Leitfaden für die Erstellung eines IT-Sicherheitskonzeptes

Eine Zusammenarbeit von

Bundesverband Gesundheits-IT e. V.

Arbeitsgruppe „Datenschutz und IT Sicherheit“

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V. (GMDS)

Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“

ZTG Zentrum für Telematik und Telemedizin GmbH (ZTG)

Autoren (alphabetisch)

Isele, Christoph	Cerner Deutschland GmbH
Kaufmann, Pierre	Agfa HealthCare GmbH
Schütze, Dr. Bernd	Deutsche Telekom Healthcare and Security GmbH
Spyra, Gerald	Kanzlei Spyra
Treinat, Lars	ZTG Zentrum für Telematik und Telemedizin GmbH
Wiedemann, Matthias	
Wichterich, Eric	ZTG Zentrum für Telematik und Telemedizin GmbH

Stand: 29.09.2017

Inhaltsverzeichnis

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Copyright

Für in diesem Dokument veröffentlichte, von den Autoren selbst erstellte Objekte gilt hinsichtlich des Copyrights die folgende Regelung:

D. h., Sie dürfen:

- Teilen: das Material in jedwedem Format oder Medium vervielfältigen und weiterverbreiten
- Bearbeiten: das Material remixen, verändern und darauf aufbauen

und zwar für beliebige Zwecke, sogar kommerziell. Der Lizenzgeber kann diese Freiheiten nicht widerrufen solange Sie sich an die Lizenzbedingungen halten.

Die Nutzung ist unter den folgenden Bedingungen möglich:

- Namensnennung: Sie müssen angemessene Urheber- und Rechteangaben machen, einen Link zur Lizenz beifügen und angeben, ob Änderungen vorgenommen wurden. Diese Angaben dürfen in jeder angemessenen Art und Weise gemacht werden, allerdings nicht so, dass der Eindruck entsteht, der Lizenzgeber unterstütze gerade Sie oder Ihre Nutzung besonders.
- Weitergabe unter gleichen Bedingungen: Wenn Sie das Material remixen, verändern oder anderweitig direkt darauf aufbauen, dürfen Sie Ihre Beiträge nur unter derselben Lizenz wie das Original verbreiten.
- Keine weiteren Einschränkungen: Sie dürfen keine zusätzlichen Klauseln oder technische Verfahren einsetzen, die anderen rechtlich irgendetwas untersagen, was die Lizenz erlaubt.

Im Weiteren gilt:

- Jede der vorgenannten Bedingungen kann aufgehoben werden, sofern Sie die Einwilligung des Rechteinhabers dazu erhalten.

Diese Lizenz lässt die Urheberpersönlichkeitsrechte unberührt.

Um sich die Lizenz anzusehen, gehen Sie bitte ins Internet auf die Webseite:

https://creativecommons.org/licenses/by-sa/4.0/deed.de

bzw. für den vollständigen Lizenztext

https://creativecommons.org/licenses/by-sa/4.0/legalcode

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

> Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Im folgenden Text werden daher, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.

Warum eigentlich ein IT-Sicherheitskonzept?

Management Summary

Die Digitalisierung in der Gesundheitsversorgung nimmt immer stärker zu, „eHealth“ wird vom deutschen und auch vom europäischen Gesetzgeber immer stärker gefordert und gefördert. Daher wird auch die Sicherheit der eingesetzten informationstechnischen Verfahren, d. h. die „IT-Sicherheit“, immer wichtiger für die Akteure der Gesundheitsversorgung: die elektronische Daten der Patientinnen und Patienten müssen sicher verarbeitet werden, was sowohl die Nutzung in der Patientenbehandlung beinhaltet als auch den Austausch dieser Daten zwischen den verschiedenen Akteuren.

Dabei müssen die Handlungen nachvollziehbar sein. Denn nur wenn bzgl. der Verarbeitung der Patientendaten größtmögliche Transparenz herrscht, kann das für die Versorgung nicht hoch genug einzuschätzende Vertrauen der Patientinnen und Patienten gewonnen werden. Zur Gewährleistung der IT-Sicherheit ist daher die Nutzung eines IT-Sicherheitskonzept unabdingbar. Nur wenn jeder an der Verarbeitung beteiligte weiß, wie die Sicherheit der Daten bei der Verarbeitung zu gewährleisten ist, kann die IT-Sicherheit auch „gelebt“ werden. Das IT-Sicherheitskonzept stellt somit einen der wichtigsten Bausteine bei der IT-Nutzung in der Gesundheitsversorgung dar.

Dabei darf IT-Sicherheit nicht als einmal abgearbeiteter Punkt verstanden werden. IT-Sicherheit ist, ebenso wie die Qualitätssicherung in der Patientenversorgung, ein „lebender“ Prozess: Ständig muss überprüft werden, ob das einmal festgelegte noch zur gelebten Wirklichkeit passt. Es muss überprüft werden, ob die einmal festgelegten Maßnahmen zur Gewährleistung der IT-Sicherheit noch ausreichend sind oder ob die Maßnahmen basierend auf neuen Erkenntnissen oder neuen Technologien angepasst werden müssen. Kurz: Auch IT-Sicherheit stellt einen Demingkreis bestehend aus den Komponenten „Plan – Do – Check – Act“ dar.

Die Umsetzung eines IT-Sicherheitskonzeptes verursacht dabei natürlich Aufwand und Kosten. Da es sich bei der IT-Sicherheit um einen Prozess handelt, sind dies auch keine einmaligen Ausgaben, sondern müssen im jährlichen Haushalt entsprechend budgetiert werden. Dabei sollte man nicht vergessen, dass gerade die Einführung von Maßnahmen andere Kosten verursachen kann, als die Erhaltung eines Status Quo. Denn gerade bei der Einführung von IT-Sicherheitsmaßnahmen kann es vorkommen, dass evtl. vorhandene Prozesse geändert und angepasst werden müssen. Dies bedingt letztlich den Einsatz verschiedener Ressourcen und bedeutet somit auch einen finanziellen Aufwand.

Dieser Leitfaden wurde verfasst, um die Erstellung eines IT-Sicherheitskonzeptes zu erleichtern. Er besteht aus drei Teilen:

1) Eine Einleitung, in der die Zielsetzung genauer beschrieben wird (Seite 1-9)
2) Teil 1 des Leitfadens, welcher den Aufbau und die Struktur eines IT-Sicherheitskonzeptes erläutert (Seite 10-16)
3) Teil 2 des Leitfadens, welcher Umsetzungshinweise bzgl. der Umsetzung der in Teil 1 dargestellten Anforderungen bietet (Seite 17-52)

Wir sind davon überzeugt, dass dieser Leitfaden darin unterstützt, IT-Sicherheit in der Patientenversorgung zu „leben“.

1 Einleitung

Information hat sich im Rahmen des ökonomischen Strukturwandels in fast allen Industrienationen zum vierten Produktionsfaktor neben Arbeit, Kapital und Boden entwickelt. Die Wertschöpfung verlagert sich in vielen Unternehmen von der Produktion hin zur Dienstleistung. Im Dienstleistungssektor Gesundheitswesen entscheiden die Informationen zu einem Patienten über dessen Wohlergehen: bei der Patientenbehandlung ist deshalb insbesondere die Gewährleistung von Verfügbarkeit und von Integrität der notwendigen Informationen essenziell.

Um den notwendigen Schutz gewährleisten zu können, ist es wesentlich, die Risiken, die mit dem Einsatz von IT einhergehen, zu erkennen und entsprechend steuern zu können. In der Folge ist auch das Erkennen und Steuern von Risiken, die sich im Zusammenhang mit dem Produktionsfaktor Information ergeben, unabdingbar. Insofern kommt dem Risikomanagementprozess eine bedeutende Aufgabe für das gesamte Unternehmen zu. Eine wichtige Rolle spielt dabei die unternehmenseigene IT-Abteilung.

Da die IT als Infrastruktur eine immer wichtigere Rolle bei der Gesundheitsversorgung einnimmt und die meisten Geschäftsprozesse mit IT abgebildet werden, handelt derjenige, der eine Verarbeitung personenbezogener Gesundheitsdaten ohne ein entsprechendes IT-Sicherheitskonzept vornimmt, zumindest fahrlässig, wenn nicht sogar grob fahrlässig. Dieses kann im Ernstfall nicht unerhebliche Haftungskonsequenzen nach sich ziehen.

Doch auch wenn man ein IT-Sicherheitskonzept als grundlegende Voraussetzung zum konstruktiven Ansatz zur Gewährleistung von „IT-Sicherheit“ ansieht, ist oftmals nicht klar, was in ein solches Konzept eigentlich alles hineingehört bzw. wie man ein solches sinnvollerweise, auf die eigene Institution zugeschnitten, entwickelt. Ferner ist oft nicht bekannt, wie bzw. nach welchen Kriterien die wesentlichen technischen und organisatorischen Maßnahmen gruppiert bzw. beschrieben werden sollen.

Zwar gibt es gängige Methoden, um ein Informationssicherheitsmanagementsystem einzurichten und ein IT-Sicherheitskonzept zu erstellen, um dadurch die IT-Sicherheit zu gewährleisten, doch fokussieren diese auf unterschiedliche Gegebenheiten, die oftmals in manchen ihrer Forderungen nicht wirklich auf die Anforderungen des Gesundheitswesens oder die Größenordnung des zu schützenden IT-Systems passen. So umfassen die IT-Grundschutzkataloge des BSI über 5000 Seiten, während ISO 27001 zwar wenige Seiten umfasst, dafür jedoch verhältnismäßig abstrakt bleibt und ISIS12 für Einrichtungen mit überwiegend normalem Schutzbedarf gedacht ist.

Der vorliegende Leitfaden ist deshalb so konzipiert, dass er bezogen auf die Anforderungen des Gesundheitswesens, praxisorientiert bei der Erstellung eines IT-Sicherheitskonzepts eine entsprechende Hilfestellung geben soll. Wie die Verfasser sich den Aufbau und Struktur eines IT-Sicherheitskonzeptes vorstellen, wird genauer im Abschnitt „Teil 1: Aufbau und Struktur eines IT-Sicherheitskonzeptes“ beschrieben. Dementsprechend sieht der grundsätzliche Aufbau eines diesem Leitfaden folgenden IT-Sicherheitskonzeptes wie folgt aus:

Kapitel 1	Zusammenfassung/Management Summary
Kapitel 2	Einleitung mit Darstellung der Ziele des IT-Sicherheitskonzeptes
Kapitel 3	Begriffsbestimmungen
Kapitel 4	Administrativa
Kapitel 5	Überblick bzgl. Zuständigkeiten, usw.

Kapitel 6 Darstellung der Rahmenbedingungen
Kapitel 7 Beschreibung der Systemarchitektur
Kapitel 8 Darlegung des Schutzbedarfs
Kapitel 9 Anzuwendende Vorgaben
Kapitel 10 Anforderungen
Kapitel 11 Implementierungsvorgaben
Kapitel 12 Darlegung der Restrisiken
Kapitel 13 Beschreibung der Kontrolle und Fortschreibung des IT-Sicherheitskonzeptes
Kapitel 14 Mitgeltende Unterlagen.

Im Abschnitt „Teil 2: Umsetzungshinweise“ werden weiterführende Informationen angeboten, z. B. Beschreibung von Akteuren, Begriffsbestimmungen und weiterführende Literatur.

2 Zielsetzung des Leitfadens

Dieser Leitfaden soll besonders Einrichtungen, Institutionen und auch Organisationen des Gesundheitswesens - unabhängig davon, ob sie im Bereich der Gesundheitsversorgung oder Gesundheitsforschung tätig sind - bei der Erstellung eines IT-Sicherheitskonzeptes unterstützen. Dabei geht es in erster Linie darum aufzuzeigen, wie ein IT-Sicherheitskonzept nach Auffassung der Verfasser strukturell beschaffen sein sollte. D.h. der Leitfaden bietet eine Übersicht über den Aufbau des IT-Sicherheitskonzeptes.

2.1 Abgrenzung

IT-Sicherheit kann nur selten auf der Basis eines einmal erstellten Konzeptes gewährleistet werden, da sich oft die genutzten Werkzeuge und die möglichen Angriffe über die Zeit verändern. Eine regelmäßige Anpassung leistet am besten ein IT-Sicherheitsmanagementsystem. Ein IT Sicherheitsmanagementsystem kann in Umfang und Detailtiefe der Komplexität des Projektes bzw. der Organisation angepasst werden. Das IT-Sicherheitskonzept enthält wichtige Grundzüge, die in einem IT-Sicherheitsmanagementsystem weiter ausgeführt und präzisiert werden

Dieser Leitfaden dient jedoch nicht der Erläuterung, wie ein Informationssicherheits-Managementsystem eingeführt oder betrieben werden sollte. Hierzu gibt es hervorragende Ausarbeitungen, z. B. ISO/IEC 27001ff. Es geht auch nicht darum, möglichst viele Maßnahmen (technischer und organisatorischer Art), die man treffen könnte, vorzustellen. Auch hierzu finden sich diverse Anleitungen, insbesondere beim BSI[1].

Das IT-Sicherheitskonzept beschreibt die grundsätzliche Motivation, welche Güter mit welcher Priorität zu schützen sind, während ein Informationssicherheitsmanagementsystem in Zyklen die kontinuierlichen Verbesserungsprozesse lebt und auf die laufenden Änderungen sowohl in der eingesetzten Technik als auch bei den Bedrohungen reagiert.

2.2 Abgrenzung der Begriffe Datenschutz und IT-Sicherheit

Da die Umsetzung des IT-Sicherheitskonzeptes zwangsläufig Aufwand und Kosten verursachen wird, sollte man planvoll und effizient vorgehen. Insbesondere gilt es zu vermeiden, dass das „Rad immer wieder neu erfunden wird“. Von daher bietet es sich an, so viel wie möglich aus anderen Konzepten, Dokumenten aus der Organisation in das IT-Sicherheitskonzept mit einfließen zu lassen. Insbesondere aus dem Datenschutzkonzept[2] lassen sich einige Aspekte/Herangehensweisen übertragen. Jedoch gilt es, sich dabei auch immer die Unterschiede zwischen „Datenschutz“ und IT-Sicherheit vor Augen zu führen und entsprechend in den Konzepten Rechnung zu tragen.

So geht es beim Datenschutz um den Schutz der informationellen Selbstbestimmung des Menschen, dessen Daten verarbeitet werden sollen. Aufgrund des Risikos, das mit einer Verarbeitung dieser Daten einhergeht, gilt es nach den datenschutzrechtlichen Prinzipien so wenig Daten wie irgend möglich von so wenig natürlichen oder juristischen Personen zu verarbeiten. „Angreifer“ auf die Daten kann aus Sicht des Datenschutzes jeder außer der betroffenen Person sein. Damit natürlich

[1] Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge. [Online, zitiert am 2015-12-09]; Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html

[2] „Leitfaden zur Erstellung eines Datenschutzkonzeptes“. [Online, zitiert am 2017-05-12]; Verfügbar unter https://gesundheitsdatenschutz.org/doku.php/gmds-dgi-empfehlungen

auch das Unternehmen auch selber, das für die Verarbeitung der Daten des Betroffenen verantwortlich ist.

Bei der IT-Sicherheit geht es hingegen darum, die aus Sicht eines Unternehmens wertvollen Daten zu schützen. Schützenswerte Daten können auch personenbezogene Daten sein. Aus Unternehmenssicht sind aber auch andere, nicht-personenbezogene Daten schützenswert wie etwa Forschungsergebnisse. Diese gilt es, aufgrund ihres Wertes für das Unternehmen, unbedingt vor ungewollten (unbefugten) Zugriffen zu schützen. Aus Sicht des Unternehmens kann deshalb jeder der Angreifer sein. Daher ist es durchaus auch möglich, dass aus Sicht der IT-Sicherheit auch die betroffene Person, deren Daten verarbeitet werden, als „Angreifer“ betrachtet werden muss.

Die technischen und organisatorischen Maßnahmen um Daten zu schützen, können dabei sowohl im Datenschutz als auch in der IT-Sicherheit ähnlich bzw. oftmals sogar identisch sein, der Unterschied liegt in den verschiedenen Schutzzielen.

Neben den Überschneidungen der beiden Bereiche gibt es aber auch Bereiche, in denen die Informationssicherheit und der Datenschutz in einen Interessenkonflikt geraten (können). Ein Beispiel für einen entsprechenden Interessenkonflikt ist das Speichern von Protokolldaten, also den Informationen, wer sich wann an welchem Computer anmeldete und was wer zu welchen Zeiten getan hat. Aus Sicht der IT-Sicherheit will man, um etwaige Angriffe etc. umfassend nachvollziehen zu können, am besten so viele Daten wie nur möglich verarbeiten und diese für die Untersuchung zukünftiger Sicherheitsvorfälle unbegrenzt aufbewahren. Allerdings beinhalten derartige Protokolldaten zwangsläufig personenbezogene Daten. Aus datenschutzrechtlichen Gründen ist eine „unendliche“, vollumfassende Speicherung ggfs. nicht legitim. Der Grundsatz der „Speicherminimierung“ führt darüber hinaus dazu, dass diese Daten so kurz wie nur möglich aufbewahrt und damit so frühestmöglich gelöscht werden müssen.

Dementsprechend beinhalten Datenschutz- und IT-Sicherheitskonzept teilweise ähnliche Angaben, jedoch mit unterschiedlichen Blickwinkeln und Schutzbereichen.

Teil 1: Aufbau und Struktur eines IT-Sicherheitskonzeptes

1 Zusammenfassung/Management Summary

Hier erfolgt eine übersichtsartige Darstellung der Gesamtlösung, wobei die Zusammenfassung den Umfang einer Seite nicht übersteigen soll. Es geht darum, einen Überblick über die Sicherheitsarchitektur zu erhalten, d.h. was wird aus welchen Gründen wie geschützt.

2 Einleitung

Die Einleitung sollte in aller Kürze die Intention des IT-Sicherheitskonzeptes vorstellen. Die Einleitung soll die folgenden Fragen beantworten:

- Wie nenne ich die Organisationseinheit bzw. das Projekt?
- Worum geht es? Was ist aus welchen Gründen vor wem zu schützen?
- Wer ist für was verantwortlich?
- Gibt es weitere Beteiligte?
- Welche Aufgaben erfüllen die Parteien?
- Was sind die typischen Verfahren, die im geschützten Raum durchgeführt werden sollen?

Es geht dabei in der Einleitung nicht um eine möglichst detaillierte Darstellung, vielmehr soll ein Überblick geboten werden, worum es in dem IT-Sicherheitskonzept geht.

2.1 Ziele des Sicherheitskonzeptes

- Darstellung von Ziel und Zweck des Konzeptes (Kurzbeschreibung)
  Es geht in diesem Abschnitt nicht darum, die Ziele und Zwecke des Konzeptes vollständig zu beschreiben, sondern in einleitenden Worten einen Eindruck zu vermitteln, worum es in diesem Konzept geht. D.h. es werden so kurz wie möglich insbesondere die folgenden Punkte angesprochen und dargestellt:
  - Authentizität
    Wer sind die Kommunikationspartner?
    Wie wird die Identität sichergestellt?
  - Datenintegrität
    Wird gewährleistet, dass Daten bei einer Übertragung nicht verfälscht werden können?
    Wird gewährleistet, dass jede Verfälschung zuverlässig erkannt wird?
  - Gewährleistung der Vertraulichkeit
    Ist sichergestellt, dass niemand außer den berechtigten Empfängern die Daten zur Kenntnis nehmen kann? (Einsatz Kryptografie)
  - Verfügbarkeit
    Ist gewährleistet, dass die Infrastruktur für autorisierte Benutzer jederzeit verfügbar ist?
  - Nichtabstreitbarkeit
    Ist die Urheberschaft der Daten beweisbar?
    Ist der Versand und der Empfang der Daten inklusive der Zeitangaben, Sender und Empfänger beweisbar?
  - Originalität

Ist sicher erkennbar, aus welcher Quelle de Daten stammen?
Ist sicher erkennbar, wann die Daten erzeugt wurden?

3 Begriffsbestimmungen

Hier werden die Fachtermini dargestellt, die im IT-Sicherheitskonzept verwendet werden. Bei der Erstellung sollte man daran denken, dass das Konzept nicht notwendigerweise nur von IT-Sicherheitsfachleuten gelesen wird. Daher sollten hier großzügig Begrifflichkeiten erklärt werden, damit möglichst wenig Missverständnisse beim Verständnis des IT-Sicherheitskonzeptes aufkommen.

Der Leitfaden enthält eine Reihe von Vorschlägen für Begriffsbestimmungen (siehe zweiter Teil dieser Ausarbeitung, Kapitel 1 Begriffsbestimmungen auf Seite 18), welche einerseits die Darstellung der Begriffsbestimmungen im eigenen IT-Sicherheitskonzept erleichtern, andererseits auch dafür sorgen sollen, dass aus dem Fachbereich der IT-Sicherheit vorhandene Begriffe einheitlich genutzt werden.

4 Überblick

Im Überblick wird der Informationsverbund (Organisation, Institution, Unternehmen) kurz vorgestellt und die wahrgenommenen Aufgaben sowie die Zuständigkeiten/Verantwortlichkeiten dargestellt. Wenn es nicht bereits in der Einleitung beschrieben wurde, sollte hier die Abgrenzung dargestellt werden, wer innerhalb des durch das IT-Sicherheitskonzept geschützten Bereichs (vgl. Kapitel 2 „Einleitung“: „zu schützendes IT-System“) arbeitet und welche Stakeholder/Partner außerhalb sind.

4.1 Informationsverbund

- Wer gehört zum Informationsverbund?
- Wer nimmt im Informationsverbund welche Aufgaben wahr?

4.2 Zuständig- und Verantwortlichkeiten

- Wer ist Ansprechpartner für inhaltliche (fachlich, technische) Fragen bei der Anwendung?

4.3 Gültigkeit und Verbindlichkeit des Dokuments

- Von wem wurde das Dokument wann in Kraft gesetzt? Wie lange gilt das Dokument?
- Für wen gilt es wo unter welchen Umständen (sachlicher und räumlicher Anwendungsbereich)?
- Für welche Teile der Organisation und Zielobjekte gilt es?

5 Rahmenbedingungen

Grundsätzlich benötigen Sicherheitsmaßnahmen Ressourcen. Zugleich verursachen Sicherheitsmaßnahmen bei Anwendern oftmals einen höheren Aufwand, als wenn dieselbe Arbeit ohne Sicherheitsmaßnahmen erfolgen würde. Z.B. könnte ein Bauarbeiter schneller auf die Baustelle gehen und mit der Arbeit beginnen, wenn auf die Sicherheitskleidung verzichtet würde. Das Grundprinzip „Sicherheit kostet Geld“ gilt auch für die IT-Sicherheit. Ein IT-Sicherheitskonzept kostet Ressourcen und damit Geld, die Integration in die tägliche Arbeit verursacht eine Anpassung des Arbeitsablaufs und damit deutlichen Aufwand bei allen Beteiligten. Zu den Rahmenbedingungen gehört damit immer – auch wenn hier nicht überall explizit angesprochen – der Wille und das Bekenntnis zur Verantwortung seitens des Managements, d.h. der Leitung.

In diesem Abschnitt erfolgt die Darstellung der Rahmenbedingungen, d. h. es wird der Frage „Wie sind die organisatorischen, personellen und technischen Rahmenbedingungen?“ nachgegangen.

5.1 Organisatorische Rahmenbedingungen

- Kurzbeschreibung des Unternehmens oder Unternehmensbereichs inkl. Organigramm
- Darstellung der Aufgabenbereiche
- Skizzierung der (Geschäfts-) Prozesse
- Lieferanten-Management für kritische Lieferanten

5.2 Personelle Rahmenbedingungen

- Personelle Struktur (Rolle, nötige Ausbildung, vorhandene Ausbildung)
- Personelle Stärke (Ist vs. Soll)

5.3 Infrastrukturelle Rahmenbedingungen

- Standorte des Unternehmens, die vom zu schützenden IT-System betroffen sind
- Eingesetzte Technologien[3]

5.4 Organisatorische Schnittstellen

- Personalmanagement
- Delegation von Verantwortung
- Gewährleistung Zuverlässigkeit externer Dienstleister

6 Systemarchitektur

Der Überblick über die Systemarchitektur wird oft in drei Blöcken dargestellt:

- Vernetzung als Zugang zu den Komponenten des IT Systems bzw. Informationsverbunds
- Plattform als zentral verfügbare Server mit Betriebssystemen, Speicher, …
- Anwendungen

6.1 Vernetzung

- Wo sind welche IT-Komponenten beziehungsweise logischen Systeme positioniert?
- Welches sind die Schnittstellen nach „außen“?
- Wie sieht die technische Vernetzung zwischen den Standorten aus? (Stichwort: WAN)
- Wie sieht die Vernetzung innerhalb der Standorte aus? (LAN)
- Werden Subnetze abgegrenzt?
- Welche Werkzeuge werden zum Management eingesetzt?
- Wer ist für den Betrieb zuständig?

[3] Technologie ist nicht gleichbedeutend mit „IT-System“, sondern weiter zu verstehen. Zu den Fragen, die man sich hier stellen kann, gehören beispielsweise:

- Wie erfolgen Eigenentwicklungen?
- Gibt es eine einheitliche Rechnerstruktur (Client/Server, Mobilgeräte, ...) oder herrscht diesbezüglich eher eine Heterogenität?
- Erfolgt die IT-Beschaffung über ein Warenwirtschaftssystem?
- Wird IT online bestellt oder konventionell?

6.2 Beschreibung der IT-Plattform

- Welche Technologien (Betriebssysteme, Anwendungen etc.) kommen zum Einsatz?
- Welche technische Funktion nimmt das System wahr? (DNS, Fileserver, …)
- Welche Werkzeuge werden zum Management eingesetzt?
- Welche fachlichen oder auch technischen Abhängigkeiten gibt es zu anderen IT-Komponenten oder Prozessen?
- Wer ist für den Betrieb zuständig?
- Sofern vorhanden, wie sehen die wichtigsten Punkte des Service Level oder Operation Level Agreement für dieses Objekt aus?
- Gibt es Anwendungen Dritter, die ebenfalls auf der Plattform laufen?

6.3 Beschreibung der Architektur der Anwendungen

- Welche Technologien (Anwendungen etc.) kommen zum Einsatz?
- Welche fachliche Funktion nimmt das System wahr? (Warenwirtschaft, KIS, …)
- Erfordern die Anwendungen spezielle Endgeräte? (z.B. Tablets, …)

7 Schutzbedarf

Darstellung der Schutzbedarfsanforderungen aus Sicht der Organisation

7.1 Darstellung der Informationswerte

- Welche Arten von Daten werden verarbeitet?
- Welche Menge von welchen Datenarten fällt an?

7.2 Schutzbedarfsanalyse

- Welche Schutzbedarfsanforderungen hinsichtlich der Kategorien
    - Verfügbarkeit
    - Vertraulichkeit
    - Integrität
    - Authentizität

  existieren?
- Welcher Grad der Verbindlichkeit resultiert aus den Schutzbedarfsanforderungen?

7.3 Risikoanalyse

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

8 Methodische Vorgaben

Darstellung der Strategie

- Umfang (Evaluationsprojekt, Pilotprojekt, Teil- oder Gesamtbereich des Unternehmens, ...)
- Umsetzungsrichtung (Botton-up,Top-down, sideway/ Both-directions)
- Akteure („Change-Agents“)
- Einführungsart (iteratives Vorgehen, „Bombenwurf“)

- Zeitplanung (Dauer, Meilensteine, ...)
- Evaluierungsphase

8.1 Business Impact Analyse

Da in der Schutzbedarfsanalyse oft viele Details eingesammelt werden, muss das Ergebnis priorisiert werden. Dabei hilft eine weitere Einschätzung welcher Schaden für den Informationsverbund / das Unternehmen entsteht, wenn ein bestimmter Vorfall eintritt.

9 Im IT-Sicherheitskonzept zu berücksichtigende Vorgaben

Während die Schutzbedarfsanalyse und die daraus resultierenden Maßnahmen vor allem aus den zu schützenden Informationswerten abgeleitet werden können, kommen hier zusätzliche Vorgaben aus Geschäftsprozessen und rechtlichen Verpflichtungen hinzu.

Grundsätzlich gilt: Aus den angegebenen Vorgabedokumenten sind die konkreten Vorgaben als Grundlage für die Anforderungsdefinition zu extrahieren.

- Welche gesetzlichen Vorgaben sind zu beachten?
  - Datenschutzrechtliche Vorgaben
  - Handelsrechtliche Vorgaben
  - Haftungsrechtliche Vorgaben
  - …
- Welche organisationsinternen Vorgaben sind zu beachten?
  - Arbeitsanweisungen
  - Betriebsvereinbarungen
  - Vorgaben der Revision
  - …

9.1 Beispiel[4]

Vorgabe	Herkunft
Einführung eines Sicherheitskonzeptes	§ 91 II AktG § 43 GmbHG
Aktualisierung Sicherheitskonzeptes	§ 91 II AktG § 43 GmbHG
Regelungen zum Zugang von Dritten	§ 9 BDSG § 823 BGB
Schutz der IT-Systeme	§ 85,88 TKG § 206 STGB
Verhinderung der Schädigung Dritter durch firmeneigene IT	§ 43 GmbHG § 823,1004,280 BGB
…	…

[4] Tabelle nach: Eschweiler J, Psille DEA (2006) Security@Work. Springer-Verlag, 1. Aufl, ISBN-10 3-540-22028-3. S. 122

10 Anforderungen

Aus den Vorgaben in Kapitel 8 werden konkrete Anforderungen abgeleitet

10.1 Beispiel[5]

Vorgabe	Anforderung
Einführung eines Sicherheitskonzeptes	Erarbeitung und Erlass eines IT-Sicherheitskonzeptes
Aktualisierung des Sicherheitskonzeptes	Sicherstellung der bedarfsgerechten Aktualisierung der IT-Sicherheitsprozesse
Regelungen zum Zugang von Dritten	Implementierung von Zutrittskontrollmechanismen
…..	

11 Implementierungsvorgaben

Aus den Vorgaben und daraus resultierenden Anforderungen werden Implementierungsvorgaben abgeleitet, die dann umgesetzt werden müssen. Implementierungsvorgaben können sowohl technischer wie auch organisatorischer Natur sein.

11.1 Beispiel[6]

Vorgabe	Anforderung	Implementierungsvorgabe
Aktualisierung des Sicherheitskonzeptes	Sicherstellung der bedarfsgerechten Aktualisierung der IT-Sicherheitsprozesse	Es ist ein IT-Sicherheitsprozess zur Kontrolle und Wirksamkeit der IT-Sicherheitsmaßnahmen einzurichten.
Regelungen zum Zugang	Implementierung von Kontrollmechanismen	Erstellung und Aktualisierung eines Rechte- und Rollenkonzeptes, auf Basis derer Anwendern Rechte auf Daten eingeräumt oder verweigert werden
…	…	…

12 Restrisiken

Es muss eine Risikoanalyse ausgearbeitet werden, z. B. entsprechend der im Datenschutzkonzept[7] (Kapitel 9, Seite 23) Methodik, beinhaltend eine Darstellung der vorhandenen Restrisiken.

[5] Tabelle nach: Eschweiler J, Psille DEA (2006)Security@Work. Springer-Verlag, 1. Aufl, ISBN-10 3-540-22028-3. S. 122

[6] Tabelle nach: Eschweiler J, Psille DEA (2006)Security@Work. Springer-Verlag, 1. Aufl, ISBN-10 3-540-22028-3. S. 123

[7] Eine Methode ist z.B. in „Leitfaden zur Erstellung eines Datenschutzkonzeptes“. [Online, zitiert am 2017-02-22]; Verfügbar unter https://gesundheitsdatenschutz.org/doku.php/gmds-dgi-empfehlungen

13 Kontrolle und Fortschreibung

13.1 Aktualisierung des Dokuments

- Wie ist der Überarbeitungszyklus?
- Wie wird das Dokument veröffentlicht?
- Wer ist für die Pflege des Dokuments verantwortlich?
- Wer ist federführend bei der Fortschreibung des IT-Sicherheitskonzeptes?[8]

13.2 Darstellung des Auditprozesses

- Wie sieht der Auditprozess aus?
- In welchen Zeitabständen prüft wer welche Komponenten bzgl. weiterhin vorhandener IT-Sicherheit?

14 Mitgeltende Unterlagen

- Welche zusätzlichen zum IT-Sicherheitskonzept (mit-) geltenden Dokumente sind zu beachten?
    - Datenschutzkonzept
    - IT-Sicherheitsleitlinie
    - Rollen- und Berechtigungskonzept
    - Archivierungskonzept
    - Löschkonzept
    - Protokollierungskonzept

[8] Der Unterschied zwischen Federführung bei der Dokumentenfortschreibung und der Pflege des Dokuments liegt in der Art der Tätigkeiten. Bei der Pflege des Dokuments geht es um Tätigkeiten wie z. B.

- Anpassungen/Änderungen/Ergänzungen werden an der richtigen Stelle angefügt
- Mitarbeitern, Auditoren stehen stets die aktuellsten Versionen zur Verfügung
- usw.

Die federführende Stelle ist für die Weiterentwicklung des Dokuments verantwortlich. Bei Änderungen des Workflows, Neuanschaffungen, neu aufgetretenen Risiken usw. erfolgen hier Aktivitäten, um das Sicherheitskonzept fortzuschreiben.

Teil 2: Umsetzungshinweise

1 Begriffsbestimmungen

Im Folgenden sind einige Begrifflichkeiten absichtlich doppelt aufgeführt, damit sich die Schreiber des Sicherheitskonzeptes die für sie am besten passende Definition heraussuchen und bei sich einfügen können. Vermieden werden muss selbstverständlich, dass im jeweiligen Sicherheitskonzept eine Begrifflichkeit mehrfach definiert wird und daher eine Unsicherheit in der Auslegung auftritt. Eine eindeutige Begriffsbestimmung ist daher im konkreten Fall unerlässlich.

Begriff	Erklärung
Akteur	Urheber einer Handlung; neben natürlichen und juristischen Personen können auch Rollen oder Funktionen als Akteure agieren.
Angriff	Versuch, einen Wert zu zerstören, offen zu legen, zu verändern, unbrauchbar zu machen, zu stehlen oder nicht autorisierten Zugriff auf ihn zu erlangen oder ihn ohne Berechtigung zu nutzen (Quelle: DIN ISO/IEC 27000)
Audit	Systematischer, unabhängiger, dokumentierter Prozess zur Erlangung von Aufzeichnungen, Darlegungen von Fakten oder anderen relevanten Informationen und deren objektiver Begutachtung, um zu ermitteln, inwieweit festgelegte Anforderungen erfüllt sind. (Quelle: DIN CEN ISO/TS 14441)
Audit-Trail	Chronologische Aufzeichnung der Aktivitäten von Nutzern eines Informationssystems, die die getreue Wiederherstellung früherer Zustände der betreffenden Informationen ermöglicht. (Quelle: DIN CEN ISO/TS 14265)
Aufzeichnung	Dokument, das erreichte Ergebnisse angibt oder einen Nachweis ausgeführter Tätigkeiten bereitstellt. (Quelle: DIN ISO IEC 27000)
Authentisierung	Beibringung eines Belegs für die von einer Entität behauptete Identität durch die sichere Verbindung eines Identifikators und seines Authentifikators. Siehe auch Authentisierung des Absenders der Daten und Authentisierung der Partnerinstanz (Quelle: DIN EN ISO 22600-1)
Authentisierung	Sicherstellung, dass die von einer Einheit behauptete Eigenschaft korrekt ist (Quelle: DIN ISO/IEC 27000)
Authentizität	Eigenschaft einer Einheit, das zu sein, was sie zu sein vorgibt (Quelle: DIN ISO/IEC 27000)
Autorisierung	Erteilung von Privilegien, einschließlich des Privilegs für den Zugriff auf Daten und Funktionen (Quelle: DIN EN ISO 22600-1)
Bedrohung	Möglicher Anlass für ein unerwünschtes Ereignis, das zu einem Schaden des Systems oder der Institution/Organisation führen kann (Quelle: DIN ISO/IEC 27000)
Datenintegrität	Eigenschaft, dass Daten nicht auf unautorisierte Art geändert oder zerstört worden sind. (Quelle: DIN EN ISO 27799)

Begriff	Erklärung
Datenlöschung	Arbeitsgang, der zur dauerhaften, unwiderruflichen Entfernung der Informationen über die betreffende Person oder den Gegenstand aus dem betreffenden Speicher oder Speichermedium führt. (Quelle: DIN CEN ISO/TS 14265)
Datennutzung	Handhabung von oder Umgang mit Informationen für einen spezifischen Zweck. (Quelle: DIN CEN ISO/TS 14265)
Datenverwendung	Handhabung von oder Umgang mit Informationen für einen spezifischen Zweck. (Quelle: DIN CEN ISO/TS 14265)
Delegierung	Übertragung eines Privilegs von einer Entität, die dieses Privileg besitzt, auf eine andere Entität (Quelle: DIN EN ISO 22600-2)
Dokument	a) als Einheit gehandhabte Zusammenfassung oder Zusammenstellung von Informationen, die nicht-flüchtig auf einem Informationsträger gespeichert sind b) festgelegte und strukturierte Menge von Informationen, die als Einheit verwaltet und zwischen Anwendern und Systemen ausgetauscht werden kann (Quelle: DIN 06789)
Dritte	Natürliche oder juristische Person, die von den involvierten Parteien für die fragliche Angelegenheit als unabhängig angesehen wird (Quelle: DIN ISO/IEC 27002)
Effizienz	Beziehung zwischen den erzielten Ergebnissen und dem Grad der Nutzung der Ressourcen (Quelle: DIN ISO/IEC 27000)
Einhaltung	Handlung, die erforderlich ist, um eine festgelegte Anforderung zu erfüllen (Quelle: DIN CEN ISO/TS 14441)
Elektronische Signaturen	Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind, und die zur Authentifizierung dienen (Quelle: §2 Abs.1 SigG)
Entität	natürliche oder juristische Person, öffentliche Behörde oder Einrichtung oder eine andere Stelle (Quelle: DIN CEN ISO/TS 14441)
Ereignis	Auftreten von ungewöhnlichen Umständen (Quelle: DIN ISO/IEC 27000)
Freigabe	a) eine bestimmten Anweisungen entsprechende Genehmigung nach abgeschlossener Prüfung b) formelle Aktion einer autorisierten Person/Organisation, mit der ein Dokument für einen deklarierten Zweck im Prozessablauf gültig erklärt wird (Quelle: DIN 06789)
Funktionelle Rolle	Funktionelle Rollen sind an eine Handlung gebunden. Funktionelle Rollen können so zugewiesen werden, dass sie während einer Handlung ausgeführt werden müssen. Sie entsprechen der RIM-Beteiligung (Quelle: DIN EN ISO 22600-3)

Begriff	Erklärung
Genehmigung	Bestätigung einer autorisierten Person/Organisation, dass etwas zuvor festgelegten Anforderungen entspricht. (Quelle: DIN 06789)
Gesundheitsversorgung	Jegliche Art von Dienstleistungen mit Auswirkungen auf den Status der Gesundheit, die von Heilberuflern oder Hilfskräften erbracht wird (Quelle: DIN EN ISO 27799)
Identifikation	Durchführung von Tests mit dem Ziel, das betreffende Datenverarbeitungssystem in die Lage zu versetzen, bestimmte Entitäten zu erkennen (Quelle: DIN EN ISO 22600-3)
Identifikator	Information, die verwendet wird, um vor einer möglichen Bestätigung durch einen entsprechenden Authentifikator eine Identität zu beanspruchen (Quelle: DIN EN ISO 22600-2)
Identifizierbare Person	Person, die direkt oder indirekt identifiziert werden kann, insbesondere über die Referenz zu einer Identifikationsnummer oder zu einem oder mehreren Kennzeichen, die bezüglich seiner körperlichen, physiologischen, geistigen, ökonomischen, kulturellen oder sozialen Identität spezifisch sind. (Quelle: DIN EN 14484)
Identifizierung	Durchführung von Tests mit dem Ziel, das betreffende Datenverarbeitungssystem in die Lage zu versetzen, bestimmte Entitäten zu erkennen (Quelle: DIN EN ISO 22600-1)
Identitätsnachweis	Als Voraussetzung ausgegebener Beleg für den Anspruch auf oder die Berechtigung zu einer Rolle (Quelle: DIN EN ISO 22600-2)
Informationssicherheit	Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen; andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nicht-Abstreitbarkeit und Verlässlichkeit können ebenfalls berücksichtigt werden (Quelle: DIN ISO/IEC 27001)
Informationssicherheitsereignis	Erkanntes Auftreten eines System-, Service- oder Netzwerkzustands, der einen möglichen Verstoß gegen die Informationssicherheitsleitlinie oder Fehler von Maßnahmen, oder eine vorher unbekannte Situation, die sicherheitsrelevant sein könnte, anzeigt (Quelle: DIN ISO/IEC 27001)
Informationssicherheitsrisiko	Möglichkeit, dass eine vorhandene Bedrohung die eine Schwachstelle eines Wertes oder einer Gruppe von Werten ausnutzt und dadurch der Institution Schaden zufügen könnte (Quelle: DIN ISO IEC 27000)
Informationssicherheitsvorfall	Einzelnes oder Reihe von unerwünschten oder unerwarteten Informationssicherheitsereignissen, bei denen eine erhebliche Wahrscheinlichkeit besteht, dass Geschäftsabläufe kompromittiert werden und die Informationssicherheit bedroht wird (Quelle: DIN ISO/IEC 27001)

Begriff	Erklärung
Informationsverbund	Unter einem Informationsverbund (oder auch IT-Verbund) ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen. Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen (Quelle: BSI[9])
Informationswert	Wissen oder Daten, die von Wert für die Institution sind (Quelle: DIN ISO IEC 27000)
Inspektion	Untersuchung der Entwicklungs- und Konstruktionsunterlagen eines Produktes, eines Prozesses oder einer Anlage und Ermittlung seiner/ihrer Konformität mit spezifischen Anforderungen oder, auf der Grundlage einer sachverständigen Beurteilung, mit allgemeinen Anforderungen (Quelle: DIN ISO IEC 27000)
Integrität	Eigenschaft, die bedingt, dass die Information in keiner Weise, weder absichtlich noch unabsichtlich, geändert wird (Quelle: DIN EN ISO 22600-2) Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten (Quelle: DIN ISO/IEC 27000)
Konformitätsbewertung	Darlegung, dass festgelegte Anforderungen bezogen auf ein Produkt, einen Prozess, ein System, eine Person oder eine Stelle erfüllt sind (Quelle: DIN CEN ISO/TS 14441)
Korrekturmaßnahme	Maßnahme zur Beseitigung der Ursache eines erkannten Fehlers oder einer anderen erkannten unerwünschten Situation (Quelle: DIN ISO/IEC 27000)
Kryptographie	Disziplin, die Grundsätze, Mittel und Verfahren für die Umwandlung von Daten mit dem Ziel verkörpert, deren Informationsgehalt zu verbergen und ihre unerkannte Änderung und/oder nicht autorisierte Nutzung zu verhindern (Quelle: DIN EN ISO 22600-3)
Leitlinie	Vom Management formell ausgedrückte Gesamtintention und −richtung (Quelle: DIN ISO/IEC 27000)
Maßnahme	Mittel zum Management von Risiken, einschließlich von Leitlinien, Verfahren, Richtlinien, Methoden oder Organisationsstrukturen, die verwaltender, technischer, leitender oder gesetzlicher Natur sein können (Quelle: DIN ISO/IEC 27000)

[9] BSI: Webkurs GSTOOL - Glossar. Online, zitiert am 2017-05-13]; Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzSchulung/WebkursGSTOOL47/05_Glossar/glosssar_node.html;jsessionid=D434C928E8BEBEB7B310E88F7CF23B2B.1_cid351#itverbund

Begriff	Erklärung
Maßnahmenziel	Beschreibung, was durch die Umsetzung von Maßnahmen als Ergebnis erreicht werden soll (Quelle: DIN ISO/IEC 27000)
Nicht-Abstreitbarkeit	Fähigkeit, das Auftreten eines behaupteten Ereignisses oder einer Handlung und die verursachenden Einheiten nachzuweisen, um Streitigkeiten über das Auftreten oder Nichtauftreten des Ereignisses oder der Handlung und die Beteiligung von Einheiten an dem Ereignis zu entscheiden (Quelle: DIN ISO/IEC 27000)
Notfallzugriff	Zugriff auf Daten für einen angemessenen und festgelegten Zweck, wenn eine bestehende Verletzungs- oder Todesgefahr spezielle Genehmigungen oder die Außerkraftsetzung anderer Steuerungseinrichtungen erfordert, um die Verfügbarkeit von Daten in unterbrechungsloser und dringlicher Art und Weise sicherzustellen (Quelle: DIN CEN ISO/TS 14265)
Offenlegung	Preisgabe von Daten an Personen, die nicht routinemäßig über die entsprechende Berechtigung verfügen (Quelle: DIN CEN ISO/TS 14265)
Persönliche Gesundheitsinformationen	Informationen über eine identifizierbare Person, die sich auf den körperlichen oder geistigen Gesundheitszustand der betreffenden Person oder auf die Erbringung von Gesundheitsdienstleistungen für die betreffende Person beziehen (Quelle: DIN EN ISO 27799)
Policy	Menge von gesetzlichen, politischen, organisatorischen, funktionellen und technischen Verpflichtungen, die sich auf Kommunikation und Kooperation beziehen (Quelle: DIN EN ISO 22600-1)
Policy-Vereinbarung	schriftliche Vereinbarung, nach der sich alle Beteiligten zur Einhaltung einer festgelegten Reihe von Policies verpflichten (Quelle: DIN EN ISO 22600-1)
Privileg	Kapazität, die einer Entität von einer Behörde entsprechend dem Attribut dieser Entität zugewiesen wird (Quelle: DIN EN ISO 22600-1)
Projekt	Vorhaben, das im Wesentlichen durch Einmaligkeit der Bedingungen in ihrer Gesamtheit gekennzeichnet ist (Quelle: DIN 69901-5)
Projekt	A temporary endeavor undertaken to create a unique product, service, or result (Vorschlag Übersetzung: ein zeitlich begrenztes Vorhaben, zur Erzeugung/Erbringung eines einzigartigen Produktes, einer einzigartigen Dienstleistung oder eines einzigartigen Ergebnisses) (Quelle: PMBOK 2004)
Prozess	Satz von in Wechselbeziehung oder -wirkung stehenden Tätigkeiten, der Eingaben in Ergebnisse umwandelt (Quelle: DIN ISO/IEC 27000)
Restrisiko	Nach der Risikobehandlung verbleibendes Risiko (Quelle: DIN ISO/IEC 27001)

Begriff	Erklärung
Revisionssicherheit	Der Begriff „Revisionssicherheit“ bezieht sich die Anforderungen a) des Handelsgesetzbuches (§§ 239, 257 HGB) b) der Abgabenordnung (§§ 146, 147 AO), c) der Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme (GoBS) d) ... d. h., auf praktisch ausnahmslos steuerrechtliche bzw. handelsrechtliche Vorgaben. Andere gesetzlichen Vorgaben werden hierbei nicht beachtet. Die revisionssichere Archivierung ist nur ein Bestandteil der rechtssicheren Archivierung. So beinhaltet eine revisionssichere Archivierung beispielsweise keine datenschutzrechtlichen Vorgaben, z. B. bzgl. des Zugriffs auf die archivierten Daten. Hingegen beinhaltet eine revisions- und rechtssichere Archivierung auch alle rechtlichen Anforderungen.
Richtlinie	Empfehlung dessen, was an Umsetzung erwartet wird, um ein Ziel zu erreichen (Quelle: DIN ISO/IEC 27000)
Richtlinienvereinbarung	schriftliche Vereinbarung, mit der sich alle beteiligten Parteien zur Einhaltung einer festgelegten Reihe von Richtlinien verpflichten (Quelle: DIN CEN ISO/TS 14265)
Risiko	Kombination aus der Wahrscheinlichkeit eines Ereignisses und dessen Auswirkungen (Quelle: DIN ISO/IEC 27000)
Risikoakzeptanz	Entscheidung, ein Risiko zu akzeptieren (Quelle: DIN ISO/IEC 27000)
Risikoanalyse	Systematischer Gebrauch von Informationen zur Identifizierung von Risikoquellen und zur Abschätzung des Risikos (Quelle: DIN ISO/IEC 27000)
Risikobehandlung	Prozess der Auswahl und Umsetzung von Maßnahmen zur Modifizierung des Risikos (Quelle: DIN ISO/IEC 27000)
Risikobestimmung	Tätigkeit, bei der der Wahrscheinlichkeit und den Auswirkungen eines Risikos Werte zugeordnet werden (Quelle: DIN ISO/IEC 27000)
Risikobewertung	Prozess, in dem das eingeschätzte Risiko mit den festgelegten Risikokriterien verglichen wird, um die Bedeutung des Risikos zu bestimmen (Quelle: DIN ISO/IEC 27000)
Risikoeinschätzung	Gesamter Prozess der Risikoanalyse und Risikobewertung (Quelle: DIN ISO/IEC 27000)
Risikokommunikation	Austausch oder gemeinsame Nutzung von Informationen über Risiken zwischen Entscheidungsträgern und anderen Stakeholdern (Quelle: DIN ISO/IEC 27000)
Risikokriterien	Bezugsrahmen für die Einschätzung der Bedeutung eines Risikos (Quelle: DIN ISO/IEC 27000)
Risikomanagement	Koordinierte Tätigkeit zur Leitung und Kontrolle einer Institution/Organisation in Bezug auf Risiken (Quelle: DIN ISO/IEC 27000)

Begriff	Erklärung
Rolle	Menge von mit einer Aufgabe verbundenen Kompetenzen und/oder Leistungen. Für das Management von rollenbezogenen Beziehungen zwischen den Entitäten können strukturelle und funktionelle Rollen festgelegt werden (Quelle: DIN EN ISO 22600-3)
Schreddern	mit mechanischen Mitteln durchgeführtes Zerkleinern auf eine festgelegte Größe (Quelle: DIN EN 15713)
Schwachstelle	Schwäche eines Werts oder einer Maßnahme, die von einer Bedrohung ausgenutzt werden kann (Quelle: DIN ISO/IEC 27000)
Sensibilität	Eigenschaft einer Ressource, die deren Wert oder Wichtigkeit impliziert (Quelle: DIN EN ISO 22600-2)
Sicherheit	Kombination von Verfügbarkeit, Vertraulichkeit, Integrität und Zurechenbarkeit (Quelle: DIN EN ISO 22600-1)
Sicherheitsdienst	Dienst, der von einer Schicht miteinander kommunizierender offener Systeme bereitgestellt wird und die Sicherheit der Systeme oder der Datenübertragung in angemessenem Maße sicherstellt (Quelle: DIN EN ISO 22600-1)
Sicherheits-Policy	Plan oder Vorgehensweise für die Sicherstellung der Rechnersicherheit (Quelle: DIN EN ISO 22600-1)
Starke Authentisierung	Authentisierung mittels kryptographisch abgeleiteter multifaktorieller Identitätsnachweise (Quelle: DIN EN ISO 22600-1)
Strukturelle Rolle	Strukturelle Rollen spezifizieren Beziehungen zwischen Entitäten im Sinne der Kompetenz (RIM-Rollen) und spiegeln damit häufig organisatorische oder strukturelle Beziehungen (Hierarchien) wider (Quelle: DIN EN ISO 22600-3)
Systemintegrität	Eigenschaft, dass ein System seine vorgesehene Funktion in einer unbeeinträchtigten Art und Weise, frei von vorsätzlicher oder zufälliger unberechtigter Veränderung des Systems ausführt (Quelle: DIN EN ISO 27799)
Unleugbarkeit	Dienstleistung, die einen Nachweis für die Integrität und die Herkunft der Daten (beides auf fälschungssichere Art und Weise) erbringt, der von einer beliebigen anderen Partei verifiziert werden kann (Quelle: DIN EN ISO 22600-2)
Unterlagen	Urkunden, Amtsbücher, Akten, Schriftstücke, amtliche Publikationen, Karteien, Karten, Risse, Pläne, Plakate, Siegel, Bild-, Film- und Tondokumente und alle anderen, auch elektronischen Aufzeichnungen, unabhängig von ihrer Speicherungsform, sowie alle Hilfsmittel und ergänzenden Daten, die für die Erhaltung, das Verständnis dieser Informationen und deren Nutzung notwendig sind. (Quelle: §2 Abs. 1 ArchivG NRW)

Begriff	Erklärung
Verarbeitung	Erfassung, Aufzeichnung, Aufbewahrung, Änderung, Abruf, Löschung oder Offenlegung von Daten (Quelle: DIN CEN ISO/TS 14265)
Verfahren	Festgelegte Art und Weise, eine Tätigkeit oder einen Prozess auszuführen (Quelle: DIN ISO/IEC 27000)
Verfälschung	unzulässige Änderung des Inhaltes eines Dokumentes nach dessen Freigabe (Quelle: DIN 06789)
Verfügbarkeit	Eigenschaft, einer berechtigten Einheit auf Verlangen zugänglich und nutzbar zu sein (Quelle: DIN ISO/IEC 27001)
Verlässlichkeit	Eigenschaft der Übereinstimmung zwischen beabsichtigtem Verhalten und den Ergebnissen (Quelle: DIN ISO/IEC 27000)
Vernichtung	Reduzierung der Größe, wodurch die Unterlagen so weit wie möglich unlesbar, unleserlich und nicht rekonstruierbar gemacht werden (Quelle: DIN EN 15713)
Vertrauen	im Allgemeinen kann davon ausgegangen werden, dass eine Entität einer anderen Entität „vertraut“, wenn sie annehmen kann, dass sich die zweite Entität genauso, wie von der ersten Entität erwartet, verhalten wird (Quelle: DIN EN ISO 22600-2)
Vertraulichkeit	Eigenschaft, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden (Quelle: DIN ISO/IEC 27000)
Vorbeugungsmaßnahme	Maßnahme zur Beseitigung der Ursache eines möglichen Fehlers oder einer anderen möglichen unerwünschten Situation (Quelle: DIN ISO/IEC 27000)
Wert	Alles, was für die Institution von Wert ist (Quelle: DIN ISO/IEC 27000)
Wirksamkeit	Ausmaß, in dem geplante Tätigkeiten verwirklicht und geplante Ergebnisse erreicht werden (Quelle: DIN ISO/IEC 27000)
Zerfasern	Mit mechanischen Mitteln durchgeführtes Zerkleinern auf eine festgelegte Größe auf mechanische Weise, kleinere Größen als mittels Schreddern erreichbar (Quelle: DIN EN 15713)
Zertifizierung	Bestätigung durch eine dritte Stelle bezogen auf Produkte, Prozesse, Systeme oder Personen (Quelle: DIN CEN ISO/TS 14441)
Ziel	Ressource, auf die von einem Anwärter zugegriffen wird (Quelle: DIN EN ISO 22600-1)
Zugriffskontrolle	Sicherstellung, dass der Zugriff auf Werte autorisiert und eingeschränkt nach den Unternehmens- und Sicherheitsanforderungen erfolgt (Quelle: DIN ISO/IEC 27000)

Begriff	Erklärung
Zugriffssteuerung	Mittel zur Sicherstellung, dass nur autorisierte Entitäten in entsprechend autorisierter Weise Zugriff auf die Ressourcen eines Datenverarbeitungssystems nehmen können (Quelle: DIN EN ISO 22600-1)
Zurechenbarkeit	Verantwortung einer Einheit für ihre Handlungen und Entscheidungen (Quelle: DIN ISO/IEC 27000)
Zustimmung	spezielle Policy, die eine Vereinbarung zwischen einer Entität, die die Rolle des Gegenstandes einer Handlung spielt, und einer handelnden Entität festlegt (Quelle: DIN EN ISO 22600-3)

2 Abkürzungen

Abs	Absatz
ACI	Zugriffssteuerungsinformation(en) (en: Access Control Information)
AIS	Arzt-Informations-System
AMIS	Arzneimittelinformationssystem
AMTS	Arzneimitteltherapiesicherheit
Art	Artikel
Artt	Artikel (Mehrzahl)
BSI	Bundesamt für Sicherheit in der Informationstechnik
bvitg	Bundesverband Gesundheits-IT e. V.
CA	Zertifizierungsstelle (en: certification authority)
CRL	Zertifikatssperrliste (en: Certificate Revocation List)
DAP	Verzeichniszugriffsprotokoll (en: Directory Access Protocol)
DB	Datenbank
DBMS	Datenbankmanagementsystem
DIB	Verzeichnisinformationsbasis (en: Directory Information Base)
DIN	Deutsche Institut für Normung e. V.
DIT	Verzeichnisinformationsbaum (en: Directory Information Tree)
DMS	Dokumentenmanagementsystem
DS-GVO	Datenschutz-Grundverordnung
EDV	Elektronische Datenverarbeitung
EFA	Elektronische Fallakte
EGA	Elektronische Gesundheitsakte
EHR	Elektronische Patientenakte (en: Electronic Health Record)
EPA	Elektronische Patientenakte
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
HIS	Hospital Information System
HL7	Health Level 7
HW	Hardware
IS	Informationssystem
ISMF	Informationssicherheits-Managementforum
ISMS	Informationssicherheits-Managementsystem
ISO	International Organization for Standardization
IT	Informationstechnik, informationstechnisches…
Kap	Kapitel
KAS	Klinisches Arbeitsplatzsystem
KIS	Krankenhaus-Informationssystem
KMU	Kleines, mittelständisches Unternehmen
LDAP	Lightweight Directory Access Protocol
LIS	Labor-Informationssystem
lit	littera (lat. „Buchstabe“)
OASIS	Organization for the Advancement of Structured Information Standards
OID	Objektbezeichner (en: Object Identifier)
PACS	Picture Archiving and Communication System
PDMS	Patientendatenmanagementsystem
PKC	Public-Key-Zertifikat (en: Public Key Certificate)
PKCS	Public-Key-Kryptosystem (en: Public Key Cryptosystem)
PKI	Public-Key-Infrastruktur (en: Public Key Infrastructure)
RA	Registrierungsbehörde (en: Registration Authority)
RBAC	Rollenbasierte Zugriffssteuerung (en: Role-Based Access Control)

RIM	Referenzinformationsmodell
RIS	Radiologisches Informationssystem
RZ	Rechenzentrum
SAML	Security Assertion Markup Language
SLA	Service Level Agreement
SOA	Erklärung zur Anwendbarkeit (en: Statement of Applicability)
SoA	Quelle der Autorität (en: Source Of Authority)
SOA	Security Assertion Markup Language
SW	Software
TK	Telekommunikation(s-)
TTP	Vertrauenswürdige dritte Partei (en: Trusted Third Party)
UHID	Universeller Identifikator im Gesundheitswesen (en: Universal Healthcare Identifier)
URI	Uniform Resource Identifier
UTC	Koordinierte Weltzeit (en: Coordinated Universal Time)
XML	eXtensible Markup Language
ZTG	ZTG Zentrum für Telematik und Telemedizin GmbH

3 Akteure

3.1 Juristische und natürliche Personen

Akteur	Beschreibung
Angreifer	Person, die versucht, mögliche Schwachstellen eines biometrischen Systems auszunutzen (Quelle: DIN EN ISO 25237)
Anwender	(Natürliche) Person, die ein Gerät oder eine Software verwendet
Behandelte Person	Eine oder mehrere Personen, die terminlich eingeplant sind, eine Leistung des Gesundheitswesens zu erhalten, diese gerade erhalten oder diese bereits erhalten haben (Quelle: DIN EN ISO 27799)
Datenbearbeiter	Jegliche Personen (andere als die Mitarbeiter des Datenbeauftragten), die die Daten im Auftrag des Datenbeauftragten bearbeiten (Quelle: DIN EN 15713)
Datenbeauftragter	Person, die (entweder alleine oder gemeinsam mit anderen Personen) die Verwendungszwecke der Daten und die Art und Weise, in der personenbezogene Daten bearbeitet werden oder bearbeitet werden sollen, festlegt. (Quelle: DIN EN 15713)
Datenverarbeiter	Jegliche Personen (andere als die Mitarbeiter des Datenbeauftragten), die die Daten im Auftrag des Datenbeauftragten bearbeiten (Quelle: DIN EN 15713)
Dritter	Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten (Quelle: Verordnung 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))
Empfänger	Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht (Quelle: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))
Entität	natürliche oder juristische Person, öffentliche Behörde oder Einrichtung oder eine andere Stelle (Quelle: DIN CEN ISO/TS 14441)
Erbringer von Gesundheitsversorgung	jegliche Person oder Organisation, die in die Erbringung von Gesundheitsversorgung für einen Klienten eingebunden ist oder dazu gehört, oder die sich um das Wohlbefinden eines Klienten kümmert (Quelle: DIN EN ISO 27799)
Heilberufler	Person, die von einer anerkannten Stelle autorisiert ist, zur Erbringung gewisser medizinischer Dienstleistungen qualifiziert zu sein (Quelle: DIN EN ISO 27799)

Akteur	Beschreibung
Hersteller	Natürliche oder juristische Person, die für die Auslegung, Herstellung, Verpackung oder Kennzeichnung eines Medizinprodukts, für den Zusammenbau eines Systems oder für die Anpassung eines Medizinprodukts vor dem Inverkehrbringen oder der Inbetriebnahme verantwortlich ist, unabhängig davon, ob diese Tätigkeiten von dieser Person selbst oder stellvertretend für diese von einer dritten Person ausgeführt werden (Quelle: DIN EN ISO 14971)
Identifizierbare Person	Jemand, der direkt oder indirekt identifiziert werden kann, insbesondere über die Referenz zu einer Identifizierungsnummer oder zu einem oder mehreren Kennzeichen, die bezüglich seiner körperlichen, physiologischen, geistigen, ökonomischen, kulturellen oder sozialen Identität spezifisch sind (Quelle: DIN EN ISO 27799)
Maßnahmenverantwortlicher	Verantwortlicher zur Umsetzung einer oder mehrerer Maßnahme(n)
Patient	Behandelte Person (Quelle: DIN EN ISO 27799)
Person, identifizierbare	Jemand, der direkt oder indirekt identifiziert werden kann, insbesondere über die Referenz zu einer Identifikationsnummer oder zu einem oder mehreren Kennzeichen, die bezüglich seiner körperlichen, physiologischen, geistigen, ökonomischen, kulturellen oder sozialen Identität spezifisch sind (Quelle: DIN CEN ISO/TS 14441)
Risikoinhaber	Verantwortlicher zur Verwaltung und Beobachtung eines Risikos
Unternehmen	Natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen (Quelle: Verordnung 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))
Verantwortlicher (für die Verarbeitung)	Natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet (Quelle: Verordnung 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))
Vertreter	Eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt (Quelle: Verordnung 2016/679 des Europäischen Parlaments und des Rates (Datenschutz-Grundverordnung))

3.2 Nicht-Personen

Akteur	Beschreibung
Anwendungssystem	System bestehend aus Hardware und Anwendungssoftware zur Unterstützung definierter Aufgaben

Akteur	Beschreibung
Archiv, digitales	Informationssystem und Strategie, welche den Erhalt und die Verfügbarkeit von Informationen in digitaler Form bei bestimmungsgemäßen Gebrauch gewährleistet
Arzneimittelinformationssystem	Softwarelösung, welche umfangreiche Informationen zu Arzneimitteln bereitstellt
Arzt-Informations-System	Softwarelösung für die Unterstützung der in einer Arztpraxis anfallenden Geschäftsprozesse
Arztpraxisinformationssystem	Ein oder mehrere Informationssysteme zur Erhebung und Speicherung sowie Bereitstellung von in einer Arztpraxis anfallenden Daten eines Patienten
Dokumenten-Management-System	Softwarelösung für das Management von digitalen Dokumenten (Erfassen, Strukturieren, Speichern, Bereitstellen)
Gesundheitsinformationssystem	Ablage für Informationen, die die Gesundheit einer behandelten Person betreffen; die in einer von Computern zu verarbeitenden Form sicher gespeichert und zugänglich für mehrere autorisierte Benutzer dargestellt werden (Quelle: DIN CEN ISO/TS 14441)
Gesundheitsinformationssystem	Ablage für Informationen, die die Gesundheit einer behandelten Person betreffen, in einer von Computern zu verarbeitenden Form, sicher gespeichert und übermittelt sowie zugänglich für mehrere autorisierte Nutzer (Quelle: DIN EN ISO 27799)
Hospital Information System	Siehe „Krankenhaus-Informationssystem“
Kommunikationsserver	Softwarelösung zum Empfang und zur Verteilung von digitalen Nachrichten zwischen verschiedenen Informationssystemen wie bspw. KIS, RIS, LIS
Krankenhaus-Informationssystem	Gesamtheit aller in einem Krankenhaus eingesetzten informationstechnischen Systeme zur Verwaltung und Dokumentation elektronischer Patientendaten. Dabei handelt es sich in aller Regel um einen Verbund selbständiger Systeme meist unterschiedlicher Hersteller. Auf einzelne Fachbereiche beschränkte Verfahren wie z. B. Labor-, Radiologie- oder Diagnosesysteme gehören als Subsysteme ebenfalls zum Krankenhausinformationssystem (Quelle OH KIS, 2. Fassung Stand März 2014)
Labor-Informationssystem	Softwarelösung für die Unterstützung der in einem Labor anfallenden Geschäftsprozesse
Medizinprodukt	Entsprechend EU Richtlinie 93/42/EWG Art. 1 Abs.2 lit. a[10]
Modalität	Gerät zur Erzeugung medizinischer Bilddaten
Patientendatenmanagement-System	Softwarelösung, welche in Krankenhäusern die patientenbezogenen Informationen erfasst, speichert und zugänglich für mehrere autorisierte Benutzer darstellt
Picture Archiving and Communication System	Softwarelösung, welche den Erhalt und die Verfügbarkeit von medizinischen Bilddaten gewährleistet

[10] Richtlinie 93/42/EWG des Rates vom 14. Juni 1993 über Medizinprodukte. [Online, zitiert am 2016-09-01]; Verfügbar unter http://eur-lex.europa.eu/legal-content/de/ALL/?uri=CELEX:31993L0042

Akteur	Beschreibung
Point-Of-Service-System	System, das an der Versorgungsstelle bei der Erbringung klinischer Dienstleistungen gegenüber der behandelten Person verwendet wird (Quelle: DIN CEN ISO/TS 14441)
Radiologisches Informationssystem	Softwarelösung für die Unterstützung der in der Radiologie anfallenden Geschäftsprozesse

4 Risikobewertung

In Deutschland werden bisher überwiegend materielle Risiken (Finanzen, Gesundheit, ...) benannt, was u.a. an unserer zivilrechtlichen Rechtsprechung bzgl. Haftung liegt. Europarechtlich sind aber auch immaterielle Risiken zu betrachten. Die folgenden Kapitel sollen helfen, diese Thematik für die eigenen Fragestellungen zu behandeln.

Grundsätzlich kennt die IT-Sicherheit drei Grundwerte:

1. Vertraulichkeit: Vertrauliche Informationen müssen vor unbefugter Preisgabe geschützt werden.
2. Verfügbarkeit: Dem Benutzer stehen Daten, Dienste und Applikationen zum geforderten Zeitpunkt zur Verfügung.
3. Integrität: Die Daten sind vollständig und unverändert.

Die europäische Datenschutz-Grundverordnung fügte als vierten Grundwert die Belastbarkeit der Systeme und Dienste hinzu.

4.1 Welche Risiken sollten immer betrachtet werden?

Grundsätzlich müssen alle für das Unternehmen relevanten Risiken betrachtet werden, die aus dem Projekt bzw. den darin enthaltenen IT-Systemen resultieren können. Dazu gehören direkte Risiken wie z.B. den Verlust der Fähigkeit, die Tätigkeit/Dienstleistung des Unternehmens erbringen zu können, aber auch indirekte Risiken, die z.B. aus einem Imageverlust resultieren können.

4.1.1 „Klassische“ potenzielle Gefährdungen

Basierend auf den drei Grundwerten adressiert die IT-Sicherheit u.a. den Schutz vor dem Verlust der drei oben dargestellten Grundwerten. Potenzielle Gefahren sind somit u.a.:

- Datenverlust
- Datendiebstahl
- Malwarebefall / Viren, Trojaner, ...)
- Systemausfall
- Personeller Ausfall, insbesondere von Administratoren
- Rechtliche Konsequenzen, insbesondere resultierend aus
  - § 91 AktG bzw. Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), d.h.
    - Unternehmen müssen Risikofrüherkennungssysteme, Risikomanagement- und -steuerungssysteme installieren,
    - potenzielle Risikofelder beobachten und
    - den davon ausgehenden Risiken gegenzusteuern
    - Adressat: Aktiengesellschaften sowie Gesellschaften, die 2 der 3 Kriterien in 2 aufeinander folgenden Jahren erfüllen:
      - Bilanzsumme > 3,44 Mio. Euro
      - Umsatz > 6,87 Mio. Euro
      - Mitarbeiterzahl > 50
  - §§ 109, 109a Telekommunikationsgesetz (TKG), beinhaltend
    - Diensteanbieter müssen technische Vorkehrungen treffen, um
      - Fernmeldegeheimnis
      - Personenbezogene Daten

    entsprechend dem Stand der Technik zu schützen.

- § 3 Produktsicherheitsgesetz (ProdSG) bzw. daraus ableitend folgende Anforderungen:
  - Risikomanagement erforderlich
  - Qualitätsmanagement notwendig
  - Technische Dokumentation muss vorhanden sein

  unter Berücksichtigung harmonisierter Normen
- Regelungen bzgl. Medizinprodukte
  - Grundsatz: Ein Medizinprodukt darf den Patent nicht schädigen
  - Medizinprodukt erfordert Risikoklassifizierung (Anhang 9 RL 93/*42/EWG, Gruppen 1, 1*, 2a, 2b, 3)
  - Medizinprodukt muss den grundlegenden Anforderungen gemäß Anhang 1 RL 93/42/EWG genügen, d.h. insbesondere harmonisierte Normen berücksichtigen, z. B.
    - DIN EN ISO 14971: Medizinprodukte - Anwendung des Risikomanagements auf Medizinprodukte
    - DIN EN 60601-1: Medizinische elektrische Geräte - Teil 1: Allgemeine Festlegungen für die Sicherheit einschließlich der wesentlichen Leistungsmerkmale
    - DIN EN 62304: Medizingeräte-Software - Software-Lebenszyklus-Prozesse

– Unternehmerische Anforderungen resultierend aus den Prüfstandards Institut der Wirtschaftsprüfer, IT insbesondere betreffend IDW PS 330: Abschlussprüfung bei Einsatz von Informationstechnologie
  - Richtlinien zur Prüfung bzgl.:
    - Ziele und Umfang von IT-Systemprüfungen
    - Durchführung von IT-Systemprüfungen
    - IT-gestützte Prüfungstechniken
    - Produktdokumentation und Berichterstattung
  - Daraus abgeleitet zu prüfende Risikofelder:
    - IT-Organisationsrisiken
    - IT-Infrastrukturrisiken
    - IT-Anwendungsrisiken,
    - IT-Geschäftsprozessrisiken
    - IT-Überwachungsrisiken
    - IT-Outsourcingrisiken (adressiert von Prüfstandard IDW PS 33)

4.1.2 Datenschutzrechtliche Risiken

Die europäische Datenschutzgrundverordnung fordert in verschiedenen Artikeln eine Risikobetrachtung und -bewertung. Art. 5 Abs. 1 lit. f DS-GVO verlangt, dass „in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen“. Ein Verstoß gegen Art. 5 DS-GVO kann gemäß Art. 83 Abs. 5 lit. a DS-GVO mit „bis zu 20.000.000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs“ geahndet werden. Damit ergibt sich die Notwendigkeit, eine Risikobewertung bzgl. der Verarbeitung personenbezogener

Daten aufzustellen. Dazu müssen natürlich zunächst einmal die Risiken für „Rechte und Freiheiten natürlicher Personen“ benannt werden.

In seiner Dissertation[11] erarbeitete Stefan Drackert eine Kategorisierung der Risiken, die bei einer Verarbeitung personenbezogener Daten auftreten können.

1. Strukturelle Risiken
   a. Gesellschaftlich-politische Risiken
      i. Informationsmacht
      ii. Konformistische Verhaltensanpassung durch Überwachungsdruck
      iii. Verantwortungsnegation
   b. Wirtschaftliche Risiken
      i. Handelshemmnisse
      ii. Nachfragerückgang durch Vertrauensverlust
2. Individuelle Risiken
   a. Erhöhung individueller Verletzlichkeit für Straftaten
   b. Schamgefühl und Publizitätsschäden
   c. Selektivitätsschäden
      i. Diskriminierung
      ii. Stigmatisierung
   d. Informationspermanenz
   e. Entkontextualisierung
      i. Kontextdefizit
      ii. Kontextinfiltration
   f. Informationsemergenz
   g. Informationsfehlerhaftigkeit
3. Risiken für Gesellschaft und Individuum
   a. Behandlung des Menschen als bloßes Objekt
   b. Bildung eines Persönlichkeitsprofils
   c. Fremdbestimmung
   d. Enttäuschung von Vertraulichkeitserwartungen
4. Grenzfälle
   a. Werbung und Zielgruppenpräzisierung
   b. Bonitätsprüfungen, Forderungsmanagement
   c. Arbeitsrechtlicher Kontext

4.2 Risikobewertung

Hierzu müssen drei Schritte absolviert werden:

1. Der Schaden muss klassifiziert werden
2. Die Eintrittswahrscheinlichkeit muss abgeschätzt werden
3. Basierend auf diesen beiden Ergebnissen muss das Risiko klassifiziert werden

[11] Stefan Drackert (2014) Die Risiken der Verarbeitung personenbezogener Daten - Eine Untersuchung zu den Grundlagen des Datenschutzrechts. Duncker & Humblot GmbH. ISBN '978-3-428-1 4730-4

4.2.1 Eintrittswahrscheinlichkeit

Die Eintrittswahrscheinlichkeit kann wie folgt klassifiziert werden:

Hoch	Tritt wahrscheinlich auf, oft, häufig
Mittel	Kann auftreten, jedoch nicht häufig
Niedrig	Unwahrscheinliches Auftreten, selten, fernliegend

4.2.2 Schadensklassifikation

Definitionen des Schweregrads:

Katastrophal:	Führt zum Tod der Patientin / des Patienten
Kritisch:	Führt zu dauernder Behinderung oder einer lebensbedrohlichen Schädigung
Ernst:	Führt zu einer Schädigung oder Behinderung, die ein sachkundiges medizinisches Eingreifen erfordert
Gering:	Führt zu einer zeitweiligen Schädigung oder Behinderung, die kein sachkundiges medizinisches Eingreifen erfordert
Vernachlässigbar:	Unannehmlichkeiten oder zeitweilige Beschwerden

4.2.3 Risikoklassifizierung

Innerhalb einer Risikomatrix wird das Risiko für die einzelnen Gefahrenpotenziale dargestellt, hier eine exemplarische Abbildung von einigen datenschutzrechtlichen Risiken:

Potenzielles Risiko		Eintrittswahrscheinlichkeit	Schadensklassifikation
Strukturelle Risiken			
	Gesellschaftlich-politische Risiken		
	Informationsmacht		
	Verhaltensanpassung durch Überwachungsdruck		
	Verantwortungsnegation		
	Wirtschaftliche Risiken		
	Handelshemmnisse		
	Nachfragerückgang		
Individuelle Risiken			
	Erhöhung individueller Verletzlichkeit für Straftaten		
	Schamgefühl und Publizitätsschäden		
	Selektivitätsschäden		
	Diskriminierung		
	Stigmatisierung		
	Informationspermanenz		
	Entkontextualisierung		
	Kontextdefizit		

Potenzielles Risiko		Eintrittswahrscheinlichkeit	Schadensklassifikation
	Kontextinfiltration		
	Informationsemergenz		
	Informationsfehlerhaftigkeit		
Risiken für Gesellschaft und Individuum			
	Behandlung des Menschen als bloßes Objekt		
	Bildung eines Persönlichkeitsprofils		
	Fremdbestimmung		
	Enttäuschung von Vertraulichkeitserwartungen		
Grenzfälle			
	Werbung und Zielgruppenpräzisierung		
	Bonitätsprüfungen, Forderungsmanagement		
	Arbeitsrechtlicher Kontext		

5 Feststellung des Schutzbedarfs

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erläutert in Kapitel 4.3 im BSI-Standard 100-2[12] das Vorgehen bei einer Schutzbedarfsfeststellung. Daher werden hier nur einige allgemeine Hinweise bzgl. des Vorgehens gegeben, nähere Einzelheiten sind in der Ausarbeitung des BSI zu finden.

Zur Schutzbedarfsanalyse müssen folgende Schritte vollzogen werden:

1) Definition der Schutzbedarfskategorien
2) Schutzbedarfsfeststellung für Anwendungen
3) Schutzbedarfsfeststellung für IT-Systeme
4) Schutzbedarfsfeststellung für Räume
5) Schutzbedarfsfeststellung für Kommunikationsverbindungen
6) Schlussfolgerungen aus den Ergebnissen 2) bis 5).

Die Definition der Schutzbedarfskategorien muss auf die eigenen Bedürfnisse erfolgen. Begrifflichkeiten wie „normal“, „hoch“ und „sehr hoch“ werden zwar universell eingesetzt, die Bedeutung, was unter „normal“ und den anderen allgemeinen Begrifflichkeiten im Einzelfall zu verstehen ist, kann aber nur im jeweiligen Einzelfall definiert werden.

Zu betrachtende Schadensszenarien bedingen natürlich auch die Betrachtung evtl. Verstöße gegen Gesetze und Verordnungen und daraus resultierende Schäden wie Bußgelder oder andere Haftungsfolgen. Andererseits müssen natürlich auch die Folgen evtl. auftretender negativer Innen- und/oder Außenwirkung betrachtet werden, aus denen Schaden erwachsen kann, z. B. durch verlorene Kundinnen und Kunden. Je nach erfolgter Verarbeitung kann für Betroffene auch eine Beeinträchtigung der körperlichen oder seelischen Unversehrtheit mit entsprechendem Schadensersatzanspruch resultieren. Letztlich muss also auch bei der Betrachtung eines potenziellen Schadens der jeweilige Einzelfall betrachtet werden. Die Schadensszenarien sind letztlich auch Ergebnisse der Risikobewertung (siehe entsprechendes Kapitel auf Seite 33).

Sind Schutzbedarfskategorien definiert und potenzielle Schadensszenarien identifiziert, erfolgt die Schutzbedarfsfeststellung für die jeweils potenziell bedrohten Ressourcen. Auch hierzu finden sich in der Ausarbeitung des BSI Beispiele.

Ist der Schutzbedarf festgestellt, so resultiert daraus als Ergebnis, welche Ressource gegen welche Bedrohung zu schützen ist. Idealerweise lassen sich aus der Identifikation des Risikos auch direkt Maßnahmen zum Schutz der Ressource ableiten. Dies ist aber nicht immer der Fall, sodass hier ggf. auch externes Wissen zur Risikominimierung eingekauft werden muss.

[12] Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise. [Online, zitiert am 2016-09-27]; Verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile

6 Vorschläge hinsichtlich zu treffender IT-Sicherheitsmaßnahmen

Nachfolgend finden sich exemplarisch einige Beispiele. Grundlegend müssen die Inhalte entsprechend dem eigenen Bedarf ausgewählt und dargestellt werden.

Die nachfolgenden Überschriften zeigen an, wie die Struktur eines entsprechenden Dokuments aussehen könnte.

Hinweise zur Umsetzung von IT-Sicherheit finden sich insbesondere bei den folgenden Quellen:

- Bundesamt für Sicherheit in der Informationstechnik (BSI): IT-Grundschutz-Kataloge. [Online, zitiert am 2017-09-08]; Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
- Deutsche Telekom: Privacy and Security Assessment Verfahren – Technische Sicherheitsanforderungen. [Online, zitiert am 2017-09-08]; Verfügbar unter https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/sicherheit/privacy-and-security-assessment-verfahren-342724
- Information Assurance Support Environment (IASE): Security Technical Implementation Guides (STIGs). . [Online, zitiert am 2017-09-08]; Verfügbar unter https://iase.disa.mil/stigs/Pages/index.aspx
- National Institute of Standards and Technology (NIST): Special Publications (SP). [Online, zitiert am 2017-09-08]; Verfügbar unter http://csrc.nist.gov/publications/PubsSPs.html

Produktbezogene Hinweise finden sich i.d.R. bei den jeweiligen Herstellern. Insbesondere zur Härtung der eingesetzten Systeme sollten die Hinweise der jeweiligen Hersteller berücksichtigt werden.

6.1 Basisschutz

6.1.1 Schulung Beschäftige

- …

6.1.2 Zugangsschutz

- Es existiert eine Klassifikation bzgl. der Sicherheit der Informationen, an Hand derer eine „Need-to-know“ Strategie erarbeitet und umgesetzt wird
- Es existiert eine Zugangsschutzrichtlinie
- …

6.1.3 Berechtigungskonzept

- Es existiert ein Rechte- und Rollenkonzept, welches regelmäßig geprüft und aktualisiert wird.
- Das Konzept sieht vor, dass miteinander in Konflikt stehende Aufgaben und Verantwortungsbereiche getrennt werden.
- …

6.1.4 Home-Office/Telearbeit

- Der Zugriff auf Unternehmensdaten durch Telearbeit ist mindestens genauso sicher wie der Zugriff auf Daten innerhalb des Unternehmens
- Es existiert eine Richtlinie zur Telearbeit
- …

6.1.5 Datensicherung

- Es existiert eine Datensicherungsrichtlinie, die mindestens beinhaltet:
  - Eine Darstellung des Vorgangs der Datensicherung wie auch der Wiederherstellungsverfahren
  - Eine Darstellung der Lagerung der Datensicherung unter besonderer Berücksichtigung, dass die Datensicherung auch bei Schäden am Hauptstandort geschützt sein muss.
  - Den Zyklus der Überprüfung der Datensicherungsmedien wie auch der Datensicherung selbst.
- …

6.1.6 Protokollierung

- Es existiert eine Protokollierungsrichtlinie
- Im Rahmen einer Auswertung sollte eine möglichst einheitliche Protokollierung erfolgen. Im Minimum sollte daran gedacht werden, dass Benutzernamen und Zeit (timestamp) in allen protokollierenden Systemen übereinstimmen.
- …

Hinweis: Bei Fragen zur Protokollierung sind oftmals auch datenschutz- und arbeitsrechtliche Fragstellungen zu beachten. Daher sollte hier an eine Beteiligung sowohl des Datenschutzbeauftragten als auch der Mitarbeitervertretung gedacht werden.

6.2 Verfügbarkeit der Daten, Dienste und Geräte

- Es existiert ein Business-Continuity-Plan zur Wiederherstellung nach Schadsoftware-Angriffen oder Schäden durch natürliche Ursachen (z.B. Regen, Sturm, Flugzeugabsturz).
- …

6.3 Härtung der eingesetzten Systeme

6.3.1 Endgeräte

6.3.1.1 Desktop / Laptop

- Es existiert eine Richtlinie bzgl. der Nutzung von IT-Systemen.
- …

6.3.1.2 Mobile Endgeräte

- Es existiert eine Richtlinie zur Nutzung von mobilen Geräten im Unternehmen.
- Ex existiert eine Regelung bzgl. der privaten Nutzung dienstlicher Geräte.
- Ex existiert eine Regelung bzgl. der dienstlichen Nutzung privater Geräte.
- Es existiert eine Regelung, wie Patienten ihre Geräte für ihre privaten Zwecke nutzen können
- …

6.3.2 Server

6.3.2.1 Allgemeine Anforderungen

- Alle Räumlichkeiten mit Servern sind durch eine angemessene Zutrittssteuerung geschützt, die gewährleistet, dass ausschließlich berechtigte Personen Zutritt haben.
- …

6.3.2.2 Fileserver

6.3.2.2.1 Allgemeine Anforderungen

- Die Nutzung und der Zugriff auf schutzbedürftige Funktionen und Informationen, dürfen nicht ohne erfolgreiche Authentifizierung und Autorisierung möglich sein.
- ...

6.3.2.2.2 Windows

- ...

6.3.2.2.3 Linux

- ...

6.3.2.2.4 ...

- ...

6.3.2.3 Datenbankserver

6.3.2.3.1 Allgemeine Anforderungen

- Default-Passwörter auf Datenbanksystemen müssen geändert werden.
- Alle Datenbankdienste müssen mit minimalen Rechten auf Betriebssystemebene aufgesetzt werden.
- ...

6.3.2.3.2 Oracle

- ...

6.3.2.3.3 MySQL/MariaDB

- ...

6.3.2.3.4 ...

- ..

6.3.2.4 Webserver

6.3.2.4.1 Allgemeine Anforderungen

- Der Webserver muss der einzige extern zugreifbare Service eines Systems sein, soweit der Webserver nicht ausschließlich für eine Administrations-Schnittstelle genutzt wird.
- Alle Webserverprozesse dürfen nicht mit Systemprivilegien laufen.
- Die Erreichbarkeit von Diensten muss eingeschränkt werden.
- ...

6.3.2.4.2 Apache

6.3.2.4.3 Tomcat

- ..

6.3.2.4.4 ...

- ...

6.3.3 Firewall

- …

6.3.4 Netzwerkkomponenten

6.3.4.1 Router/Switche

– …

6.3.4.2 Proxy-Server

– …

6.3.5 TK-Anlagen

– ….

6.3.6 Virtualisierung

6.3.6.1 Cytrix XEN

– …

6.3.6.2 Hyper-V

– ….

6.3.6.3 …

– ….

7 Weiterführende Literatur

7.1 Online-Ressourcen

- Bundesamt für Sicherheit in der Informationstechnik (BSI): BSI-Standards. [Online, zitiert am 2016-12-29]; Verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html;jsessionid=A4BD6A096C0F99008DA28B8D96A81D11.1_cid091
- Deutsche Telekom: Privacy and Security Assessment Verfahren – Technische Sicherheitsanforderungen. [Online, zitiert am 2017-09-08]; Verfügbar unter https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/sicherheit/sicherheit/privacy-and-security-assessment-verfahren-342724
- Information Assurance Support Environment (IASE): Security Technical Implementation Guides (STIGs). . [Online, zitiert am 2017-09-08]; Verfügbar unter https://iase.disa.mil/stigs/Pages/index.aspx
- ISIS12-InformationsSIcherheitsmanagementSystem in 12 Schritten. [Online, zitiert am 2016-12-29]; Verfügbar unter https://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12.html
- National Institute of Standards and Technology (NIST): Special Publications (SP). [Online, zitiert am 2017-09-08]; Verfügbar unter http://csrc.nist.gov/publications/PubsSPs.html
- Open Web Application Security Project (OWASP) [Online, zitiert am 2016-12-29]; Verfügbar unter https://www.owasp.org/index.php/Germany

7.1.1 Mailinglisten

- SecLists.Org Security Mailing List
  http://seclists.org/
- Bugtraq
  http://www.securityfocus.com/
- US-Cert
  https://www.us-cert.gov/mailing-lists-and-feeds

Übersicht über verschiedene Mailinglisten:
http://www.securityawareness.com/is_lists.htm

7.2 Bücher

- Buchmann J. Einführung in die Kryptographie. Springer Verlag, 6. Auflage 2016. ISBN 978-3-642-39774-5
- Grünendahl T, Steinbacher A, Will P. Das IT-Gesetz: Compliance in der IT-Sicherheit - Leitfaden für ein Regelwerk zur IT-Sicherheit im Unternehmen. Springer Verlag, 2. Auflage 2012. ISBN 978-3-8348-1680-1
- Halang W.A. (Hrsg.) Funktionale Sicherheit. Springer Verlag, 2013. ISBN 978-3-642-41308-7
- Harkins M. Managing Risk and Information Security. Apress Media, 1. Auflage 2013. ISBN 978-1-4302-5113-2
- Huber E. (Hrsg.) Sicherheit in Cyber-Netzwerken - Computer Emergency Response Teams und ihre Kommunikation. Springer Verlag, 1. Auflage 2015. ISBN 978-3-658-09057-9
- Kappes M. Netzwerk- und Datensicherheit - Eine praktische Einführung. Springer Verlag, 2. Auflage 2013. ISBN 978-3-8348-0636-9

- Kersten H, Klett G. Der IT Security Manager. Springer Verlag, 4. Auflage 2015. ISBN 978-3-658-09973-2
- Kersten H, Reuter J, Schröder KW. IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz. Springer Verlag, 4. Auflage 2013. ISBN 978-3-658-01723-1
- Klipper S. Cyber Security - Ein Einblick für Wirtschaftswissenschaftler. Springer Verlag, 1. Auflage 2015, ISBN 978-3-658-11576-0
- Klipper S. Information Security Risk Management - Risikomanagement mit ISO/IEC 27001, 27005 und 31010. Springer Verlag, 2. Auflage 2015. ISBN 978-3-658-08773-9
- Kohne A, Ringleb S, Yücel C. Bring your own Device - Einsatz von privaten Endgeräten im beruflichen Umfeld – Chancen, Risiken und Möglichkeiten. Springer Verlag. 1. Auflage 2015. ISBN 978-3-658-03716-1
- Leopold H, Bleier T, Skopik F. Cyber Attack Information System - Erfahrungen und Erkenntnisse aus der IKT-Sicherheitsforschung. Springer Verlag, 1. Auflage 2015. ISBN 978-3-662-44305-7
- Müller K. Handbuch Unternehmenssicherheit. Springer Verlag, 3. Auflage 2015. ISBN 978-3-658-10150-3
- Müller K. T-Sicherheit mit System - Integratives IT-Sicherheits-, Kontinuitäts- und Risikomanagement – Sichere Anwendungen – Standards und Practices. Springer Verlag, 5. Auflage 2014. ISBN 978-3-658-04333-9
- Nowey T. Konzeption eines Systems zur überbetrieblichen Sammlung und Nutzung von quantitativen Daten über Informationssicherheitsvorfälle. Vieweg Verlag. 1. Auflage 2011. ISBN 978-3-8348-1423-4
- Rohr M. Sicherheit von Webanwendungen in der Praxis. Springer Verlag, 1. Auflage 2015. ISBN 978-3-658-03850-2
- Schneider S, Sunyaev A. Cloud-Service-Zertifizierung - Ein Rahmenwerk und Kriterienkatalog zur Zertifizierung von Cloud-Services. Springer Verlag, 1. Auflage 2015. ISBN 978-3-662-47285-9
- Schwenk J. Sicherheit und Kryptographie im Internet. Springer Verlag, 4. Auflage 2014. ISBN 978-3-658-06543-0
- Sowa A. Metriken – der Schlüssel zum erfolgreichen Security und Compliance Monitoring. Vieweg Verlag, 1. Auflage 2011. ISBN 978-3-8348-1480-7
- Sowa A, Duscha P, Schreiber S. IT-Revision, IT-Audit und IT-Compliance. Springer Verlag, 2015. ISBN 978-3-658-02807-7

7.3 Standards

- Cobit
  - ISACA International
    https://www.isaca.org/COBIT/Pages/default.aspx
  - ISACA German Chapter
    http://www.isaca.de/
  - COBIT-Campus
    http://www.isaca.org/Education/on-demand-learning/Pages/default.aspx bzw.
    https://www.isaca.org/ecommerce/Pages/vCampusLogin.aspx?returnurl=/ecommerce/Pages/ProcessLogin.aspx?vt=2
- IDW PS 330 Abschlussprüfung bei Einsatz von Informationstechnologie
  - Institut der Wirtschaftsprüfer
    https://shop.idw-verlag.de/product.idw?product=20068

  - IDW Prüfungsnavigator Grundversion
    https://www.idw.de/idw/im-fokus/idw-pruefungsnavigator/idw-pruefungsnavigator-grundversion---zip-datei/28246
  - IT-Auditor IDW - Richtlinie
    https://www.idw.de/blob/87038/eac3b57db3b9a8c8a8bb1417fa1ba1bc/down-it-au-richtlinie-data.pdf
- IT Infrastructure Library (ITIL)
  - Axelos: Best Practices
    https://www.axelos.com/best-practice-solutions/itil
  - ITIL Wiki
    http://wiki.de.it-processmaps.com/index.php/Hauptseite
  - Studien des BSI bzgl. ITIL
    https://www.bsi.bund.de/DE/Publikationen/Studien/ITIL/index_htm.html
  - ITIL Blog
    https://www.itil.de/

7.4 Zeitschriften

- <kes> Zeitschrift für Informations-Sicherheit
  Verlag: DATAKONTEXT GmbH
  Homepage: https://www.kes.info
- IT-Sicherheit
  Verlag: DATAKONTEXT GmbH
  Homepage: https://www.itsicherheit-online.com/zeitschrift
- Protector & WIK
  Verlag: I.G.T. Informationsgesellschaft Technik mbH
  Homepage:
  http://www.sicherheit.info/SI/cms.nsf/html/protector.html?Open&SessionID=2333897-125610
- SECURITYinsight
  Verlag: ProSecurity Publishing GmbH & Co. KG
  Homepage: http://www.prosecurity.de/verlag/zeitschriften

7.5 Normen

7.5.1 Anonymisierung/Pseudonymisierung

- DIN EN ISO 25237 „Pseudonymisierung“
  Stand: 2017-05 (Norm)
- DIN EN ISO/IEC 27038 „Informationstechnik - IT-Sicherheitsverfahren - Spezifikation für digitales Schwärzen“
  Stand: 2016-12 (Norm)

7.5.2 Authentifizierung/ID-Management

- ISO/IEC FDIS 2382-37 „Information technology - Vocabulary - Part 37: Biometrics“
  Stand: 2012-123 (Norm) bzw. 2016-10 (Entwurf)
- ISO/IEC 9798-1 „Information technology - Security techniques - Entity authentication - Part 1: General“
  Stand: 2010-07 (Norm)

- ISO/IEC 9798-2 „Information technology - Security techniques - Entity authentication - Part 2: Mechanisms using symmetric encipherment algorithms“
  Stand: 2008-12 (Norm), 2013-02 (Technical Corrigendum)
- ISO/IEC 9798-3 „Information technology - Security techniques - Entity authentication - Part 3: Mechanisms using digital signature techniques“
  Stand: 1998-10 (Norm), 2009-09 (Technical Corrigendum), 2012-03 (Technical Corrigendum)
- DIN EN 12251 „Health informatics - Secure User Identification for Health Care - Management and Security of Authentication by Passwords“
  Stand: 2005-07 (Norm)
- ISO/IEC 15816 „Information technology - Security techniques - Security information objects for access control“
  Stand: 2002-02 (Norm)
- ISO IEC 24760-1 „Information technology — Security techniques — A framework for identity management - Part 1: Terminology and concepts“
  Stand: 2011-02 (Norm)
- ISO IEC 24760-2 „Information technology — Security techniques — A framework for identity management - Part 2: Reference architecture and requirements“
  Stand: 2015-06 (Norm)
- ISO IEC 24760-3 „Information technology — Security techniques — A framework for identity management - Part 3: Practice“
  Stand: 2016-08 (Norm)
- ISO IEC 30107-1 „Information technology - Biometric presentation attack detection - Part 1: Framework“
  Stand: 2016-01 (Norm)
- ISO/IEC DIS 30107-2 „Information technology - Biometric presentation attack detection - Part 2: Data formats“
  Stand: 2016-10 (Entwurf)
- ISO/IEC DIS 30107-3 „Information technology - Biometric presentation attack detection - Part 3: Testing and reporting“
  Stand: 2016-10 (Entwurf)

7.5.3 Berechtigungsmanagement

- ISO/FDIS 21298 „Health informatics - Functional and structural roles“
  Stand: 2016-10 (Draft)
- DIN EN ISO 22600-1 „Privilegienmanagement und Zugriffssteuerung - Teil 1 Übersicht und Policy-Management“
  Stand: 2015-02 (Norm)
- DIN EN ISO 22600-2 „Privilegienmanagement und Zugriffssteuerung - Teil 2 Formale Modelle“
  Stand: 2015-02 (Norm)
- DIN EN ISO 22600-3 „Privilegienmanagement und Zugriffssteuerung - Teil 3 Implementierungen“
  Stand: 2015-02 (Norm)
- ISO/IEC 29146 „Information technology - Security techniques - A framework for access management“
  Stand: 2016-06 (Norm)

7.5.4 Datenschutz

- ISO/IEC 29100 „Information technology - Security techniques - Privacy framework“
  Stand: 2011-12 (Norm)
- ISO/IEC 29101 „Information technology - Security techniques - Privacy architecture framework“
  Stand: 2013-10 (Norm)

7.5.5 Evaluierung

- ISO/IEC 15408-1 „Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model“
  Stand: 2009-12 (Norm)
- ISO/IEC 15408-2 „Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components“
  Stand: 2008-08 (Norm)
- ISO/IEC 15408-3 „Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components“
  Stand: 2008-08 (Norm)
- ISO/IEC TR 15443-1 „Information technology - Security techniques - Security assurance framework - Part 1: Introduction and concepts“
  Stand: 2012-11 (Technische Regel)
- ISO/IEC TR 15443-2 „Information technology - Security techniques - Security assurance framework - Part 2: Analysis“
  Stand: 2012-11 (Technische Regel)
- ISO/IEC TR 15443-3 „Information technology. Security techniques. A framework for IT security assurance. Analysis of assurance methods“
  Stand: 2008-01-31 (Technische Regel)
- ISO/IEC 18045 „Information technology - Security techniques - Methodology for IT security evaluation“
  Stand: 2008-08 (Norm)
- ISO/IEC TR 19791 „Information technology - Security techniques - Security assessment of operational systems“
  Stand: 2010-04 (Technische Regel)
- ISO/IEC 19792 „Information technology - Security techniques - Security evaluation of biometrics“
  Stand: 2009-08 (Norm)

7.5.6 Informationssicherheits-Managementsysteme (ISMS)

- ISO/TR 11633-1 „Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 1: Requirements and risk analysis“
  Stand: 2009-11 (Technische Regel)
- ISO/TR 11633-2 „Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 2: Implementation of an information security management system (ISMS)“
  Stand: 2009-11 (Technische Regel)
- DIN ISO IEC 27000 „IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie“
  Stand: 2015-12 (Entwurf)

- DIN ISO IEC 27001 „IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen“
  Stand: 2015-03 (Norm)
- DIN ISO IEC 27002 „IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management“
  Stand: 2016-11 (Norm)
- ISO/IEC 27003 „Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsystem-Einführungsleitlinie“
  Stand: 2010-02 (Norm) bzw. 2016-12 (Entwurf)
- ISO/IEC 27004 „Informationstechnik - Sicherheitsverfahren - Informationssicherheits-Management - Überwachung, Messung, Analyse und Evaluation“
  Stand: 2016-12 (Norm)
- ISO/IEC 27005 „Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheits-Risikomanagement“
  Stand: 2011-06 (Norm)
- ISO/IEC 27006 „Informationstechnik - IT-Sicherheitsverfahren - Anforderungen an Institutionen, die Audits und Zertifizierungen von Informationssicherheits-Managmentsystemen anbieten“
  Stand: 2015-10 (Norm)
- ISO/IEC 27007 „Informationstechnik - IT-Sicherheitsverfahren - Richtlinien für Informationssicherheits-Managementsystemaudits“
  Stand: 2011-11 (Norm)
- ISO/IEC TR 27008 „Informationstechnik - IT-Sicherheitsverfahren - Richtlinien für Auditoren von Informationssicherheits-controls“
  Stand: 2011-10 (Technische Regel)
- DIN ISO/IEC 27009 „Informationstechnik - IT-Sicherheitsverfahren - Sektorspezifische Anwendung der ISO/IEC 27001 - Anforderungen“
  Stand: 2016-11 (Norm)
- ISO/IEC 27010 „Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagement für sektor- und organisationsübergreifende Kommunikation“
  Stand 2015-11 (Norm)
- ISO/IEC 27011 „Informationstechnik - Sicherheitsverfahren - Leitfaden für Informationssicherheitsmaßnahmen auf Grundlage von ISO/IEC 27002 für Telekommunikationsorganisationen“
  Stand: 2016-12 (Norm)
- ISO/IEC 27013 „Informationstechnik - Sicherheitsverfahren - Leitfaden für die gemeinsame Einführung von ISO/IEC 27001 und ISO/IEC 20000-1“
  Stand: 2015-12 (Norm)
- ISO/IEC 27014 „Informationstechnik - IT-Sicherheitsverfahren - Governance von informationssicherheit“
  Stand: 2013-05 (Norm)
- ISO/IEC TR 27015 „Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheitsmanagement-Leitlinie für Financial services“
  Stand: 2012-12 (Technische Regel)

- ISO/IEC TR 27016 „Informationstechnik - IT-Sicherheitsverfahren - Informationssicherheitsmanagement - organisationelle Wirtschaftlichkeit“
  Stand: 2014-03 (Technische Regel)
- ISO/IEC 27017 „Informationstechnik - Sicherheitsverfahren - Anwendungsleitfaden für Informationssicherheitsmaßnahmen basierend auf ISO/IEC 27002 für Cloud Dienste“
  Stand: 2015-12 (Norm)
- DIN ISO/IEC 27018 „Informationstechnik - Sicherheitsverfahren - Leitfaden zum Schutz personenbezogener Daten (PII) in öffentlichen Cloud-Diensten als Auftragsdatenverarbeitung“
  Stand: 2016-12 (Entwurf)
- DIN ISO/IEC TR 27019 „Informationstechnik - Sicherheitsverfahren - Leitfaden für das Informationssicherheitsmanagement von Steuerungssystemen der Energieversorgung auf Grundlage der ISO/IEC 27002“
  Stand: 2015-03 (Technische Regel)

7.5.7 Dokumentation/digitale Signatur

- DIN 6789 „Dokumentationssystematik - Verfälschungssicherheit und Qualitätskriterien für die Freigabe digitaler Produktdaten“
  Stand: 2013-10 (Norm)

7.5.8 Gesundheitswesen

- ISO/TR 11633-1 „Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 1: Requirements and risk analysis“
  Stand: 2009-11 (Technische Regel)
- ISO/TR 11633-2 „Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 2: Implementation of an information security management system (ISMS)“
  Stand: 2009-11 (Technische Regel)
- DIN EN 12251 „Health informatics - Secure User Identification for Health Care - Management and Security of Authentication by Passwords“
  Stand: 2005-07 (Norm)
- DIN CEN ISO/TS 14265 „Klassifikation des Zwecks zur Verarbeitung von persönlichen Gesundheitsinformationen“
  Stand: 2014-03 (Technische Regel)
- ISO/FDIS 21298 „Medizinische Informatik - Funktionelle und strukturelle Rollen“
  Stand: 2017-07 (Norm)
- ISO/TS 21547 „Security requirements for archiving of electronic health records — Principles“
  Stand: 2010-02 (Vornorm)
- DIN EN ISO 27789 „Audit-Trails für elektronische Gesundheitsakten“
  Stand: 2013-06 (Norm)
- DIN EN ISO 27799 „Sicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO IEC 27002“
  Stand: 2016-12 (Norm)

7.5.9 Hardwarenahe Sicherheitsmaßnahmen

- ISO IEC 11889-1 „Information technology - Trusted Platform Module - Part 1: Overview“
  Stand: 2015-12 (Norm)

- ISO IEC 11889-2 „Information technology - Trusted Platform Module - Part 2: Design principles“
  Stand: 2015-12 (Norm)
- ISO IEC 11889-3 „Information technology - Trusted Platform Module - Part 3: Structures“
  Stand: 2015-12 (Norm)
- ISO IEC 11889-4 „Information technology - Trusted Platform Module - Part 4: Commands“
  Stand: 2015-12 (Norm)
- ISO IEC 19678 „Information Technology - BIOS Protection Guidelines“
  Stand: 2015-05 (Norm)

7.5.10 Löschung

- DIN EN 15713 „Sichere Vernichtung von vertraulichen Unterlagen – Verfahrensregeln“
  Stand: 2009-08 (Norm)
- DIN 66398 „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“
  Stand: 2016-05 (Norm)
- DIN 66399-1 „Vernichten von Datenträgern“, Teil 1: Grundlagen und Begriffe“
  Stand: 2012-10 (Norm)
- DIN 66399-2 „Vernichten von Datenträgern“, Teil 2: Anforderungen an Maschinen zur Vernichtung von Datenträgern“
  Stand: 2012-10 (Norm)
- DIN 66399-3 „Vernichten von Datenträgern“, Teil 3: Prozess der Datenträgervernichtung“
  Stand: 2013-02 (Norm)

7.5.11 Protokollierung

- DIN EN ISO 27789 „Audit-Trails für elektronische Gesundheitsakten“
  Stand: 2013-06 (Norm)

7.5.12 Prozesssteuerung

- ISO ISO IEC TR 15446 „Information technology - Security techniques - Guide for the production of Protection Profiles and Security Targets“
  Stand: 2009-03 (Technische Regel)
- IEC 21827 „Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model® (SSE-CMM®)“
  Stand: 2008-10 (Norm)
- ISO/IEC 27031 „Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity“
  Stand: 2011-03 (Norm)
- DIN EN 61511-1 (VDE 0810-2) „Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 1: Allgemeines, Begriffe, Anforderungen an Systeme, Software und Hardware“
  Stand: 2012-10 (Norm-Entwurf)
- DIN EN 61511-2 „Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 2: Informative Anleitungen zur Anwendung des Teils 1“
  Stand:2013-01 (Entwurf)

- DIN EN 61511-3 „Funktionale Sicherheit - Sicherheitstechnische Systeme für die Prozessindustrie - Teil 3: Informative Anleitung für die Bestimmung der erforderlichen Sicherheits-Integritätslevel“
  Stand:2013-01 (Entwurf)

7.5.13 Risikomanagement/Evaluierung IT-Sicherheit

- ISO IEC 15408-1 „Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model“
  Stand: 2009-12 (Norm)
- ISO/IEC 15408-2 „Security techniques — Evaluation criteria for IT security — Part 2: Security functional requirements“
  Stand: 2008-08 (Norm)
- ISO IEC 15408-3 „Information technology Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components (Corrected version 2011-06-01)“
  Stand: 2008-08 (Norm)
- ISO/IEC 18045 „Information technology - Security techniques - Methodology for IT security evaluation“
  Stand: 2008-08 (Norm)
- ISO IEC 29147 „Information technology - Security techniques - Vulnerability disclosure“
  Stand: 2014-02 (Norm)
- DIN ISO 31000 „Risikomanagement - Grundsätze und Leitlinien“
  Stand: 2011-05 (Norm)

7.5.14 Sicherheitsmaßnahmen

- BS ISO/IEC 24762 „Information technology - Security techniques - Guidelines for information and communications technology disaster recovery services“
  Stand: 2008-02-29 (Norm)
- ISO/IEC 27033-1 „Information technology - Security techniques - Network security - Part 1: Overview and concepts“
  Stand: 2015-08 (Norm)
- ISO/IEC 27033-2 „Information technology - Security techniques - Network security - Part 2: Guidelines for the design and implementation of network security“
  Stand: 2012-08 (Norm)
- ISO/IEC 27033-3 „Information technology - Security techniques - Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues“
  Stand: 2010-12 (Norm)
- ISO/IEC 27033-4 „Information technology - Security techniques - Network security - Part 4: Securing communications between networks using security gateways“
  Stand: 2014-03 (Norm)
- ISO/IEC 27033-5 „Information technology - Security techniques - Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)“
  Stand: 2013-08 (Norm)
- ISO/IEC 27033-6 „Information technology - Security techniques - Network security - Part 6: Securing wireless IP network access“
  Stand: 2016-06 (Norm)

- ISO IEC 27036-1 „Information technology - Security techniques - Information security for supplier relationships - Part 1: Overview and concepts“
  Stand: 2014-04 (Norm)
- ISO/IEC 27036-2 „Information technology - Security techniques - Information security for supplier relationships - Part 2: Requirements“
  Stand: 2014-08 (Norm)
- ISO/IEC 27036-3 „Information technology - Security techniques - Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security“
  Stand: 2013-11 (Norm)
- ISO/IEC 27036-4 „Information technology - Security techniques - Information security for supplier relationships - Part 4: Guidelines for security of cloud services“
  Stand: 2016-10(Norm)

7.5.15 Verschlüsselung

- ISO/IEC 7064 „Information technology - Security techniques - Check character systems“
  Stand: 2003-02 (Norm)
- ISO/IEC 10116 „Information technology - Security techniques - Modes of operation for an n-bit block cipher“
  Stand: 2006-02 (Norm), 2016-08 (Norm-Entwurf)
- ISO/IEC 10118-1 „Information technology - Security techniques - Hash-functions - Part 1: General“
  Stand: 2016-10 (Norm)
- ISO/IEC 10118-2 „Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-bit block cipher“
  Stand: 2010-10 (Norm), 2011-12 (Technical Corrigendum)
- ISO/IEC 10118-3 „Information technology - Security techniques - Hash-functions - Part 3: Dedicated hash-functions“
  Stand: 2004-03 (Norm), 2016-10 (Norm-Entwurf)
- ISO/TR 11636: „Health Informatics - Dynamic on-demand virtual private network for health information infrastructure“
  Stand: 2009-12 (Technische Regel)
- ISO/IEC 18031 „Information technology - Security techniques - Random bit generation“
  Stand: 2011-11 (Norm), 2014-10 (Technical Corrigendum)
- ISO/IEC 18033-1 „Information technology - Security techniques - Encryption algorithms - Part 1: General“
  Stand: 2015-08 (Norm)
- ISO/IEC 18033-2 „Information technology - Security techniques - Encryption algorithms - Part 2: Asymmetric ciphers“
  Stand: 2006-05 (Norm)
- ISO/IEC 18033-3 „Information technology - Security techniques - Encryption algorithms - Part 3: Block ciphers“
  Stand: 2010-12 (Norm)
- ISO/IEC 18033-4 „Information technology - Security techniques - Encryption algorithms - Part 4: Stream ciphers“
  Stand: 2011-12 (Norm)

- ISO/IEC 19772 „Authentifizierte Verschlüsselung“ “
  Stand: 2009-02 (Norm), 2014-09 (Technical Corrigendum 1)
- ISO/IEC 19790 „Information technology - Security techniques - Security requirements for cryptographic modules“
  Stand: 2012-08 (Norm)
- ISO/IEC 24759 „Information technology - Security techniques - Test requirements for cryptographic modules“
  Stand: 2014-02 (Norm), 2016-12 (Norm-Entwurf)
- ISO/IEC 29192-1 „Information technology - Security techniques - Lightweight cryptography - Part 1: General“
  Stand: 2012-06 (Norm)
- ISO/IEC 29192-2 „Information technology - Security techniques - Lightweight cryptography - Part 2: Block ciphers“
  Stand: 2012-01 (Norm)
- ISO/IEC 29192-3 „Information technology - Security techniques - Lightweight cryptography - Part 3: Stream ciphers“
  Stand: 2012-10 (Norm)
- ISO/IEC 29192-4 „Information technology - Security techniques - Lightweight cryptography - Part 4: Mechanisms using asymmetric techniques“
  Stand: 2013-06 (Norm)

7.5.16 Wartung/Fernwartung

- ISO/TR 11633-1 „Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 1: Requirements and risk analysis“
  Stand: 2009-11 (Technische Regel)
- ISO/TR 11633-2 „Health informatics - Information security management for remote maintenance of medical devices and medical information systems - Part 2: Implementation of an information security management system (ISMS)“
  Stand: 2009-11 (Technische Regel)