a StGB),
  - Abfangen von Daten (§202 StGB),
  - Vorbereiten des Ausspähens und Abfangens von Daten (§202c StGB),
  - Computerbetrug (§263 StGB),
  - Datenveränderung (§303a StGB) sowie
  - Computersabotage (§303b StGB)

UNKLARHEITEN, DIE DURCH DAS GESETZ ENTSTANDEN SIND FEHLENDE DEFINITIONEN

Entwurf enthält viele Unklarheiten

- Für wen gilt das Gesetz? Wer betreibt eine „kritische Infrastruktur“?
- Unklare Begriffsbestimmungen wie bspw. „Stand der Technik“
- Unklarer Verwendungszweck der bei den geforderten Meldungen von Sicherheitsvorfällen angefallenen Daten
- Was ist als „Beeinträchtigung“ zu bewerten?
  Was als erhebliche Beeinträchtigung?
  - Hinweis: EU Cybersicherheitsrichtlinie verwendet und definiert Begriff „Ereignis“
- Was sind meldepflichtige „Sicherheitsmängel“?
  Was „erhebliche Sicherheitsmängel“?

UNKLARHEITEN, DIE DURCH DAS GESETZ ENTSTANDEN SIND RECHTLICHE FRAGEN

Offene rechtliche Fragen

- Pflicht zur Selbstanzeige, aber keine Befreiung bzgl. StGB, OWiG oder StPO wie sie im §42a BDSG („Informationspflicht“) vorhanden ist
- Einführung einer „Vorratsdatenspeicherung“
  - §100 Abs. 1 TKG erlaubt Speicherung von Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer
  - Speicherung rechtlich in Ordnung? Angesichts Urteile
    - ✓ Bundesverfassungsgericht (Urteil vom 02. März 2010, Az. 1 BvR 256/08) und
    - ✓ Europäische Gerichtshof (Urteil vom 08. April 2014. Az. C-293/12 und C-594/12)
- BKA kann bei Antragsdelikten §§ 202a, 202b, 202c StGB direkt ermitteln, d.h. Antrag muss nicht vorliegen:
  - kann BSI Meldungen an BKA weitergeben, woraufhin BKA ohne Rücksprache mit Betreiber ermittelt...?

UNKLARHEITEN, DIE DURCH DAS GESETZ ENTSTANDEN SIND DATENSCHUTZ?

- Gesetz beschreibt weder hinreichend genau was zu einer Meldung führt noch den Inhalt der jeweiligen Meldung
- Vorgaben zur Datensparsamkeit und dem Vorrang der Verwendung anonymer Daten, wenn möglich, entsprechend gesetzlicher Vorgabe des BDSG fehlt
- In Meldungen können somit – entsprechend Vorgaben des BSI –
  - Patientendaten
  - Mitarbeiterdaten

  enthalten sein
- Internationale Arbeiten wie beispielsweise Global Cyber Definitions Database zur Definitionsbildung im Gesetz ignoriert

BIN ICH ALS KRANKENHAUS DAVON ÜBERHAUPT BETROFFEN?

- §10 Abs. 1 BSI-Gesetz:
  „Das *Bundesministerium des Innern* bestimmt durch *Rechtsverordnung*, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung ... unter Festlegung der in den jeweiligen Sektoren im Hinblick auf § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrads, *welche Einrichtungen, Anlagen oder Teile* davon als *Kritische Infrastrukturen im Sinne dieses Gesetzes* gelten
- D.h., wer Betreiber einer kritischen Infrastruktur im Sinne des IT-Sicherheitsgesetzes ist, steht erst nach Rechtsverordnung fest

ABER

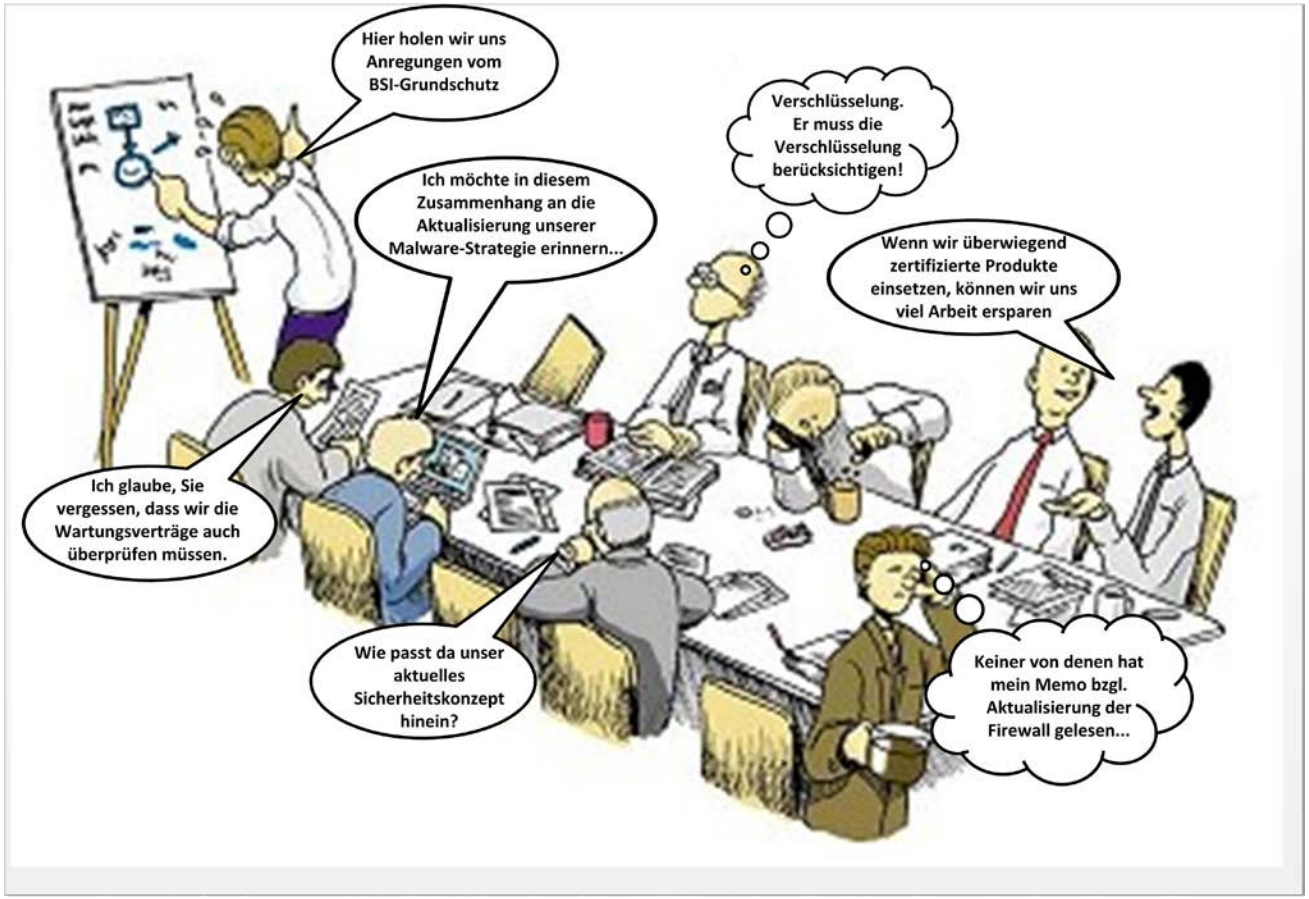
- Gesundheitsdaten gehören zu den Daten mit dem höchsten Schutzbedarf
- Wenn ein branchenspezifischer Standard das „Mindestniveau an IT-Sicherheit“ (Gesetzesbegründung) definiert
- und es zum Schadensfall kommt
- und ich als Krankenhaus diesen Standard nicht eingehalten habe
- ...

Letztlich wird der branchenspezifische Standard von allen Krankenhäusern umzusetzen sein

FAZIT

- **Für Betreiber Kritischer Infrastrukturen aus dem Bereich Gesundheitswesen gelten Regelungen wie Meldepflicht, Benennung Ansprechpartner usw. erst nach Inkrafttreten der Rechtsverordnung**
- **Pflicht zur Einhaltung von IT-Sicherheitsstandards (Stand der Technik) besteht erst zwei Jahre nach Inkrafttreten der Verordnung**
  - **Schwierigkeit:**
    - Hersteller an Erstellung Branchenstandard ausgeschlossen, d.h. Anforderung Herstellern erst nach Veröffentlichung bekannt
    - Evtl. notwendige technische Umsetzungen in Produkten damit nicht zwangsläufig innerhalb von 2 Jahren verfügbar
- **Cave Webangebot/Portallösung:**
  - **Geschäftsmäßige Telemedien-Anbieter müssen technische und organisatorische Maßnahmen nach dem Stand der Technik ergreifen, um sowohl unerlaubte Zugriffe auf ihre technischen Einrichtungen und Daten als auch Störungen zu verhindern**
  - **Und zwar mit Inkrafttreten des IT-Sicherheitsgesetzes**
  - **Geschäftsmäßig bedeutet dabei nicht zwangsläufig gewinnorientiert (Grundregel: besteht Impressumspflicht, gilt auch Anforderung ITSiG**
- **Verstöße gegen BSI-Gesetz: ggfs. Ordnungswidrigkeit (50.000 oder 100.000 € Sanktionsmöglichkeit)**
- **Aus haftungsrechtlichen Gründen werden alle Krankenhäuser den branchenspezifischen Standard umsetzen müssen** (er ist ja eh nur die „Minimalanforderung an die IT-Sicherheit...)

FRAGEN?



Kontakt: Bernd.Schuetze@T-Systems.com