

## **IT-Sicherheitsstandards im Gesundheitssektor – Entwicklungen und Besonderheiten**

IT-Sicherheitsnormen und -standards haben in den letzten Jahren zunehmend ihre Nützlichkeit bei der Schaffung sicherer IT-Systeme belegt. Das Vordringen der Informationstechnologie im Gesundheitssektor führt zwangsläufig zu einer wachsenden Bedeutung der IT-Sicherheit. Dadurch wird die IT-Sicherheitsproblematik in den Institutionen des Gesundheitswesens ebenfalls zunehmend wichtiger. Hierzu gibt es seit einiger Zeit eine Norm - die „ISO/IEC 27001-27799 IT-Sicherheit im Gesundheitswesen“. Mit Hilfe dieser Norm ist es den Institutionen leicht möglich, eine Planung, Umsetzung, Kontrolle und Verbesserung der IT-Sicherheit vorzunehmen und diese in den Institutionen - Kliniken, Krankenhäuser, medizinische Versorgungszentren - effizient und umfassend normenkonform zu gestalten. Im Folgenden wird gezeigt, wie sinnvoll mit der betreffenden Norm umzugehen und welcher praktische Nutzen aus ihrer Anwendung zu ziehen ist.

### **1. Entwicklungen im Gesundheitswesen als Grundlage für IT-Sicherheitsbedürfnis**

Der Medizinsektor ist durch eine hohe Dynamik auf dem Gebiet der Informationstechnik IT und – hierdurch bedingt – der IT-Sicherheitstechnik gekennzeichnet: Eine Vielzahl von Entwicklungen führt dazu, dass eine große Anzahl von Funktionen in der ärztlichen Praxis, in Kliniken, medizinischen Versorgungszentren MVZ und Heimen computergestützt oder voll computerisiert abgewickelt und dass insbesondere das gesamte, bisher auf Karteikarten, Papier und anderen Medien wie Filmen geführte Aktenwesen zunehmend mehr digitalisiert wird. Bei der Umsetzung dieser Entwicklungen entstehen eine Vielzahl von IT-Sicherheits- und Datenschutzproblemen sowie Ordnungsmäßigkeitsfragen, die gelöst werden müssen.

- |   |
|---|
| <ol style="list-style-type: none"><li>1. Vollelektronische Abrechnung</li><li>2. Einführung der elektronischen Gesundheitskarte</li><li>3. Zunehmende Digitalisierung von Patientenakten</li><li>4. Digitale Aufzeichnung von durchgeführten Diagnosen</li><li>5. Digitale Übermittlung von Diagnosedaten</li><li>6. Digitale Archivierung von Akten, Berichten und Bildaufzeichnungen</li><li>7. Vernetzung von bisher allein stehenden Systemen und Arbeitsplatz-PCs in z.B. einer Arztpraxis</li><li>8. Vernetzung von Systemen in unterschiedlichen Lokationen (z.B. Kliniksystemen, Arztpraxen und MVZ etc.)</li></ol> |
|---|

Abb. 1: Technologische Entwicklungen im Gesundheitssektor

Eine andere Frage ist die Entwicklung des Sicherheitsbedürfnisses. Hier sind zwei Kategorien von Sicherheitsansprüchen zu unterscheiden und zwar

- vom und beim medizinischen Personal sowie
- bei Patienten.

Die Beschäftigten des Gesundheitssektor werden in ihren Sicherheitsansprüchen einerseits durch die berufsständisch fundierten Sicherheitsbedürfnisse wie zum Beispiel Geheimhaltung von Patientendaten, Sicherung der ärztlichen Schweigepflicht und Ähnliches motiviert, andererseits durch Ordnungsmäßigkeitsansprüche wie Richtigkeit/Integrität von Daten, Verfügbarkeit zu Zeitpunkten der Behandlung wie aber auch nach erfolgter Archivierung beeinflusst. Eng hiermit zusammenhängen auch die Befolgung von Datenschutzerfordernungen, die allerdings im Verständnis der Mitarbeiter des Gesundheitswesens oft durch die Befolgung der berufsständischen Regelungen „erledigt“ werden.

Patienten richten ihre Ansprüche an sichere Systeme häufig stärker an den formalen Anforderungen des Datenschutzes aus, wobei sie voraussetzen, dass die sicherheitsspezifischen Bedingungen wie Integrität und Verfügbarkeit nicht diskutiert zu werden brauchen, da sie selbstverständlich erfüllt sein müssen. Der Datenschutz hingegen - der in vielen Punkten in der Realität mit der Befolgung der Regeln der ärztlichen Schweigepflicht zusammenhängt - nimmt in seiner Bedeutung und in seinem Stellenwert ständig zu, obwohl die damit zusammenhängenden konkreten Maßnahmen in den meisten Fällen eher diffus bleiben. So ist die Anzahl und Qualität der Anfragen von Betroffenen/Patienten an die Institutionen eher gering und meist wenig substantiiert.

## **2. IT-Sicherheitsmanagementnormen und ihre Scopes**

Auf dem Gebiet der IT-Sicherheit sind in den letzten Jahren eine Vielzahl von Normen von Normungsgremien und Arbeitsgruppen entwickelt und verabschiedet worden. Diese sind zum Teil technischer Natur, beschäftigen sich demnach mit der Normung von Hardware sowie kryptografischen Verfahren, zum Teil mit dem Problem des IT-Sicherheitsmanagements und haben hier unterschiedliche Ansätze und Schwerpunkte. Bei diesen sicherheitsmanagementorientierten Normen handelt es sich vor allem um:

- ISO/IEC 27001:2005 auf Basis der Ursprungsnorm ISO 17799/BS 7799
- ISO 27001 auf Basis Grundschutz
- ISO/IEC 27002, praxisorientierter Leitfaden (Code of practice) zur Norm ISO 27001
- Spezifische Scopes zur ISO/IEC 27001 (Prototypenschutz, Gesundheitswesen).

Da der Gesundheitssektor durch die IT-technischen Entwicklungen bedingt besondere Bedeutung erlangt hat, soll im Folgenden speziell auf die Inhalte der diesbezüglichen Norm eingegangen werden.

### **Grundlage für Anforderungen auf dem Sektor der IT-Sicherheit im Gesundheitswesen: ISO/IEC-Norm 27799 als Scopespezialisierung der ISO 27001-02<sup>1</sup>**

Die neue Norm ISO/IEC-Norm 27799 als Scopespezialisierung der ISO 27001-02 setzt neue Maßstäbe für Institutionen des Gesundheitssektors. Hier sind die Institutionen wie Kliniken, Verbände, medizinische Versorgungszentren und Praxisgemeinschaften dazu aufgerufen, ihre IT-Systeme so zu gestalten, dass sie Anforderungen an die Sicherheitstechnik und -organisation erfüllen. Programmsysteme zur Abwicklung von Prozessen auf dem Medizinsektor sind in das organisatorische Umfeld eingebettet und sind unabdingbar Bestandteil der gesamten IT-Organisation.

Hiermit werden an die IT-Sicherheit völlig neue Anforderungen gestellt. Die bewährten Normen und Standards auf dem Gebiet der IT-Sicherheit - wie ISO/IEC 27001-02 sind im Prinzip branchenunabhängig auf das Problemfeld ISMS (Informationssicherheitsmanagementsysteme) ausgerichtet, wobei bei einer Auditierung und Zertifizierung die spezifischen Eigenheiten des Gesundheitswesens zu berücksichtigen sind. Dies ändert die Spezialnorm ISO 27799 „Gesundheitswesen“. Im Folgenden ist die Struktur der Norm aufgeführt; dabei stehen die kursiven Kapitel als spezielle Regelungen besonders im Vordergrund.

---

<sup>1</sup> Quelle: Medizinische Informatik – Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002 (ISO 27799:2008); Deutsche Fassung EN ISO 27799:2008

### 3. Die Norm ISO 27799 Gesundheitswesen

Die Norm ISO 27799 sollte als Spezifizierung der Ursprungsnorm ISO/IEC 27002 (Code of Practice) gewertet werden. Es ist daher insbesondere für den im Umgang mit IT-Sicherheitsnormen wenig erfahrenen Mitarbeiter sinnvoll, sich zusätzlich mit der Ursprungsnorm zu beschäftigen.

#### **Gliederung der Norm DIN EN ISO 27799:2008-10 (D)**

Medizinische Informatik - Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002 (ISO 27799:2008); Deutsche Fassung EN ISO 27799:2008

#### Inhalt

Vorwort

Einleitung

1 Anwendungsbereich

1.1 Allgemeines

1.2 Ausschlüsse aus dem Anwendungsbereich

2 Normative Verweisungen

3 Begriffe

3.1 Begriffe aus dem Gesundheitswesen

3.2 Begriffe aus dem Bereich der Informationssicherheit

4 Abkürzungen

5 Sicherheit von Gesundheitsinformationen

5.4 Zu schützende Gesundheitsinformationen

5.5 Bedrohungen und Schwachstellen der Sicherheit von Gesundheitsinformationen

6 Praktischer Arbeitsplan für die Umsetzung der ISO/IEC 27002

6.1 Systematik der Normen ISO/IEC 27002 und ISO/IEC 27001

6.2 Engagement des Managements bei der Umsetzung der ISO/IEC 27002

6.3 Einrichten, betreiben, pflegen und verbessern des ISMS

6.4 Planen: Einführen des ISMS

6.5 Ausführen: Umsetzen und Betreiben des ISMS

6.6 Überprüfen: Überwachen und Überprüfen des ISMS

6.7 Handeln: Pflegen und Verbessern des ISMS

7 Folgerungen aus ISO/IEC 27002 für die Gesundheitsversorgung

7.1 Allgemeines

7.2 Leitlinie zur Informationssicherheit

7.3 Organisation der Informationssicherheit

7.4 Management organisationseigener Werte

7.5 Personalsicherheit

7.6 Physische und umgebungsbezogene Sicherheit

7.7 Betriebs- und Kommunikationsmanagement

7.8 Zugriffskontrolle

7.9 Beschaffung, Entwicklung und Wartung von Informationssystemen

7.10 Umgang mit Informationssicherheitsvorfällen

7.11 Informationssicherheitsaspekte beim Management zur Aufrechterhaltung des Geschäftsbetriebs

7.12 Einhaltung von Vorgaben

Anhang A (informativ) Bedrohungen der Sicherheit von Gesundheitsinformationen

Anhang B (informativ) Aufgaben und zugehörige Dokumente des Informationssicherheits-Managementsystems

Die Struktur der Prüfgebiete zeigt klar, dass die Grundlage der ISO 27002 für das Gesundheitswesen modifiziert aber nicht verlassen wurde. Hiermit eröffnet sich die Chance für Unternehmen des Gesundheitssektors ihr ISMS normgerecht zu gestalten und sich gemäß einer international anerkannten Norm auditieren und zertifizieren zu lassen.

Die Norm enthält - und das ist für die praktische Arbeit mit ihr besonders wertvoll - darüber hinaus in den nicht gesundheitswesensspezifischen Kapiteln eine Vielzahl von Anregungen, zum Beispiel für die Struktur von Dokumentationen, die in dieser Form in dem Code of Practice, der ursprünglichen ISO 27002, nicht enthalten sind.

Die in ihr entwickelten Vertiefungen für das Gesundheitswesen sollen an zwei Beispielen erläutert werden und zwar am Beispiel des Umgangs mit Informationen und der Bedrohung der Sicherheit von Informationen, wobei im Kapitel 7 der Norm die Struktur einer Unterscheidung zwischen „Maßnahmen“ und „Anleitung zur Umsetzung“ ziemlich konsequent durchgehalten wurde.

#### **7.4.2.2 Kennzeichnung von und Umgang mit Informationen**

##### **Maßnahme**

Alle medizinischen Informationssysteme, die persönliche Gesundheitsinformationen verarbeiten, **sollten** die Benutzer über die Vertraulichkeit der persönlichen Gesundheitsinformationen, die über das System zugänglich sind, informieren (z. B. beim Start oder beim Log-in) und **sollten** Hardcopy-Ausgaben als vertraulich kennzeichnen, wenn diese persönliche Gesundheitsinformationen enthalten.

##### **Anleitung zur Umsetzung**

Nicht alle Gesundheitsinformationen sind vertraulich und nicht alle medizinischen Informationssysteme ermöglichen den Benutzern den Zugriff auf persönliche Gesundheitsinformationen. Benutzer von medizinischen Informationssystemen müssen wissen, wann die Daten, auf die sie zugreifen, persönliche Gesundheitsinformationen enthalten.

Beispiel: Umgang mit Informationen (Auszug aus Kap. 7 der ISO 27799 Gesundheitswesen)

#### **12. Zufällige Fehlleitungen**

Zu dieser Bedrohung zählt die Möglichkeit, dass die über ein Netzwerk gesendeten Informationen zu einer falschen Adresse geleitet werden. Zufällige Fehlleitungen könnten auf ein Versagen bei der Nutzerausbildung oder auf ein Versagen bei der Pflege der Integrität von Verzeichnissen von Gesundheitsdienstleistern (oder auf beides) hindeuten.

Beispiel: Bedrohung der Sicherheit von Informationen (Auszug aus Anhang A der ISO 27799 Gesundheitswesen)

Wenn keine spezifischen Anmerkungen notwendig sind, enthält die Norm z. B. den Hinweis:

#### **7.10.2.1 Verantwortlichkeiten und Verfahren**

Keine ergänzende Anleitung für das Sicherheitsmanagement im Gesundheitswesen.

Die zitierten Beispiele zeigen, dass die Norm sich bemüht, die spezifischen Eigenheiten der IT-Sicherheit im Gesundheitswesen herauszuarbeiten. Dies ist insofern wichtig, da nach den Erfahrungen im Gesundheitssektor IT-Sicherheitsprobleme oft durch mangelnde Qualifikation und geringes Verständnis für die informationstechnologischen Lösungen entstehen: Ärzte und Praxispersonal sind im allgemeinen keine IT-Fachleute.

## **4. Praktischer Einsatz und Anwendungsnutzen**

Das Einrichten, Betreiben, Pflegen und Verbessern des ISMS wird auch in dieser Norm analog zu der generell üblichen Lösung der Strukturierung von Managementsystemen in Form des so genannten PDCA-Zyklus dargestellt.

Die vier Unterabschnitte bieten eine Anleitung zum Einrichten und nachfolgenden Betreiben eines ISMS im Umfeld des Gesundheitswesens. Dies erfordert eine zyklische Abarbeitung von Aktivitäten. Sie werden in der Norm im Anhang B. im Detail dargestellt und sind stark an

den generell üblichen Vorgehensweisen ausgerichtet. Allerdings sei darauf hingewiesen, dass die ISO 27799 deutliche Ergänzungen zu der Ursprungs-/Bezugsnorm ISO 27002 aufweist und damit selbst für den Kenner der Ursprungsnorm wertvolle Ergänzungen enthält, wobei der spezifische Bezug zum Gesundheitswesen deutlich geringer ausgeprägt ist.

Dies verringert nicht den Nutzen für die Gestaltung sicherer IT-Systeme. Wenn ein Verantwortlicher im Gesundheitswesen ein ISMS planen betreiben kontrollieren und verbessern soll, sollte er sich vor allem dann, wenn zu einem späteren Zeitpunkt eine Zertifizierung geplant ist, an den Basisnormen ISO/IEC 27001 und 27002 orientieren.

Selbst wenn von der Voraussetzung ausgegangen werden kann, dass die Norm durch ihre Allgemeingültigkeit auch durchaus des Öfteren für den Spezial- und Einzelfall nicht relevante Inhalte aufweist, ist bei den genannten Prozessen des Aufbaus und Betriebens eines ISMS der Effizienzerhöhungs- und Rationalisierungseffekt so groß, dass es sich kaum ein Verantwortlicher leisten kann, auf die Orientierung an den Normen zu verzichten.

## **5. Zertifizierung der IT-Sicherheit im Gesundheitssektor**

### **IT-Sicherheit vs. Datenschutz**

IT-Sicherheit und Datenschutz sind untrennbar miteinander verbunden. Ordnungsgemäße IT-Systeme im Sinne des Datenschutzes können nicht ohne die technischen Maßnahmen zur IT-Sicherheit erstellt und betrieben werden. Im Hinblick auf die Sensitivität der in solchen Systemen verarbeiteten Daten ist es unerlässlich, Datenschutzgeprüfte und -gesiegelte Systeme in größerem Umfang einzusetzen da nur diese eine Gewähr dafür bieten, eine dem Stand der Technik angemessene IT-Sicherheit realisiert zu haben. Da Institution des Gesundheitswesens die Einhaltung der Datenschutzgesetzgebung eher als lästiges Übel betrachten, sollten die Hersteller so viel wie möglich dafür tun, nur solche Systeme einzusetzen, die als "sicher und/oder ordnungsgemäß" anerkannt sind.

### **Stand der Zertifizierung**

Da Zertifizierungen/Gütesiegel grundsätzlich zu veröffentlichen sind, kann nachgeprüft werden, welche auf dem Markt befindlichen Systeme über die Anerkennung der Kassenärztlichen Bundesvereinigung KBV hinaus Zertifizierungen oder Gütesiegel erworben haben.

Zweifellos bildeten die von der KBV in regelmäßigen Abständen veröffentlichten Zulassungslisten für verschiedene Hard- und Softwareprodukte (so zum Beispiel für Telematikgeräte und die elektronische Gesundheitskarte) Ansätze, um dem Qualitätsgedanken auf diesem Sektor Vorschub zu leisten. Sie sind jedoch auf Grund ihrer Konzentration auf ein enges Gebiet nicht geeignet, umfassendere Zertifizierungen und Gütesiegel im dargestellten Sinne zu ersetzen.

Die typische Eigenart dieser Programme auf dem Anwendungssektor Gesundheitswesen, insbesondere ihrer Abrechnungsrelevanz, führt dazu, dass sie in ihrer Gesamtheit von der KBV erfasst werden. Systeme, die anerkannt werden, müssen bestimmte, von der KBV festgelegte Qualitätskriterien erfüllen, die jedoch im Sinne von Ordnungsmäßigkeitsanforderungen der Norm nur wenige IT-Sicherheitskriterien beinhalten.

Die Bundesärztekammer und die kassenärztliche Bundesvereinigung haben im Jahre 2008 Empfehlungen zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis veröffentlicht. Hierin sind unter anderem rechtliche, technische und organisatorische Orientierungshilfen bei der Umsetzung von Datenschutz und Datensicherheit in der Praxis enthalten. Die Empfehlungen stellen eine Anzahl von außerordentlich wichtigen Maßnahmen zusammen, die in Bezug auf eingesetzte Hardware, Software und Organisationslösungen dazu beitragen, Datenschutz und IT-Sicherheit in Arztpraxen/Institutionen des Gesundheitswesens zu realisieren. Sie stellen allerdings keine Grundlage dar, aufgrund derer es möglich wäre, eingesetzte Systeme in ihren Einsatzumfeld zu prüfen und gegebenenfalls zu zertifizieren.

Die Anzahl der mit einem Zertifikat oder Gütesiegel gem. Norm versehenen Produkte auf

dem Gesundheitssektor geht im Hinblick auf die Vielzahl der eingesetzten Programme sowie der faktisch zur IT-Sicherheit verpflichteten Institutionen gegen Null.

## **6. Vorbild Niederlande: NEN 7510 – IT-Sicherheit im niederländischen Gesundheitswesen**

Die niederländische Norm NEN 7510 hat im Prinzip die gleiche Zielsetzung wie die deutsche/internationale Norm: Anders ist, dass sie hierzu die Grundlagen durch eine starke Normierung der Auditierungsvorgänge, der zu prüfenden Inhalte sowie eine Vielzahl von verweisenden Hinweisen auf andere, die IT-Sicherheit im Gesundheitswesen regelnden Normen und Vorschriften enthält. Zu diesem Zweck wurde in den Niederlanden ein Handbuch entwickelt, welches mit einem Umfang von 126 Seiten insbesondere eine gute Unterstützung für die zu zertifizierenden Institutionen liefert. Die derzeit vorliegenden Informationen über bereits erfolgte Zertifizierungen konnten nicht verifiziert werden. Ihnen zufolge ist die Zertifizierung gemäß der niederländischen Norm erheblich weiter fortgeschritten als in Deutschland gemäß der ISO/IEC 27001-02.

## **7. Fazit**

Die neue Norm „ISO 27799 Gesundheitswesen“ bietet den Institutionen des Gesundheitswesens eine solide Grundlage um die IT-Sicherheitssysteme normenkonform gestalten zu können. Der Vorteil einer Ausrichtung an der Norm liegt vor allem in der Rationalisierung der durchzuführenden Aktivitäten.

Bei der Tendenz, Zertifikate zur Grundlage normenkonformer Systemgestaltung im Gesundheitswesen zu machen, dient die Befolgung der Anforderungen der Norm aber auch dazu, eine Institution auf eine mögliche Zertifizierung vorzubereiten und damit bestätigt zu bekommen, dass das IT-Sicherheitssystem ordnungsgemäß ist und in seinen Merkmalen nach dem „State of the Art“ gestaltet wurde. Allerdings sind zurzeit noch keine ISO-zertifizierten Systeme bekannt.