

4 Informationssicherheitsmanagement als Basis für eine erfolgreiche Digitalisierung im Gesundheitswesen

Thomas Jäschke und Jan Domnik

Die Lage der Informationssicherheit im Gesundheitswesen ist unzureichend und dem Aspekt geschuldet, dass sie im Branchenvergleich unterdurchschnittlich fortgeschritten ist. Zahlreiche, erfolgreiche Angriffe von Erpressungstrojanern haben Datenschützern und IT-Sicherheitsverantwortlichen bereits die Augen geöffnet – geändert hat sich bisher wenig und dennoch existiert die fortschreitende Digitalisierung des Gesundheitswesens. Eine Kombination, die im schlimmsten Fall die existierende, hiesige Lücke zwischen Informationssicherheit und technologischem Fortschritt weiter vergrößert und erst zu spät sichtbar macht, dass unsere Lücken in der Informationssicherheit zu groß geworden sind, als dass wir sie zufriedenstellend wieder schließen könnten.

Bedeutung und Stellenwert von ISMS für die Digitalisierung

Die Bedeutung der IT-Sicherheit ist abhängig von deren Bedeutung für die Gesellschaft (BSI 2016, S. 55). Der besonders hohe Stellenwert des Gesundheitswesens in der Gesamtbevölkerung ist unumstritten. Neben der Gewährleistung der Notfallversorgung, gilt es zudem, die Sicherung der Grundversorgung zu gewährleisten. Was das Gesundheitswesen bei einer immer älter werdenden Gesellschaft immer wieder vor neue Herausforderungen stellt. Ein Gegenwarts- und weiterwachsendes Zukunftsszenario, das ohne eine funktionierende IT-Infrastruktur nicht mehr vorstellbar ist. Umso mehr verwundert es, dass die Budgets der IT-Verantwortlichen im Verhältnis zu anderen Branchen eher gering ausfallen (Deutsches Ärzteblatt 2009). Neben einem geringen IT-Budget hat der Verantwortliche für die Informationstechnologien heute besonders

auch mit der Komplexität seiner IT-Systeme zu kämpfen. Diese hohe Komplexität führt dazu, dass vom Endanwender und teilweise bis hin zum IT-Verantwortlichen, kaum noch jemand weiß, wie die IT im Detail eigentlich funktioniert. Beide Aspekte führen dazu, dass IT im Gesundheitswesen ein zunehmend beliebtes Einfallstor für Angreifer im Gesundheitswesen wird, um die hierdurch entstehenden Sicherheitslücken auszunutzen und hoch sensible und schützenswerte Daten von Patienten abzugreifen oder durch Verschlüsselung die Daten unbrauchbar zu machen und die Institutionen damit zu erpressen. Die Sorge, über den Verlust von Daten wächst und das zu recht. Die Hackerszene ist ein schnelllebiges Markt, der den Herstellern von Anti-Virus Software immer einen Schritt voraus ist, und auf Einrichtungen trifft, die gänzlich unvorbereitet, ohne Notfallmanagement oder Backups, sind.

Beschreibung des Transformationsprozesses (oder diese Transformation muss das ISMS vollziehen)



Sicherheitslücken sind häufig bekannt.

Während auf Ebene des Vorstands oftmals noch das Bild vom unaufhaltsamen und elitären Hacker vorherrscht, können Administratoren offene Sicherheitslücken ihrer Systeme i. d. R. klar benennen. Mit einem gewissen Maß an Zynismus wird dabei oft festgestellt, dass nicht verwunderlich sei, dass einfachste Angriffe auf IT-Infrastrukturen so oft erfolgreich verlaufen. Viel verwunderlicher sei hingegen, dass Angriffe so selten passieren (Jäschke u. Domnik 2016).

Probleme sowie Risiken sind demnach auf operativer Ebene häufig bekannt, allerdings aufgrund fehlender monetärer und personeller Ressourcen nicht änderbar. Der Versuch, Sicherheitslücken durch Firewalls und Antiviren Software entgegen zu wirken, ist zwar schön, löst aber nicht das Grundproblem einer mangelnden Strategie für das IT-Sicherheitsmanagement.

Die Informationssicherheitsstrategie stellt das Fundament des Informationssicherheitskonzeptes in dokumentierter Form dar. An erster Stelle steht dabei ein definier-



Abb. 1 Bestandteile einer umfassenden Sicherheitspolitik

ter Leitfaden – die Policy (s. Abb. 1), welche die Strategie beschreibt und die Basis für die Arbeit des Informationssicherheitsbeauftragten (ISB) bildet. Dieses wird in der Regel durch ein Dokument ergänzt, welches zentrale Komponenten des IT-Sicherheitsprozesses definiert. Darunter folgen dann Konzepte, Regelungen und Richtlinien sowie Arbeitsanweisungen, welche für die Mitarbeiter des Unternehmens bindend sind. Auch Foliensammlungen zur Schulung von Mitarbeitern finden hier ihren Platz.

Exkurs – Die Rolle des Informationssicherheitsbeauftragten

Die Aufgaben des ISB weichen je nach Größe und Aufbau einer Organisation stark voneinander ab. In größeren Institutionen nimmt der ISB eher eine koordinierende Rolle ein. In kleineren Institutionen erledigt der Informationssicherheitsbeauftragte – falls vorhanden – dagegen oft lediglich einen Aufgabenbereich, den er neben dem Alltagsgeschäft ausführt.

Die benötigten zeitlichen und monetären Ressourcen für die Tätigkeit eines Informationssicherheitsbeauftragten wachsen mit der Größe, der Komplexität und natürlich der Schutzwürdigkeit der Daten einer Unternehmung.

Bei der Wahrnehmung seiner Aufgaben beeinflusst der ISB oftmals unmittelbar die IT-Strategie des Unternehmens und steht in enger Abstimmung mit den dafür verantwortlichen Stellen. Sämtliche Konzepte, Regelungen und Richtlinien, Arbeitsanweisungen, usw. werden vom Informationssicherheitsbeauftragten nicht nur erlassen, sondern auch aktiv weiterentwickelt und ergänzt. Darüber hinaus werden sie regelmäßig auf Compliance, Aktualität und Anwendbarkeit hin überprüft.

In der Vergangenheit haben sich im Informationssicherheitsmanagement (ISMS) zwei Standards etabliert.

Informationssicherheitsmanagement nach ISO/IEC 27001 Norm

- Hauptaugenmerk liegt auf der Implementierung eines Informationssicherheitsprozesses.
- Umfang ist vergleichsweise gering. Auf rund 20 Seiten werden die Anforderungen der 114 Maßnahmen aufgeführt.
- Generischer Ansatz und
- Geschäftsrisikobasierter Ansatz.

Dieser Ansatz ist konkret von Experten für den Einsatz im Unternehmen entwickelt worden und beschreibt den PDCA-Zyklus, der durch einen Verantwortlichen (Informationssicherheitsbeauftragter) koordiniert werden soll. Dieser sorgt dafür, dass eine Strategie zum Erhalt der Informationssicherheit implementiert wird und für das Risikomanagement die Basis bildet.

Für den Auditor, der das Unternehmen zertifiziert, gilt in der Regel, dass Maßnahmen zu genannten Themenfeldern umgesetzt werden. Die konkrete Maßnahmenausgestaltung obliegt in der Regel dem Unternehmen, solange diese plausibel begründet werden können.

Informationssicherheitsmanagement nach BSI Grundschutz

- Gefährdungspotenziale sind bereits vorgegeben, nur in Ausnahmefällen ist eine eigene Bewertung nötig.
- Umfang mit mehreren 1000 Seiten ist nicht praktikabel.

Beim BSI Grundschutz handelt es sich um einen deutschen Standard, der bereits konkrete Handlungsanweisungen vorgibt. Aufgrund des Umfangs ist die Praxistauglichkeit allerdings fraglich, da eine Umsetzung im Rahmen des Maßnahmenkatalogs mit einem enormen Aufwand verbunden ist. Nicht zuletzt ist bei der Auditierung nach BSI Grundschutz der Fall gegeben, dass mehr Auditoren im Markt unterwegs sind als auditierte Unternehmen existieren. Nichtsdestotrotz kann ein ISMS in Anlehnung an den BSI Grundschutz sinnvoll sein und ähnliche Ergebnisse wie die ISO-Standard bringen. Nachfolgend sind die Unterschiede beider Ansätze grafisch aufgeführt (s. Abb. 2).

Wirkliche IT-Sicherheitsexperten denken sich keine eigenen Vorgehensmodelle aus, sondern arbeiten auf etablierten Standards und passen diese auf ihre individuellen Belange an.

Die Zertifizierung kann sehr kosten-, ressourcen- und zeitintensiv sein. Sollte dies in Ermangelung ausreichend hoher Budgets, in Anbetracht der Unternehmensgröße oder des verfügbaren Personals nicht leistbar sein, sollte ein ISMS in Anlehnung an einem der etablierten Standard durchgeführt werden und auf eine Zertifizierung, so

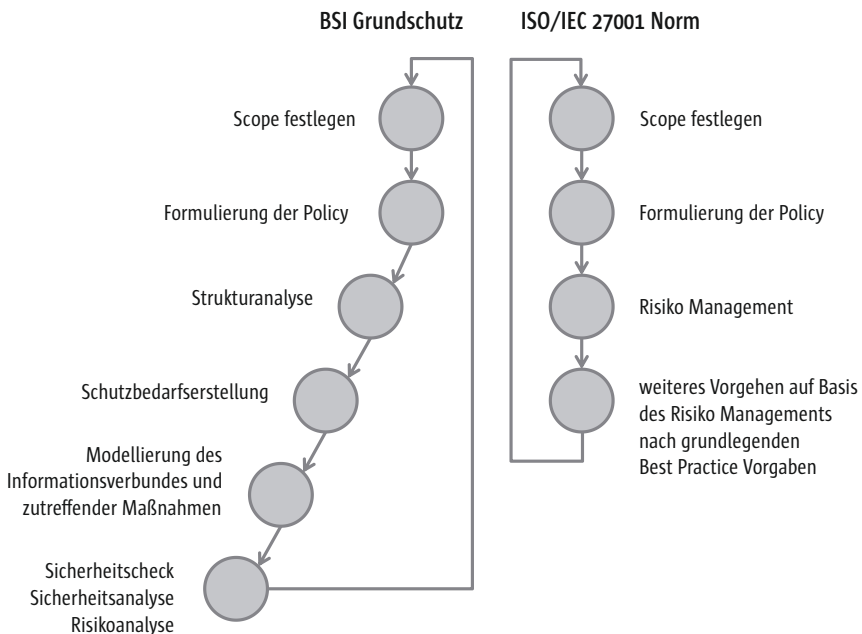


Abb. 2 Grobe Beschreibung ISMS nach BSI Grundschutz/ISO/IEC 27001 Norm (DATATREE 2017)

diese nicht zwingend (gesetzlich oder aus Vertragsanforderungen) notwendig ist, verzichtet werden.

Grob betrachtet sind vier Schritte notwendig, um ein ISMS erfolgreich zu implementieren:

- **Schritt 1: Planung**
 - Innerhalb des Planungsprozesses gilt es die Zuständigkeiten und den Hauptverantwortlichen festzulegen. Dies sollte in der Regel der ernannte Informationssicherheitsbeauftragte sein, welcher sich anschließend um die Risikoanalyse und Bewertung für die relevanten Bereiche kümmert. Aufgrund des hohen Abstimmungsbedarfs mit anderen Abteilungen, bietet sich hier die Analyse und Evaluierung in Form eines Workshops an. Anschließend muss die Planung der Risikobehandlung vorgenommen werden und zusammen mit der Geschäftsleitung der konkrete Umgang mit möglichen Restrisiken geklärt werden.
- **Schritt 2: Durchführung**
 - Innerhalb der Durchführungsphase ist ein konkreter Problembehandlungsplan zu erstellen, aus dem konkrete Handlungsmaßnahmen und deren Umsetzung aufgeführt sind. Da es für ein funktionierendes ISMS nicht ausreichend ist eine Strategie zu entwickeln, bedarf es ebenso der Sensibilisierung und Schulung der Mitarbeiter.
- **Schritt 3: Überprüfung**
 - Nach Umsetzung ist die Wirksamkeit der durchgeführten Maßnahmen zu überprüfen. Hierzu eignen sich beispielsweise interne Audits.
- **Schritt 4: Evaluierung**
 - Um eine kontinuierliche Optimierung des ISMS herbeiführen zu können, ist eine Erfolgskontrolle durchzuführen. Sollten Maßnahmen nicht den geplanten Erfolg verzeichnen, gilt es diese zu korrigieren und zu optimieren.

Fazit

Der Handlungsbedarf innerhalb der IT-Sicherheit ist enorm groß, angesichts der fortschreitenden und unaufhaltsamen Digitalisierung im Gesundheitswesen. Hierzu existieren anerkannte Standards, die jedoch selten ohne Anpassungen übernommen werden können. Insbesondere für kleine Unternehmen ist dies schwierig, weshalb sich ein pragmatischer Ansatz in Anlehnung an Standards durchgesetzt hat. Insbesondere diese Einrichtungen sind gut beraten, wenn sie sich z.B. in der Planungsphase externer Unterstützung bedienen.

Literatur

- Bundesamt für Sicherheit in der Informationstechnik (BSI) (2016) Die Lage der IT-Sicherheit in Deutschland 2016. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5 (abgerufen am 22.05.2017)
- Deutsches Ärzteblatt (2009) IT-Sicherheit im Gesundheitswesen: Budgets unzureichend. URL: <https://www.aerzteblatt.de/archiv/65744/IT-Sicherheit-im-Gesundheitswesen-Budgets-unzureichend> (abgerufen am 22.05.2017)
- Jäschke T, Domnik J (2016) Der Informationssicherheitsbeauftragte, In: Jäschke T (Hrsg.) Datenschutz im Gesundheitswesen, MWV Medizinisch Wissenschaftliche Verlagsgesellschaft, Berlin, S. 115–121