Auswirkungen des IT-Sicherheitsgesetzes für Krankenhäuser

Umsetzungshinweise

DICOM 2015, Mainz, 20.06.2015

dubois it-consulting gmbh

dubois it-consulting gmbh, Holzhofstr. 10, 55116 Mainz, ☎ +49 6131 2150691 oder ☎+49 177 4104045, ✉ ingrid.dubois@dubois-it-consulting.de

Agenda

- Einleitung
- Informationssicherheits-Standards
- Sicherheitsmaßnahmen
- Audit / Überprüfung
- Umsetzungshinweise

Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Ziel des Gesetzes sind

- die **Verbesserung der IT-Sicherheit** von Organisationen,
- der verstärkte **Schutz der Bürgerinnen und Bürger im Internet**
- die dazu notwendige **Stärkung von BSI und BKA (**Bundeskriminalamt).

Besondere Bedeutung kommt im Bereich der IT-Sicherheit denjenigen Infrastrukturen zu, die **für das Funktionieren unseres Gemeinwesens zentral sind**.

Der **Schutz der IT-Systeme von solchen Kritischen Infrastrukturen und der für den Infrastrukturbetrieb nötigen Netze** ist daher von größter Wichtigkeit.

Betreiber kritischer Infrastrukturen

Organisationen aus den Bereichen

- **Energie,**
- **Informationstechnik und Telekommunikation,**
- **Transport und Verkehr,**
- **Wasser,**
- **Ernährung,**
- **Gesundheit,**
- **Finanz- und Versicherungswesen**

- (Staat und Verwaltung)
- (Medien und Kultur)

IT-Sicherheitsgesetz – Inhalt (ausgewählte Passagen)

Anforderungen

Betreiber Kritischer Infrastrukturen sind wegen der weitreichenden gesellschaftlichen Folgen, die ein Ausfall oder eine Beeinträchtigung ihrer Infrastrukturen nach sich ziehen kann, und ihrer insoweit besonderen **Verantwortung für das Gemeinwohl** zu verpflichten,

- ein **Mindestniveau an IT-Sicherheit einzuhalten**
- und dem BSI **IT- Sicherheitsvorfälle zu melden**.

Telekommunikationsanbieter, die eine Schlüsselrolle für die Sicherheit des Cyberraums haben, werden verpflichtet, IT-Sicherheit nach dem Stand der Technik nicht nur zum **Schutz des Fernmeldegeheimnisses** und zum **Schutz personenbezogener Daten**, sondern auch im Hinblick auf die **Verfügbarkeit ihrer Telekommunikations- und Datenverarbeitungssysteme** zu gewährleisten.

Aufklärung der Öffentlichkeit durch einen jährlichen Bericht.

Das BKA wird zur **Cyberkriminalitätsbekämpfung** in seinen Rechten gestärkt.

IT-Sicherheitsgesetz – Anforderungen

Erfüllungsaufwand allgemein (wenn für einzelne Sektoren nicht individuell geregelt)

- **Einhaltung eines Mindestniveaus an IT-Sicherheit**
  - generische und/oder branchenspezifische Anforderungskataloge
  - IT-Sicherheitskonzepte

- **Nachweis der Erfüllung durch Sicherheitsaudits**

- **Einrichtung und Aufrechterhaltung von Verfahren für die Meldung erheblicher IT-Sicherheitsvorfälle an das BSI**

- **Betreiben einer Kontaktstelle (24*7*365).**

Informationssicherheitsstandards

- **ISO/IEC 27000er-Serie**
  - **ISO/IEC 27001:2013** (Ausgabe von 2005 wird voraussichtlich Ende 2015 zurückgezogen)
    Information security management systems – Requirements
    Informationssicherheits-Managementsysteme – Anforderungen
  - **ISO/IEC 27002:2013** (Ausgabe von 2005 wird voraussichtlich Ende 2015 zurückgezogen)
    Code of practice for information security management
    (offizielle deutsch-sprachige Übersetzung noch nicht veröffentlicht)
  - **ISO/IEC 270xx**

- **Bundesamt für Sicherheit in der Informationstechnik (BSI)**
  - **BSI Standard 100-1**
    Managementsysteme für Informationssicherheit (ISMS)
  - **BSI Standard 100-2**
    IT-Grundschutz-Vorgehensweise
  - **BSI Standard 100-3**
    Risikoanalyse auf der Basis von IT-Grundschutz
  - **BSI Standard 100-4**
    Notfallmanagement
  - **IT-Grundschutzkataloge** (Baustein-, Maßnahmen-, Gefährdungskatalog)

- **...**

Informationssicherheit und zuverlässige KRITIS-Funktionen

Einflussfaktoren

- Gesetze
- Vorschriften
- Verträge
- Mögl. Gefahren
- Kunden
- Lieferanten
- Mitarbeiter
- Umfeld
- Technik
- ...

Betreiber einer kritischen Infrastruktur

Regelwerke

- ISO/IEC 27001
- Grundschutz*
- CObIT
- ISO 22301
- MaRisk
- ITIL
- ISO 9001
- PCI-DSS
- Techn. Richtl.
- ...

* ISO 27001 auf Basis von IT-Grundschutz

Nachweis der Einhaltung eines Mindestniveaus an IT-Sicherheit

Aufbau der ISO/IEC 27001:2013

- Grundlagen, Kapitel 0 – 3
  Einleitung, Anwendungsbereich, Normative Referenzen, Definitionen

- **Managementrahmen, Kapitel 4 – 10** (Verbindlich zu erfüllen für Zertifizierung*)
  - **Kontext der Organisation** (Kontext, Erfordernisse, Erwartungen, Anwendungsbereich, ISMS)
  - **Führung** (Verpflichtung, Politik, Rollen, Verantwortlichkeiten, Befugnisse)
  - **Planung** (Umgang mit Chancen und Risiken, Sicherheitsziele, Planung zu deren Erreichung)
  - **Unterstützung** (Ressourcen, Kompetenzen, Bewusstsein, Kommunikation, Dokumentierte Information)
  - **Betrieb** (Planung und Steuerung, Risikobeurteilung, Risikobehandlung)
  - **Bewertung der Leistung** (Überwachung, internes Audit, Managementbewertung)
  - **Verbesserung** (Nichtkonformität und Korrekturmaßnahmen, Fortlaufende Verbesserung)

- **Anhang A** (Verbindlich zu erfüllen für Zertifizierung**)
  - **Maßnahmenziele und Maßnahmen**

- Bibliografie

* ➔ Jedes Unternehmen, das eine ISO 27001 Zertifizierung erhalten will, muss nachweisen, dass sie alle diese Anforderungen erfüllt. **Ausschlüsse sind nicht zulässig.** (ISO/IEC 27001, Kapitel 1)

** ➔ Maßnahmen können nach Bedarf gestaltet und aus einer beliebigen Quelle ausgewählt werden. Für eine Zertifizierung ist – um zu überprüfen, dass keine erforderlichen Maßnahmen ausgelassen wurden – nachzuweisen, dass die festgelegten Maßnahmen mit denen in Anhang A abgeglichen wurden (ISO/IEC 27001, Kapitel 6.1.3 c))

Anforderungskatalog aus ISO/IEC 27001:2013, Anhang A

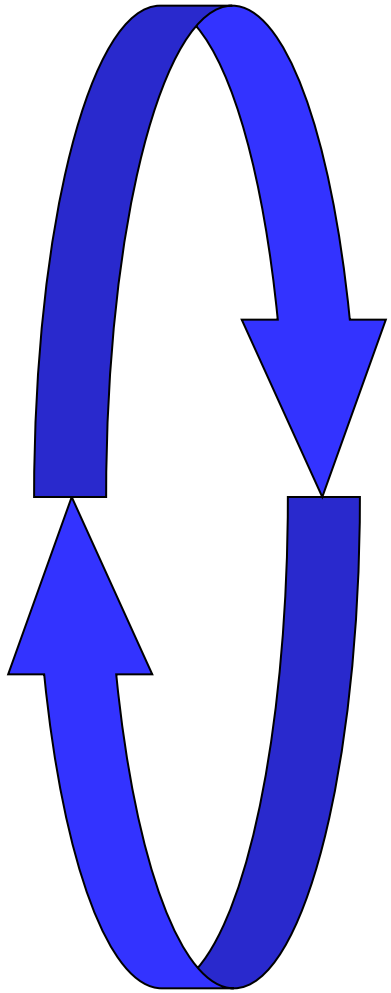
- Abschnitte mit Maßnahmen und Maßnahmenzielen
  - A.5 Informationssicherheitsrichtlinien
  - A.6 Organisation der Informationssicherheit
  - A.7 Personalsicherheit
  - A.8 Verwaltung der Werte
  - A.9 Zugriffssteuerung
  - A.10 Kryptographie
  - A.11 Physische und umgebungsbezogene Sicherheit
  - A.12 Betriebssicherheit
  - A.13 Netzwerksicherheitsmanagement
  - A.14 Anschaffung, Entwicklung und Instandhaltung von Systemen
  - A.15 Lieferantenbeziehungen
  - A.16 Management von Informationssicherheitsvorfällen
  - A.17 Informationssicherheitsaspekte des Business Continuity Managements
  - A.18 Compliance

- Jeder Abschnitt / jede Sicherheitskategorie enthält
  - das Ziel der Maßnahme(n)
  - eine oder mehrere Anforderung(en) und Maßnahme(n)

Die 14 Abschnitte des Anforderungskatalogs enthalten insgesamt 114 Maßnahmen

Vorgehensplan nach IT-Grundschutz

- **Initiieren des Sicherheitsprozesses**
  - **Strategie, Ziele, Informationsverbund festlegen**
  - **Leitlinie formulieren**
  - **Organisatorische Rahmenbedingungen schaffen**
- **Erstellen des Sicherheitskonzeptes**
  - **Strukturanalyse**
  - **Schutzbedarfsfeststellung**
  - **Modellierung und Maßnahmenauswahl**
  - **Basis-Sicherheits-Check**
  - **Ergänzende Sicherheitsanalyse**
    für Objekte mit hohem oder sehr hohem Schutzbedarf
  - **Risikoanalyse** (falls erforderlich)
  - **Konsolidieren der Sicherheitsmaßnahmen**
  - **Planung der Umsetzung**
- **Umsetzen des Sicherheitskonzeptes**
- **Aufrechterhalten und Verbessern des Sicherheitsniveaus**



BSI IT-Grundschutz: Schichten und Bausteine (14. Ergänzungslieferung, 2014)

BSI IT-Grundschutzkataloge, 14te Ergänzungslieferung – Schichten und Bausteine

Übergreifende Aspekte

B 1.0 Sicherheits-management	B 1.9 Hard- und Software Management
B 1.1 Organisation	B 1.10 Standardsoftware
B 1.2 Personal	B 1.11 Outsourcing
B 1.3 Notfallmanagement	B 1.12 Archivierung
B 1.4 Datensicherungs-Konzept	B 1.13 Sensibilisierung und Schulung
B 1.5 Datenschutz	B 1.14 Patch- & Änderungs-managmeent
B 1.6 Schutz vor Schadprogrammen	B 1.15 Löschen und Vernichten von Daten
B 1.7 Kryptokonzept	B 1.16 Anforderungs-management
B 1.8 Behandlung von Sicherheitsvorfällen	B 1.17 Cloud-Nutzung

Infrastruktur

B 2.1 Allgemeines Gebäude
B 2.2 Elektrotechnische Verkabelung
B 2.3 Büroraum, lokaler Arbeitsplatz
B 2.4 Serverraum
B 2.5 Datenträgerarchiv
B 2.6 Raum für technische Infrastruktur
B 2.7 Schutzschränke
B 2.8 Häuslicher Arbeitsplatz
B 2.9 Rechenzentrum
B 2.10 Mobiler Arbeitsplatz
B 2.11 Besprechungs-, Veranstaltungsraum
B 2.12 IT-Verkabelung

IT-Systeme

B 3.101 Allgemeiner Server	B 3.211 Client unter MAC OS X
B 3.102 Server unter Unix	B 3.212 Client unter Windows 7
B 3.107 S/390 und zSeries-Mainframe	B 3.301 Sicherheitsgateway (Firewall)
B 3.108 Windows Server 2003	B 3.302 Router und Switches
B 3.109 Windows Server 2008	B 3.303 Speicherlösungen / Cloud Storage
B 3.201 Allgemeiner Client	B 3.304 Virtualisierung
B 3.202 Allgemeines nicht vernetztes IT-System	B 3.305 Terminalserver
B 3.203 Laptop	B 3.401 TK-Anlage
B 3.204 Client unter UNIX	B 3.402 Faxgerät
B 3.208 Internet-PC	B 3.304 Mobiltelefon
B 3.209 Client unter Windows XP	B 3.405 Smartphones, Tables und PDAs
B 3.210 Client unter Windows Vista	B 3.406 Drucker, Kopierer, Multifunktionsgeräte

Netze

B 4.1 Heterogene Netze
B 4.2 Netz- und Systemmanagement
B 4.3 Modem
B 4.4 VPN
B 4.5 LAN-Anbindung e. Systems über ISDN
B 4.6 WLAN
B 4.7 VoIP
B 4.8 Bluetooth

Anwendungen

B 5.2 Datenträger-austausch	B 5.15 Allgemeiner Verzeichnisdienst
B 5.3 Groupware	B 5.16 Active Directory
B 5.4 Webserver	B 5.17 Samba
B 5.5 Lotus Notes / Domino	B 5.18 DNS-Server
B 5.6 Faxserver	B 5.19 Internet-Nutzung
B 5.7 Datenbanken	B 5.20 OpenLDAP
B 5.8 Telearbeit	B 5.21 Webanwendungen
B 5.9 Novell eDirectory	B 5.22 Protokollierung
B 5.12 Microsoft Exchange / Outlook	B 5.23 Cloud-Management
B 5.13 SAP System	B 5.24 Web-Services
B 5.14 Mobile Datenträger	B 5.25 Allgemeine Anwendung

IT-Sicherheitsgesetz – Anforderungen

Erfüllungsaufwand allgemein (wenn für einzelne Sektoren nicht individuell geregelt)

- **Einhaltung eines Mindestniveaus an IT-Sicherheit**
  - generische und/oder branchenspezifische Anforderungskataloge
  - IT-Sicherheitskonzepte

- **Nachweis der Erfüllung durch Sicherheitsaudits**

- **Einrichtung und Aufrechterhaltung von Verfahren für die Meldung erheblicher IT-Sicherheitsvorfälle an das BSI**

- **Betreiben einer Kontaktstelle (24*7*365).**

Umsetzungshinweise

- aufmerksam weitere Entscheidungen und Veröffentlichungen verfolgen
  - Sektorstudien, insbesondere die Sektorstudie Gesundheit
  - Verordnung(en), die das IT-Sicherheitsgesetz ergänzen

- für die Organisation kritische Bereiche / Aufgaben identifizieren
  - Abläufe, Geschäftsprozesse
  - Personal (intern/extern)
  - Dienstleister
  - IT-Technik: Systeme, Anwendungen, Dienste, Netze, Kommunikationskanäle
  - Gebäude, Infrastruktur

- Soll-Ist-Vergleich
  - Status von bereits umgesetzten Sicherheitsmaßnahmen erfassen
  - Status mit Anforderungen aus einem gängigen Sicherheitsstandard abgleichen
  - priorisierten Maßnahmenkatalog aufstellen, abstimmen, umsetzen

- Unterstützung durch Dritte
  - Planung
  - Umsetzung
  - Überprüfung

Weiterführende Informationen und Links

- **Bundesministerium des Inneren, Gesetzestexte, Sektorstudien**
  - www.bmi.bund.de
  - www.gesetze-im-internet.de
  - http://www.kritis.bund.de/SubSites/Kritis/DE/Publikationen/publikationen_node.html

- **Bundesamt für Sicherheit in der Informationstechnik (BSI)**
  - www.bsi.bund.de (homepage)
  - Seiten zum IT-Grundschutz: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html
  - BSI-Standards: .../ITGrundschutzStandards/ITGrundschutzStandards_node.html
  - Grundschutzkataloge: .../ITGrundschutzKataloge/itgrundschutzkataloge_node.html
  - Tools und Hilfsmittel: https://www.bsi.bund.de/DE/Themen/weitereThemen/GSTOOL/gstool_node.htm

- **Allianz für Cybersicherheit**
  - https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Home/startseite.html

- **Normen und Standards**
  - ISO: www.iso.org
  - Beuth-Verlag: www.beuth.de

- **Viele Informationen und Links rund um Sicherheit und Datenschutz**
  - www.secupedia.info
  - www.datenschutz.de