Bundesamt
für Sicherheit in der
Informationstechnik

Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT

Leitfaden

Erstellt im Auftrag des BSI in Zusammenarbeit mit

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Einleitung ... 5
1.1 Abgrenzung ... 5
1.2 Anwendungshinweise ... 6
2 Vorbereitende Aktivitäten ... 9
2.1 IT-Risikoanalyse als Projekt initialisieren ... 9
2.2 Schutzziele festlegen ... 11
2.3 Untersuchungsbereich abgrenzen ... 13
2.4 Prozesse erheben ... 14
3 Kritikalität analysieren ... 17
3.1 Kritische Prozesse ermitteln ... 18
3.2 IT-Unterstützung ermitteln ... 20
3.3 Kritikalität der IT-Unterstützung bestimmen ... 23
3.4 Kritische IT-Komponenten ermitteln ... 25
4 Risiken identifizieren und bewerten ... 29
4.1 Risikoszenarien ermitteln ... 30
4.2 Eintrittswahrscheinlichkeiten abschätzen ... 34
4.3 Auswirkungen bewerten ... 38
4.4 Risikowert ermitteln ... 40
4.5 Bestehende Maßnahmen berücksichtigen ... 42
5 Risiken behandeln ... 45
5.1 Behandlung der Risiken entscheiden ... 45
5.2 Präventive Maßnahmen bestimmen und Ersatzverfahren vorsehen ... 47
6 Grundlegende Maßnahmen zur IT-Sicherheit ... 53
6.1 Organisation der Informationssicherheit und Notfallmanagement ... 53
6.2 Absicherung des Krankenhausnetzes ... 55
6.3 Absicherung der IT-Systeme ... 57
6.4 Weitere Informationsquellen ... 60
7 Ausblick: Sicherheit aufrechterhalten und weiterentwickeln ... 63
Hilfsmittel ... 65
H 1: Fragenkatalog ... 65
H 2: Kriterien zur Bestimmung der Eintrittswahrscheinlichkeit ... 66
Glossar ... 69
Literaturverzeichnis ... 73

1 Einleitung

Krankenhäuser zählen aufgrund ihrer herausragenden Bedeutung für das Wohlergehen der Bevölkerung zu den **Kritischen Infrastrukturen** unserer Gesellschaft, also zu den Einrichtungen, „deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen“ nach sich ziehen würde.[1] Sie haben daher eine besondere Verpflichtung, die Verfügbarkeit ihrer Dienste und der Prozesse, mit denen diese erbracht werden, sicherzustellen.

In Krankenhäusern werden Geschäftsprozesse, insbesondere auch die Kernprozesse im Bereich der medizinischen und pflegerischen Patientenversorgung, immer stärker durch Informationstechnik (IT) unterstützt. Krankenhausinformationssysteme und den Behandlungsprozess begleitende elektronische Krankenakten gehören in den meisten Einrichtungen schon zum Standard, ebenso die umfassende Vernetzung dieser und weiterer Anwendungssysteme. Neben Vorteilen für die Effizienz der Krankenhausprozesse und die Qualität ihrer Ergebnisse birgt diese Entwicklung aber auch die Gefahr, dass Ausfälle und Störungen der IT wichtige Prozesse erheblich beeinträchtigen und in Folge die Gesundheit und das Leben von Patienten gefährden können. Diese Gefahr ist umso größer, je abhängiger ein Prozess von einer reibungslos funktionierenden IT ist und je schwächer er gegen Risiken abgesichert ist, die mit diesen Abhängigkeiten verbunden sind.

In diesem Dokument wird eine Methode beschrieben, mit der kritische IT-Abhängigkeiten in einem Krankenhaus und daraus erwachsende Risiken für die Patientenversorgung und weitere wichtige Prozesse identifiziert und bewertet werden können. Die Anwendung dieser Vorgehensweise führt zu einer Übersicht potenzieller Risiken, die es erleichtert, Entscheidungen für angemessene Maßnahmen zur Erhöhung der Ausfallsicherheit des Krankenhauses zu treffen. Die Vorgehensweise wird Schritt für Schritt mit konkreten Handlungsanleitungen und ergänzenden Informationen zur praktischen Umsetzung beschrieben.

Der vorliegende Leitfaden ist ein Ergebnis des Projekts „Risikoanalyse Krankenhaus-IT“ (RiKrIT). Das Vorhaben wurde in den Jahren 2011 und 2012 im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) in Kooperation mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK), der Senatsverwaltung für Gesundheit und Soziales (SenGS) des Landes Berlin sowie dem Unfallkrankenhaus Berlin (ukb) durch Auftragnehmer aus Industrie und Wissenschaft durchgeführt.

1.1 Abgrenzung

IT-Risikoanalyse und Risikomanagement Kritischer Infrastrukturen

Die in diesem Dokument beschriebene Vorgehensweise, die aufgrund ihres spezifischen Anwendungsgegenstandes als **IT-Risikoanalyse** bezeichnet wird, ist allgemein anwendbar und kann in bereits existierende Managementkonzepte integriert werden, beispielsweise in das Informationssicherheits- oder Notfallmanagement.

Darüber hinaus kann die IT-Risikoanalyse als weiteres wichtiges Instrument des Risikomanagements von Krankenhäusern angesehen werden, wozu deren Träger respektive Leitungen aufgrund rechtlicher Vorgaben, beispielsweise des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), verpflichtet sein können.[2] Die folgenden beiden Dokumente beschreiben einen Ansatz zum übergeordneten Risiko- und Krisenmanagement Kritischer Infrastrukturen:

- „Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement: Leitfaden für Unternehmen und Behörden“ des Bundesministeriums des Innern [BMI-LF] und
- „Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus: Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens“ des Bundesamts

1 Zur Definition des Begriffs „Kritische Infrastruktur“ siehe [KRITIS-STRAT], Seite 3.
2 Zu den rechtlichen Verpflichtungen zum Risikomanagement siehe [BMI-LF], Seite 11 und [BBK-RM-KH], Seite 6.

für Bevölkerungsschutz und Katastrophenhilfe [BBK-LF], der die in [BMI-LF] genannten Empfehlungen auf die spezifischen Eigenschaften eines Krankenhauses konkretisiert.

In den genannten Leitfäden werden Risiken durch Informationstechnik für die Kritische Infrastruktur Krankenhaus berücksichtigt, jedoch nicht im Detail betrachtet (siehe [BMI-LF], Seite 15 und [BBK-LF], Kapitel 4.2.4). Die vorliegende IT-Risikoanalyse mit speziellem Fokus auf die aus IT-Abhängigkeiten resultierenden Risiken für die Prozesse eines Krankenhauses stellt somit eine Spezialisierung der allgemeinen Risikoanalyse für den Bereich der Informationstechnik dar. Die Methode ist jedoch auch mit anderen Modellen zum Risikomanagement vereinbar.

IT-Risikoanalyse und umfassende Katastrophen

Der Schwerpunkt der in diesem Leitfaden dargestellten IT-Risikoanalyse liegt in der Identifikation und Bewertung IT-spezifischer Risiken, die zu Ausfällen und schwerwiegenden Störungen der Funktionsfähigkeit eines Krankenhauses führen können. Hochwasser, Erdbeben und andere Extremereignisse, die sich umfassend auf ein Krankenhaus auswirken und dessen Prozesse großräumig und unmittelbar gravierend beeinträchtigen, sind weitgehend im Kontext einer auch aus rechtlichen Verpflichtungen erforderlichen umfassenden Risikoanalyse der Kritischen Infrastruktur Krankenhaus zu betrachten. Der drohende Ausfall der IT ist bei solchen Ereignissen, die Existenz und Handlungsfähigkeit der gesamten Einrichtung gefährden, in der Regel nicht das vordringlich zu lösende Problem. Im Rahmen der IT-Risikoanalyse werden derartige Katastrophen daher nur insoweit betrachtet, als sich aus ihnen besondere Konsequenzen für die Informationstechnik ergeben.

IT-Risikoanalyse und Datenschutz

Angesichts des hohen Personenbezugs der vorliegenden Informationen hat der Datenschutz und haben Datenschutzrisiken naturgemäß einen hohen Stellenwert für die Vorkehrungen, die in einem Krankenhaus zur Informationssicherheit zu treffen sind. Im Rahmen der hier beschriebenen IT-Risikoanalyse werden aufgrund ihrer Zielsetzung – dem Schutz der Kritischen Infrastruktur Krankenhaus – Datenschutzaspekte jedoch nicht näher betrachtet. Gleichwohl ist bei der Konkretisierung von Sicherheitsmaßnahmen im Rahmen der Risikobehandlung der Datenschutz angemessen zu berücksichtigen, wann immer personenbezogene oder -beziehbare Daten betroffen sind.

IT-Risikoanalyse und Risikobehandlung

Aufgabe der IT-Risikoanalyse ist die Identifizierung und Bewertung von Ausfallrisiken aufgrund kritischer IT-Abhängigkeiten. Die Behandlung der identifizierten Risiken sowie die Planung und Umsetzung risikomindernder Maßnahmen sind Aufgaben des Risikomanagements im Nachgang der Risikoanalyse. In Kapitel 6 dieses Leitfadens werden hierzu einige allgemeine Empfehlungen gegeben. Für die Umsetzung dieser Empfehlungen und weiterer erforderlicher Sicherheitsmaßnahmen wird auf einschlägige Standards zur Informationssicherheit verwiesen. Am Anfang von Kapitel 5.2 befindet sich hierzu eine Übersicht.

1.2 Anwendungshinweise

Adressatenkreis

Der Leitfaden richtet sich grundsätzlich an Mitarbeiter für den IT-Betrieb und das Sicherheits- und Risikomanagement im Krankenhaus, die sich mit der Durchführung einer IT-Risikoanalyse befassen, aber auch an externe Stellen, z. B. Sicherheitsberater, die entsprechende Dienstleistungen anbieten.

Bei der Anfertigung des Leitfadens wurde berücksichtigt, dass er sowohl Anwendern ohne vertiefte Kenntnisse zur IT-Sicherheit als auch Experten eine Hilfestellung bei der Umsetzung einer IT-Risikoanalyse bietet. Der Leser sollte jedoch über grundlegende Kenntnisse im Bereich Informationssicherheit verfügen.

Neben diesem Leitfaden ist unter dem Titel „Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT – Management-Kurzfassung“ [RiKrIT-ÜB] zusätzlich eine Broschüre zur Sensibilisierung und Information der Leitungsebene verfügbar.

Gliederung des Leitfadens

In Tabelle 1 sind die übergeordneten Phasen und Schritte der in diesem Leitfaden beschriebenen IT-Risikoanalyse und der begleitenden Aktivitäten dargestellt.

Phase	*Arbeitsschritte*
Vorbereitende Aktivitäten	Schritt 1: IT-Risikoanalyse als Projekt initialisieren Schritt 2: Schutzziele festlegen Schritt 3: Untersuchungsbereich abgrenzen Schritt 4: Prozesse erheben
Kritikalität analysieren	Schritt 5: Kritische Prozesse ermitteln Schritt 6: IT-Unterstützung ermitteln Schritt 7: Kritikalität der IT-Unterstützung bestimmen Schritt 8: Kritische IT-Komponenten ermitteln
Risiken identifizieren und bewerten	Schritt 9: Risikoszenarien ermitteln Schritt 10: Eintrittswahrscheinlichkeiten abschätzen Schritt 11: Auswirkungen bewerten Schritt 12: Risikowert ermitteln Schritt 13: Bestehende Maßnahmen berücksichtigen
Risiken behandeln	Schritt 14: Behandlung der Risiken entscheiden Schritt 15: Präventive Maßnahmen bestimmen und Ersatzverfahren vorsehen

Tabelle 1: In diesem Leitfaden beschriebene Arbeitsschritte

Der Leitfaden ist entsprechend dieser Vorgehensweise gegliedert:

- Kapitel 2, **Vorbereitende Aktivitäten**, beschreibt wichtige Vorarbeiten, die Voraussetzung für eine erfolgreiche IT-Risikoanalyse sind. Hierzu zählen insbesondere die organisatorische Verankerung einer solchen Untersuchung in der Einrichtung, die Definition der Schutzziele und die Abgrenzung des Anwendungsbereichs der IT-Risikoanalyse.
- Kapitel 3, **Kritikalität analysieren**, beschreibt eine Methode zur Analyse der Kritikalität der Geschäftsprozesse und deren IT-Abhängigkeiten, um auf dieser Basis die kritischen IT-Komponenten zu identifizieren, deren Gefährdungslage in einer IT-Risikoanalyse zu untersuchen ist.
- Kapitel 4, **Risiken identifizieren und bewerten**, beschreibt den Kern der IT-Risikoanalyse: die Identifikation relevanter Risikoszenarien, die Bestimmung von Eintrittswahrscheinlichkeiten und Schadensauswirkungen sowie darauf fußend die Bewertung des resultierenden Risikos.
- Kapitel 5, **Risiken behandeln**, beschreibt grundsätzliche Optionen zur Behandlung von Risiken und Vorgehensweisen bei der Auswahl risikomindernder Maßnahmen im Nachgang der IT-Risikoanalyse.

Die abschließenden Kapitel 6 und 7 ergänzen die Beschreibung der Vorgehensweise um Hinweise auf grundlegende Maßnahmen zum Schutz gegen kritische IT-Abhängigkeiten (Kapitel 6) und weisen auf die Notwendigkeit einer kontinuierlichen Anpassung und Weiterentwicklung der IT-Risikoanalyse im Krankenhaus hin (Kapitel 7).

Rollen bei der IT-Risikoanalyse

Bei der Vorbereitung, Durchführung und Auswertung der hier dargestellten Methode zur Analyse und Behandlung von IT-Abhängigkeiten sind verschiedene Stellen eines Krankenhauses zu beteiligen. In diesem Leitfaden werden im Wesentlichen die folgenden Rollen unterschieden:

- **Krankenhausleitung** – hierzu zählen Geschäftsführung, Vorstand, ärztliche und kaufmännische Leitung sowie Pflegedienstleitung. Die Krankenhausleitung trägt die Verantwortung für das Risikomanagement in der Einrichtung und kann diese auch nicht an andere Personen delegieren (siehe [BMI-LF], Seite 11 und [BBK-RM-KH], Seite 6).
- **Risikomanagement** – diese Rolle kennzeichnet diejenigen Personen, die in einem weiten Sinn für die Umsetzung des Risikomanagements im Krankenhaus zuständig sind. Zum Risikomanagement zählen unter anderem auch das Sicherheits- und Notfallmanagement. In der Regel werden die damit verbundenen Aufgaben von den Prozessverantwortlichen, beispielsweise den Chefärzten oder Abteilungsleitern, wahrgenommen und es existieren keine Stellen, die exklusiv mit dem Risikomanagement befasst sind. Der Begriff Risikomanagement wird dennoch in diesem Leitfaden verwendet, um die besondere Rolle und die daran geknüpften Aufgaben zu kennzeichnen. Die Verantwortung für das Risikomanagement verbleibt aber in jedem Fall bei der Krankenhausleitung.
- **IT-Verantwortliche bzw. IT-Mitarbeiter** – dieser Personenkreis besteht aus der Leitung der IT-Abteilung sowie den Mitarbeitern, die für den Betrieb der IT-Infrastruktur zuständig sind.
- **Prozessverantwortliche bzw. Prozessbeteiligte** – dies sind alle Personen, die für Geschäftsprozesse oder Fachaufgaben verantwortlich sind. Hierzu zählen insbesondere die ärztlichen Leiter der Fachabteilungen und das dazugehörige Fachpersonal, aber auch die Zuständigen für Infrastruktur oder andere im Rahmen der IT-Risikoanalyse tangierte Krankenhausbereiche (mit Ausnahme der IT).

Daneben werden im Einzelfall weitere Rollen betrachtet, beispielsweise der Datenschutzbeauftragte oder die Mitarbeitervertretung.

Beispiele zur IT-Risikoanalyse

Alle Einzelschritte werden in diesem Leitfaden anhand des fiktiven Krankenhauses „MUSTERKLINIK“ beschrieben. Alle Angaben zu dieser Klinik sind ebenso fiktiv wie ihr Name.

Ergänzende Hilfsmittel

Dieser Leitfaden wird durch die folgenden beiden Hilfsmittel ergänzt, die den Anwender bei der praktischen Umsetzung ausgewählter Arbeitsschritte unterstützen können:

- für Schritt 9, Risikoszenarien ermitteln, das Dokument *Kreuztabelle Bedrohungen – Schwachstellen* [RIKRIT-RISIKEN],
- für Schritt 15, Präventive Schutzmaßnahmen festlegen und Ersatzverfahren vorsehen, das Dokument *Zusammenstellung Bedrohungen – Maßnahmen – IT-Komponentengruppen* [RIKRIT-BMTAB].

Die Anwendung dieser Hilfsmittel wird bei der Erläuterung der betreffenden Schritte in den Kapiteln 4.1 und 5.2 näher beschrieben. Die genannten Dokumente können unter www.kritis.bund.de heruntergeladen werden.

2 Vorbereitende Aktivitäten

Die Durchführung einer IT-Risikoanalyse kann leicht eine sehr hohe Komplexität erreichen und mit einem entsprechend hohen Zeitaufwand verbunden sein, vor allem wenn noch keine verwertbaren Ergebnisse aus früheren Analysen oder verwandten Projekten vorliegen. Durch eine sorgfältige Vorplanung, die frühzeitige Einbeziehung relevanter Wissens- und Verantwortungsträger und klar kommunizierte Entscheidungen kann dieser Aufwand in der Frühphase des Projekts am effektivsten auf ein angemessenes Maß begrenzt werden.

Im Rahmen der vorbereitenden Aktivitäten sind insbesondere die folgenden grundlegenden Arbeiten durchzuführen:

- **Schritt 1:** IT-Risikoanalyse als Projekt initialisieren,
- **Schritt 2:** Schutzziele festlegen,
- **Schritt 3:** Untersuchungsbereich abgrenzen,
- **Schritt 4:** Prozesse erheben.

2.1 IT-Risikoanalyse als Projekt initialisieren

Aufgabe:	Organisatorische Voraussetzungen für das Vorhaben schaffen
Input:	Kein weiterer Input
Ergebnis:	In der Einrichtung etabliertes und mit hinreichenden Ressourcen ausgestattetes Projekt zur IT-Risikoanalyse
Beteiligte:	Krankenhausleitung, Risikomanagement, IT-Verantwortliche, Prozessverantwortliche, Mitarbeitervertretung und gegebenenfalls weitere Wissens- und Verantwortungsträger
Hilfsmittel:	Keine weiteren Hilfsmittel

Ziel der IT-Risikoanalyse ist es, Risiken für die kritischen Prozesse im Krankenhaus zu untersuchen, die sich bei Ausfällen oder Störungen der dort eingesetzten Informationstechnik ergeben können, um auf dieser Grundlage geeignete Maßnahmen zum Schutz der Einrichtung und der Patientenversorgung ableiten zu können. Für eine erfolgreiche Durchführung einer solchen Untersuchung sind einige organisatorische Voraussetzungen zu schaffen, die nachfolgend skizziert werden.

Es muss ein **Projektteam** eingerichtet werden. Der Kern dieses Teams sollte aus IT-Verantwortlichen, Personen, die für die Sicherheitsbelange des Krankenhauses zuständig sind, sowie mindestens einer Person gebildet werden, die einen Gesamtüberblick über die Prozesse des Krankenhauses hat. Dieses Kernteam kann im Verlauf der IT-Risikoanalyse bei Bedarf um fachkundige Mitarbeiter aus den verschiedenen in die Untersuchung einbezogenen Organisationseinheiten ergänzt werden.

Für die allgemeine Akzeptanz ist es außerdem wichtig, dass alle „Schlüsselpersonen", auf deren Mitwirkung und Unterstützung das Vorhaben angewiesen ist, frühzeitig eingebunden werden. Hierzu zählt auch die Mitarbeitervertretung, die bereits vor dem Start über die Ziele der IT-Risikoanalyse und die hierfür erforderlichen Untersuchungsschritte (z. B. geplante Interviews und Erhebungen) informiert werden sollte. Es sollte von Anfang an allen Beteiligten verdeutlicht werden, dass die Untersuchungen und Befragungen weder dazu dienen, entbehrliche Prozesse zu finden, noch dazu, die Leistungen der an den Prozessen beteiligten Mitarbeiter zu bewerten.

Die **Krankenhausleitung** muss aufgrund der weitreichenden Bedeutung einer solchen Untersuchung für das Krankenhaus und der zu treffenden strategischen Entscheidungen **das Vorhaben aktiv unterstützen und die Gesamtverantwortung für dessen Durchführung übernehmen**. Diese Notwendigkeit ergibt sich aus der gesetzlichen Verpflichtung zum Risikomanagement und der daraus resultierenden Gesamtverantwortung der Leitung. Eine IT-Risikoanalyse erfordert den Einsatz von Arbeitszeit und gegebenenfalls weite-

ren Ressourcen. Die Krankenhausleitung muss die erforderlichen personellen, finanziellen und zeitlichen Ressourcen zur Durchführung der Analyse und zu den gegebenenfalls für die Absicherung der Prozesse notwendigen Maßnahmen zur Verfügung stellen.

Die Krankenhausleitung sollte durch **regelmäßige Berichte** in den Fortgang des Projekts eingebunden werden. Dies gilt insbesondere für alle Entscheidungen, die wichtige Weichenstellungen für die Ergebnisse der IT-Risikoanalyse bedeuten, beispielsweise die Definition von Schutzzielen (siehe Kapitel 2.2), die Abgrenzung des Untersuchungsbereichs (siehe Kapitel 2.3), den bewussten Ausschluss wesentlicher Prozesse von einer detaillierten Untersuchung (siehe Kapitel 3.1) oder die Entscheidungen zur Risikobehandlung (siehe Kapitel 5.1).

Je nach Zielsetzung, Aufwand und vorhandenen Kenntnissen zu und Erfahrungen mit einer solchen Untersuchung ist zu entscheiden, ob die IT-Risikoanalyse vollständig in Eigenleistung durchgeführt oder zumindest in Teilen extern beauftragt werden soll.

Wichtige Weichenstellungen für die Durchführung der IT-Risikoanalyse ergeben sich aus den Bezügen der IT-Risikoanalyse zu einem möglicherweise etablierten und ganzheitlich auf die Risiken des Krankenhauses bezogenen **Risikomanagement** (beispielsweise gemäß [BBK-LF]):

- Existiert in der Einrichtung bereits ein übergeordnetes Risikomanagement, sollte die IT-Risikoanalyse in diesen Prozess eingebunden werden. Ergebnisse und Verfahrensweisen der übergeordneten Risikoanalyse sollten für die IT-Risikoanalyse übernommen werden und umgekehrt sollten Ergebnisse der IT-Risikoanalyse in das übergeordnete Risikomanagement einfließen. Die Mitwirkung der für das übergeordnete Risikomanagement Verantwortlichen im Projektteam für die IT-Risikoanalyse ist zu empfehlen.
- Falls die IT im Rahmen der übergeordneten Risikoanalyse bereits erfasst wurde, kann eine IT-Risikoanalyse dazu dienen, diese Untersuchung zu detaillieren. Alternativ kann die IT-Risikoanalyse als eigenständiges Projekt unabhängig von einer gegebenenfalls zu einem früheren Zeitpunkt durchgeführten oder für die Zukunft geplanten umfassenden Krankenhaus-Risikoanalyse durchgeführt werden. Eine zwingende Notwendigkeit zur aufeinander aufbauenden oder gar gleichzeitigen Durchführung besteht nicht.
- Die IT-Risikoanalyse ist auch dann sinnvoll, wenn ein Risikomanagement noch nicht existiert. Gegebenenfalls kann ein solches Projekt auch einen Impuls für ein umfassendes Risikomanagement geben.

So gehen Sie vor

Voraussetzung ist, dass in Ihrer Einrichtung die Bereitschaft zur Durchführung einer Untersuchung kritischer IT-Abhängigkeiten besteht. Zur Initialisierung des Vorhabens beachten Sie die folgenden Punkte:

- Sichern Sie die Unterstützung der Krankenhausleitung für das Vorhaben. Legen Sie fest, wie die Leitung über Berichte und Freigabeprozesse in die IT-Risikoanalyse eingebunden wird.
- Achten Sie bei der Zusammenstellung des Projektteams darauf, dass sowohl die Sicht der Geschäftsprozesse als auch die IT-Sicht in das Vorhaben einfließt. Beteiligen Sie frühzeitig die Mitarbeitervertretung.
- Klären Sie die Bezüge zu einem gegebenenfalls vorhandenen Risikomanagement des Krankenhauses.

2.2 Schutzziele festlegen

Aufgabe:	Festlegen der Schutzziele, die nicht verletzt werden dürfen und an denen die IT-Risikoanalyse auszurichten ist
Input:	Kein weiterer Input
Ergebnis:	Übergeordnete Schutzziele der Einrichtung und darauf bezogene IT-Schutzziele als Grundlage für die Kritikalitätsanalyse und die Risikobehandlung
Beteiligte:	Krankenhausleitung, Risikomanagement
Hilfsmittel:	Keine weiteren Hilfsmittel

Vor Beginn der IT-Risikoanalyse sind die Schutzziele festzulegen, an denen sich diese Untersuchung zu orientieren hat. Schutzziele beschreiben einen herbeizuführenden Sollzustand bezüglich zu schützender Bereiche des Krankenhauses (siehe [BBK-LF], Glossar). Sie dienen als Maßstab für die Ermittlung kritischer Prozesse und deren IT-Abhängigkeiten sowie die Entscheidungen zur Risikobehandlung.

Ausgangspunkt der IT-Risikoanalyse sind die **übergeordneten Schutzziele des Krankenhauses**. Im Mittelpunkt steht dabei – insbesondere auch vor dem Hintergrund der Zugehörigkeit zu den Kritischen Infrastrukturen der Gesellschaft – die **Sicherstellung der Verfügbarkeit** wichtiger Dienstleistungen der Einrichtung. Daraus ergeben sich die folgenden beiden Schutzziele:

- Sicherung der Patientenversorgung und Verhinderung der Gefährdung für Menschenleben (**Schutz der Patienten**),
- wirtschaftliche und rechtliche Existenzsicherung der Einrichtung (**Schutz der Einrichtung**).

Je nach Anwendungskontext der IT-Risikoanalyse können weitere Schutzziele definiert werden, etwa die Erhaltung der Funktionsfähigkeit lebensnotwendiger Bereiche für die Notfallversorgung im Kontext des Krisenmanagements. Dabei sollte berücksichtigt werden, dass die definierten Schutzziele möglichst die Erwartungshaltung aller Beteiligten berücksichtigen.

Die übergeordneten Schutzziele des Krankenhauses liefern Kriterien für die Auswahl von Prozessen im Rahmen der Kritikalitätsanalyse, die mit hoher Priorität abzusichern sind (siehe Kapitel 3.1). Sie setzen außerdem einen Rahmen für die **Schutzziele der Informationstechnik** (kurz **IT-Schutzziele**), anhand derer grundlegende Anforderungen an die IT-Sicherheit beschrieben und die Auswirkungen von IT-Störungen bewertet werden können.

Für die Definition dieser IT-Schutzziele können die drei in der Informationssicherheit üblichen Grundwerte **Verfügbarkeit**, **Integrität** und **Vertraulichkeit** herangezogen werden. Dem übergeordneten Schutzziel der Einrichtung entsprechend werden diese drei Grundwerte allerdings im Rahmen der IT-Risikoanalyse nicht als gleichrangig betrachtet, sondern sind untereinander priorisiert. An oberster Stelle steht die Sicherung der Verfügbarkeit von Anwendungen und IT-Systemen sowie der Verfügbarkeit und Integrität der mit diesen verknüpften Informationen. Das Schutzziel der Vertraulichkeit wird zwar ebenfalls in die Betrachtung einbezogen, allerdings unter dem Blickwinkel der Folgen betrachtet, die sich aus einer Verletzung dieses Schutzziels für die Verfügbarkeit und Integrität ergeben können.

Hinweise

Schutzziele und übergeordnetes Risikomanagement
Die Formulierung von Schutzzielen ist ein wesentliches Element des übergeordneten Risikomanagements. Falls ein solches bereits etabliert ist, sind die Schutzziele der Einrichtung schon definiert und sollten für die IT-Risikoanalyse übernommen werden.

Aufgrund ihrer Verantwortung für das Risikomanagement, müssen die Schutzziele in enger Abstimmung mit der Krankenhausleitung festgelegt werden.

Konzentration auf das übergeordnete Schutzziel „Schutz der Patienten“
Der vorliegende Leitfaden beschränkt sich zur Darstellung der Methode zur IT-Risikoanalyse aus Gründen der Übersichtlichkeit ausschließlich auf das übergeordnete Schutzziel „Schutz der Patienten“. Weitere mögliche Schutzziele, beispielsweise in Bezug auf wirtschaftliche und rechtliche Aspekte der Einrichtung, werden nicht betrachtet.

So gehen Sie vor

- Legen Sie in Abstimmung mit der Krankenhausleitung die für die IT-Risikoanalyse relevanten übergeordneten Schutzziele der Einrichtung fest. Nehmen Sie in Abhängigkeit vom Anwendungskontext gegebenenfalls eine Priorisierung vor. So ist beispielsweise vor dem Hintergrund einer für den Krisenfall vorgesehenen notwendigen Minimalversorgung der Schutz der Patienten höher zu bewerten als der wirtschaftliche Schutz der Einrichtung.
- Definieren Sie für die übergeordneten Schutzziele auf der zweiten Zielebene die IT-Schutzziele basierend auf den Grundwerten der Informationssicherheit (Verfügbarkeit, Integrität, Vertraulichkeit).
- Dokumentieren Sie alle Schutzziele und sichern Sie die Zustimmung der Krankenhausleitung für die festgelegten Definitionen.

Beispiel

Im fiktiven Krankenhaus MUSTERKLINIK hat die Krankenhausleitung beschlossen, die IT-Abhängigkeiten der Prozesse der Einrichtung einer Risikoanalyse zu unterziehen. Hohe Priorität hat der Schutz der Patienten. Wirtschaftliche und rechtliche Belange sollen nicht betrachtet werden. Das übergeordnete Schutzziel der Einrichtung „Schutz der Patienten“ wird von der hierfür eingesetzten Arbeitsgruppe für die IT-Risikoanalyse wie in Tabelle 2 definiert und mit der Krankenhausleitung abgestimmt.

Übergeordnetes Schutzziel	*Definition*
Schutz der Patienten	Der gesundheitliche Zustand eines Patienten darf sich **nicht** aufgrund unterbleibender oder qualitativ/quantitativ eingeschränkter Behandlung bedingt durch Ausfälle oder Störungen der IT im Krankenhaus verschlechtern.

Tabelle 2: Definition des übergeordneten Schutzziels „Schutz der Patienten“

An diesem Schutzziel ausgerichtet werden die IT-Schutzziele wie folgt definiert:

IT-Schutzziele	*Übergeordnetes Schutzziel: Schutz der Patienten*
Verfügbarkeit	IT-Störungen dürfen nicht dazu führen, dass die medizinischen Versorgungskapazitäten nicht mehr in angemessener Qualität und Quantität aufrechterhalten werden können.
Integrität	IT-Störungen dürfen nicht dazu führen, dass Daten verfälscht werden, deren Richtigkeit für die Versorgung eines Patienten unbedingt erforderlich ist.
Vertraulichkeit	IT-Störungen dürfen nicht dazu führen, dass Daten, • deren Bekanntwerden sekundär zu einer Beeinträchtigung der Verfügbarkeit oder Integrität von Systemen und/oder Daten führt oder • die für die sichere Versorgung eines Patienten nur einem berechtigten Personenkreis bekannt sein dürfen (z. B. Personen, die unter den Zeugenschutz gestellt sind oder Personen des öffentlichen Interesses), unberechtigten Dritten zugänglich werden.

Tabelle 3: Auf das übergeordnete Schutzziel „Schutz der Patienten“ bezogene Definitionen der IT-Schutzziele

2.3 Untersuchungsbereich abgrenzen

Aufgabe:	Festlegen, für welchen Ausschnitt des Krankenhauses die IT-Risikoanalyse durchgeführt werden soll
Input:	Beschreibung der Aufbau- und Ablauforganisation des Krankenhauses
Ergebnis:	Beschreibung des abgegrenzten Untersuchungsbereichs
Beteiligte:	IT-Verantwortliche, Risikomanager, Prozessverantwortliche, Krankenhausleitung
Hilfsmittel:	Keine weiteren Hilfsmittel

Im Rahmen der vorbereitenden Aktivitäten muss entschieden werden, welcher Ausschnitt des Krankenhauses Gegenstand der IT-Risikoanalyse sein soll und welche Teile nicht betrachtet werden sollen. Dieser Ausschnitt wird als **Untersuchungsbereich** der IT-Risikoanalyse bezeichnet. Er kann die gesamte Einrichtung umfassen, aber auch auf einzelne Standorte, Gebäude oder organisatorische Einheiten begrenzt werden.

Hat ein Krankenhaus mehrere Standorte mit dezentralem IT-Betrieb, kann es sinnvoll sein, die Untersuchung jeweils für einen einzelnen, räumlich abgetrennten Standort durchzuführen und die Ergebnisse später zusammenzuführen (siehe auch [BBK-LF], Seite 26). Werden die IT-Dienstleistungen für mehrere oder alle Standorte zentral bereitgestellt, so ist zu überlegen, ob wiederum durch eine übergreifende Untersuchung Vorteile entstehen können.

In allen Fällen sollte der Untersuchungsbereich in sich abgeschlossen sein und die Organisationseinheiten vollständig enthalten, die aus medizinischer, pflegerischer oder administrativer Sicht zur Funktion oder Unterstützung der Prozesse benötigt werden. Die vollständige Abdeckung technischer Abhängigkeiten durch die IT wird im Verlauf der Kritikalitätsanalyse (siehe Kapitel 3.2) sichergestellt.

Da der Aufwand für die nachfolgenden Schritte steigt, je weiter der Untersuchungsbereich gewählt wird, ist es, etwa bei begrenzten Ressourcen für die IT-Risikoanalyse, durchaus zulässig, sich auf einen sinnvoll abgegrenzten Ausschnitt des Krankenhauses zu beschränken. Dies können beispielsweise solche Organisationseinheiten sein, für die eine IT-Risikoanalyse aus Sicht der Krankenhausleitung besonders dringlich erscheint.

Hinweis

Zustimmung der Krankenhausleitung
Die Entscheidung zur Abgrenzung des Untersuchungsbereichs muss von der Krankenhausleitung getragen werden, da sie die Verantwortung für das Risikomanagement trägt. Ihre Zustimmung ist daher erforderlich.

So gehen Sie vor

- Legen Sie den Untersuchungsbereich eindeutig fest. Achten Sie darauf, dass dieser in sich abgeschlossen ist und externe Schnittstellen, beispielsweise zu IT-Dienstleistern, klar definiert sind.
- Sichern Sie die Zustimmung der Krankenhausleitung für den gewählten Untersuchungsbereich.

Beispiel

In der MUSTERKLINIK hat die Krankenhausleitung beschlossen, die IT-Risikoanalyse zunächst im kleinen Umfang zu erproben, um erste Erfahrungen mit der Anwendung dieser Vorgehensweise zu sammeln.

Um einen sinnvoll abgegrenzten Untersuchungsbereich zu erhalten, beschließt das Projektteam in Abstimmung mit der Leitung, sich an einem generischen Behandlungsprozess eines Patienten von der Aufnahme bis zur Entlassung zu orientieren (wie in Abbildung 1 schematisch dargestellt).

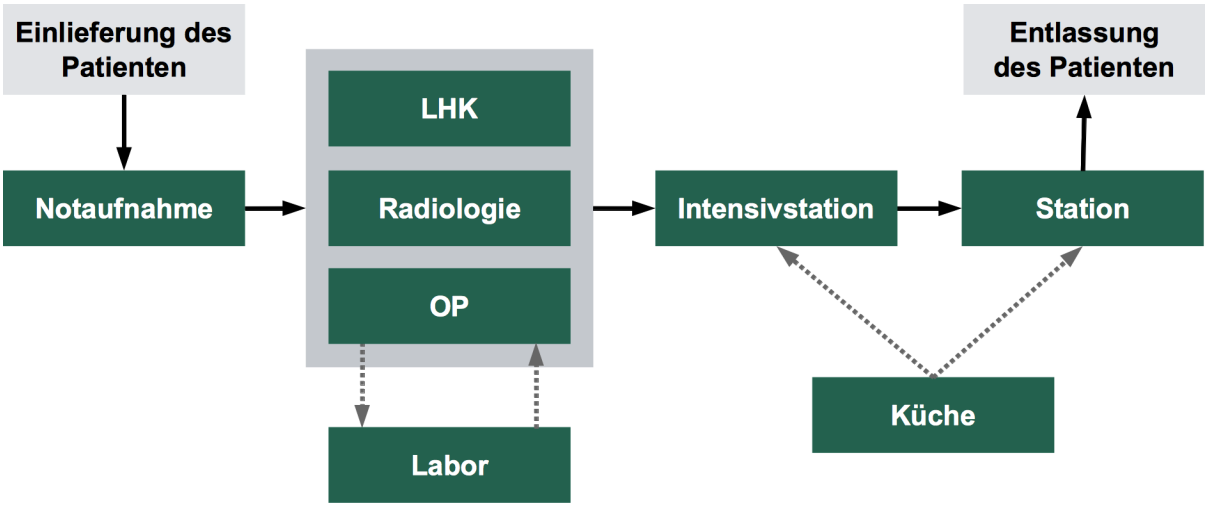

Abbildung 1: Ablaufschema Patientendurchlauf

Bestandteil des Untersuchungsbereichs sind alle Organisationseinheiten, die am medizinischen Behandlungsprozess beteiligt sind (z. B. Intensivstation, Radiologie oder Linksherzkatheter – LHK) sowie einige Einheiten, die unterstützend tätig sind (beispielsweise die Küche). Administrative Einheiten des Krankenhauses (z. B. die Personalabteilung oder die Buchhaltung) werden nicht in den Untersuchungsbereich aufgenommen.

2.4 Prozesse erheben

Aufgabe:	Erheben und Beschreiben der zum Untersuchungsbereich gehörenden Prozesse
Input:	Beschreibung des abgegrenzten Untersuchungsbereichs
Ergebnis:	Prozessübersicht des Untersuchungsbereichs
Beteiligte:	Prozessverantwortliche, Krankenhausleitung
Hilfsmittel:	Fragen zur Prozesserhebung in Abschnitt H 1: Fragenkatalog

Für die Ermittlung der kritischen Prozesse (siehe Kapitel 3.1) ist eine Gesamtübersicht der zum Untersuchungsbereich gehörenden Prozesse notwendig. Diese Prozessübersicht sollte die zugehörigen Kernprozesse und die Unterstützungsprozesse enthalten:

- **Kernprozesse** sind alle Prozesse zur pflegerischen und medizinischen Patientenversorgung, z. B. Behandlung eines Notfallpatienten, Aufnahme, medizinische Diagnostik, medizinische Behandlung, Intensivmedizin, radiologische Untersuchung, Pflege und Entlassung.
- **Unterstützungsprozesse** sind alle Prozesse, die für den reibungslosen Ablauf der Kernprozesse benötigt werden. Beispiele sind Verpflegung, Beschaffung von medizinischem Verbrauchsmaterial und Implantaten, Entsorgung biologischen Materials.

Wenn bereits eine aktuelle Prozessübersicht existiert, beispielsweise weil diese für ein prozessorientiertes Qualitätsmanagement nach DIN EN ISO 9001:2008 [ISO 9001] angefertigt wurde, kann sie für die IT-Risikoanalyse herangezogen werden. Anderenfalls ist für diese Untersuchung eine eigene Prozesserhebung durch-

zuführen. Hierbei ist von entscheidender Bedeutung, dass die Prozessübersicht alle für den Untersuchungsbereich wesentlichen Prozesse in der notwendigen Detailtiefe umfasst.

Prozesse können in Teilprozesse zerlegt werden, beispielsweise der Patientendurchlauf in die Teilprozesse „Aufnahme", Behandlung" und „Entlassung". Jeder Teilprozess ist selbst wieder ein Prozess, der weiter zerlegt werden kann, der Behandlungsprozess etwa in Teilprozesse wie „Intensivbehandlung", „Radiologische Untersuchung" und „Operation". Im Prinzip obliegt es jeder Einrichtung selbst, zu entscheiden, wie feingliedrig diese Zerlegung in Teilprozesse sein soll. Je detaillierter die Prozesse aufgeschlüsselt werden, desto aussagekräftiger kann die IT-Risikoanalyse werden. Andererseits produziert ein zu großer Detaillierungsgrad einen hohen Aufwand für die Prozesserhebung und die nachfolgenden Schritte der Untersuchung.

Gleiches gilt für den Umfang der Informationen, die zu einem Prozess ermittelt und dokumentiert werden. Wird die Prozesserhebung im Rahmen der IT-Risikoanalyse durchgeführt und ist sie ausschließlich für diesen Zweck erforderlich, genügen für den Einstieg in die IT-Risikoanalyse vergleichsweise wenige Angaben zur Beschreibung eines Prozesses. Dies sind neben einer eindeutigen Kennzeichnung und einer Beschreibung seiner Aufgabe Angaben zu den Schnittstellen mit anderen Prozessen (Vorgänger- und Nachfolgeprozess, benötigter Input, Output).

Diese Informationen können auf unterschiedlichen Wegen erhoben werden. Ein übliches Mittel sind Interviews in den einzelnen Organisationseinheiten des Untersuchungsbereichs. Gegebenenfalls genügt es aber auch, die Prozesserhebung im Rahmen eines Workshops des IT-Risikoanalyse-Teams auf der Grundlage von Beschreibungen der Aufbau- und Ablauforganisation des Krankenhauses zusammenzustellen und fehlende Informationen nur bei Bedarf durch gezielte Befragungen zu ergänzen.

Hinweis

Erhebung von Informationen für die IT-Risikoanalyse
Für die nachfolgenden Schritte der IT-Risikoanalyse werden weitere Informationen zu den Prozessen benötigt. Dazu zählen insbesondere Angaben zu den eingesetzten IT-Anwendungen und deren Kritikalität (siehe Kapitel 3.3) sowie zu der nötigen technischen Infrastruktur für den Betrieb dieser Anwendungen.

In dem vorliegenden Leitfaden werden die notwendigen Informationen in den entsprechenden Arbeitsschritten im Rahmen von Interviews erhoben. Dieses Vorgehen ist zu empfehlen, da beispielsweise Informationen zu den IT-Anwendungen und IT-Abhängigkeiten nur für solche Prozesse erfasst werden müssen, die im Hinblick auf die formulierten Schutzziele als kritisch einzustufen sind (siehe Kapitel 3.1) und auf die sich die die weiteren Schritte fokussieren sollten.

Alternativ können alle relevanten Informationen bereits bei der Prozesserhebung ermittelt werden. Dies bietet sich jedoch nur dann an, wenn es in dem für die IT-Risikoanalyse gesetzten Zeitrahmen nicht möglich ist, diese Informationen in der gewünschten Qualität in mehreren Gesprächsterminen zu erhalten.

Abschnitt H 1: Fragenkatalog enthält eine Zusammenstellung von Fragen zur Erhebung der erforderlichen Informationen.

So gehen Sie vor

Ausgangspunkt ist ein abgegrenzter Untersuchungsbereich.

- Falls bereits eine Prozessübersicht für den Untersuchungsbereich vorliegt, übernehmen Sie diese und prüfen Sie deren Aktualität und Vollständigkeit. Nehmen Sie erforderliche Anpassungen vor. Falls noch keine Prozessübersicht existiert, erstellen Sie eine solche basierend auf der Betrachtung der Aufbau- und Ablauforganisation in dem festgelegten Untersuchungsbereich.
- Achten Sie auf einen angemessenen Detaillierungsgrad der erfassten Prozesse und Teilprozesse.

Ergebnis des Arbeitsschritts ist eine Übersicht über die Prozesse des abgegrenzten Untersuchungsbereichs.

Beispiel

Für die Prozesserhebung in der MUSTERKLINIK werden Interviews mit Mitarbeitern der in den Untersuchungsbereich einbezogenen Organisationseinheiten geführt, unter anderem in der Notaufnahme, der Abteilung „Linksherzkatheter (LHK)“, der Radiologie, der OP-Abteilung, dem Labor, auf den Stationen (darunter der Intensivstation) und in der Küche (siehe Abbildung 1). Die identifizierten Prozesse (z. B. „Intensivbehandlung“, „Radiologische Diagnostik“, „Operation“, „Verpflegung“) werden tabellarisch zusammengestellt (siehe Tabelle 4). Hierbei werden einzelne Prozesse weiter detailliert, beispielsweise der in der Intensivstation angesiedelte Prozess „Intensivbehandlung“ in die drei Teilprozesse „Aufnahme“, „Behandlung“ sowie „Verlegung/Entlassung“.

Organisationseinheit	***Prozess***
Intensivstation	Aufnahme
	Behandlung
	Verlegung/Entlassung
Radiologie	Radiologische Diagnostik
Chirurgische Station	Stationäre Behandlung
Notaufnahme	Notaufnahme
Labor	Probenbestätigung
	Probenverteilung
	Befundrückmeldung
	Blutkonservenbereitstellung
Küche	Verpflegung

Tabelle 4: Beispiel für die tabellarische Prozessübersicht in der MUSTERKLINIK

3 Kritikalität analysieren

Ziel der Kritikalitätsanalyse ist es, kritische IT-Abhängigkeiten der Prozesse des Untersuchungsbereichs zu erkennen und diejenigen Bestandteile der IT-Infrastruktur zu identifizieren, deren Ausfall oder Störung zu schwerwiegenden Beeinträchtigungen kritischer Krankenhausprozesse führen würde.

Zu diesem Aufgabenblock gehören die folgenden Teilschritte (siehe Abbildung 2):

- **Schritt 5**: Kritische Prozesse ermitteln – Identifizieren derjenigen Prozesse, deren Störung oder Ausfall die übergeordneten Schutzziele der Einrichtung in schwerwiegender Weise verletzen würde,
- **Schritt 6:** IT-Unterstützung ermitteln – Zusammenstellen der in den kritischen Prozessen eingesetzten IT-Anwendungen,
- **Schritt 7:** Kritikalität der IT-Unterstützung bestimmen – Identifizieren derjenigen IT-Anwendungen, deren Störung oder Ausfall sich schwerwiegend auf die Funktionsfähigkeit der kritischen Prozesse auswirken würde,
- **Schritt 8**: Kritische IT-Komponenten ermitteln – Zusammenstellung der technischen Komponenten, die für den Betrieb der kritischen Anwendungen benötigt werden.

Aus Sicht der Anwender stellt sich ein IT-Ausfall als Ausfall der IT-Anwendung dar. Aus dem Blickwinkel der IT-Risikoanalyse ist darüber hinaus nach den Ursachen des IT-Ausfalls zu fragen. Diese sind aber nicht in der IT-Anwendung als solcher anzusiedeln, sondern sie liegen als Störung oder Ausfall einer oder mehrerer IT-Komponenten begründet. Daher ist das Ergebnis der Kritikalitätsanalyse eine Liste der in den folgenden Schritten der IT-Risikoanalyse zu betrachtenden kritischen IT-Komponenten.

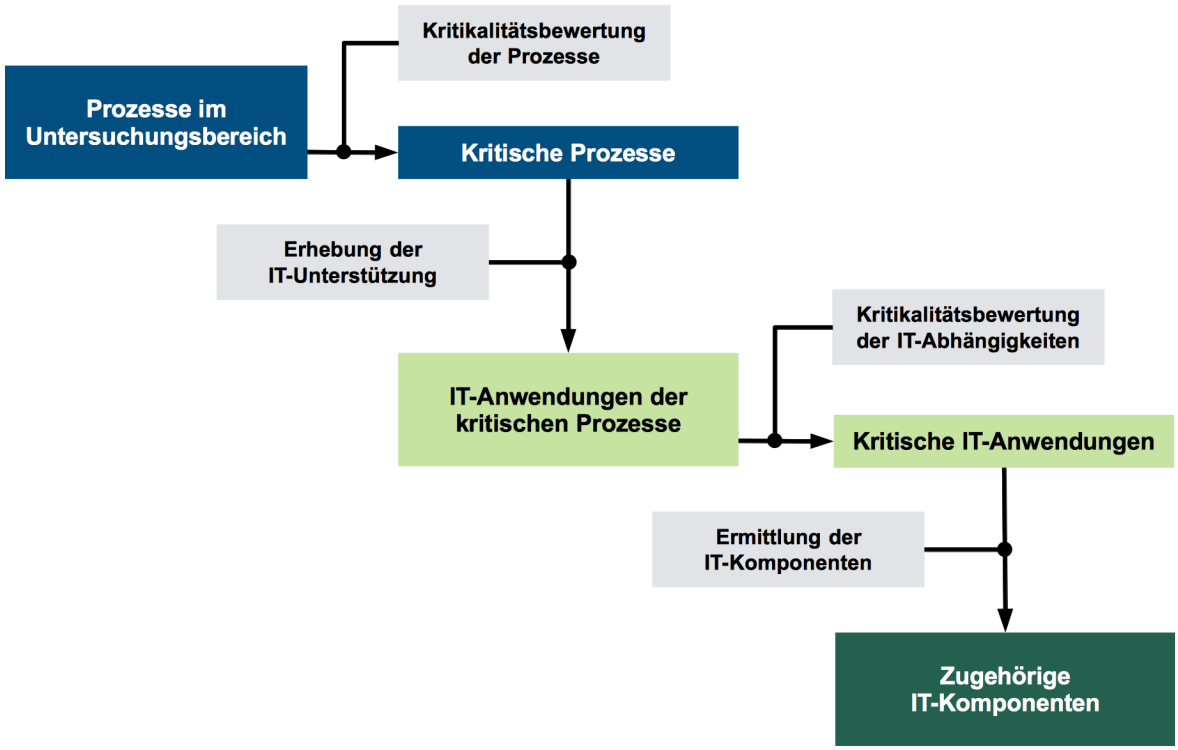

Abbildung 2: Ablauf der Kritikalitätsanalyse

3.1 Kritische Prozesse ermitteln

Aufgabe:	Identifizieren der kritischen Prozesse anhand der definierten Schutzziele der Einrichtung
Input:	Prozessübersicht des Untersuchungsbereichs
Ergebnis:	Liste der kritischen Prozesse im Untersuchungsbereich
Beteiligte:	Prozessverantwortliche, Krankenhausleitung
Hilfsmittel:	Übergeordnete Schutzziele der Einrichtung (als Beispiel siehe Tabelle 2); Fragen zur Bestimmung der Kritikalität von Prozessen in Abschnitt H 1: Fragenkatalog

In diesem Teilschritt der Kritikalitätsanalyse werden aus der Prozessübersicht des Untersuchungsbereichs diejenigen Prozesse ausgewählt, deren Ausfall oder Störung zu schwerwiegenden Verletzungen der Schutzziele der Einrichtung führen würde. Diese Prozesse werden als **kritische Prozesse** bezeichnet.

Zur Auswahl der kritischen Prozesse sind geeignete **Kriterien** zu formulieren, deren Anzahl und Art in die Entscheidungsfreiheit des jeweiligen Krankenhauses gestellt ist. Beispielsweise benennt hierzu der Leitfaden des Bundesministeriums des Innern (siehe [BMI-LF], Seite 16) als mögliche Kriterien:

- die Auswirkungen eines Prozessausfalls auf Leben und Gesundheit,
- der Umfang eines Prozessausfalls,
- den Zeitpunkt, an dem die Auswirkungen eines Ausfalls als kritisch anzusehen sind,
- die vertragliche, ordnungspolitische oder gesetzliche Relevanz der Ausfallfolgen,
- die mit einem Ausfall verbundenen wirtschaftlichen Schäden sowie
- die potenziellen Auswirkungen eines Ausfalls auf die Umwelt.

In diesem Leitfaden wird ebenfalls empfohlen, diese Festlegung mithilfe einfacher Prüffragen zu treffen. Diese sind **aus den übergeordneten Schutzzielen der Einrichtung abzuleiten**. Entsprechend dem Ziel „Schutz des Patienten“, das in Tabelle 2 definiert wurde, sind beispielsweise Ausfälle von Prozessen, die für die Patientenversorgung und das Leben und die Gesundheit der Patienten (Kernprozess) unmittelbar oder (Unterstützungsprozess) mittelbar wichtig sind, üblicherweise bereits nach sehr kurzer Zeit als kritisch zu bezeichnen, sodass sich eine entsprechend formulierte Prüffrage als Auswahlkriterium anbietet. Abschnitt H 1: Fragenkatalog enthält einige Beispiele für solche Fragestellungen.[3]

Darüber hinaus wird empfohlen, die Bestimmung der Prozesskritikalität als reine **Ja-Nein-Entscheidung** durchzuführen, also auf eine differenzierte Betrachtung und eine dadurch mögliche weitergehende Priorisierung von Prozessen zu verzichten, wie sie beispielsweise im Rahmen des Notfallmanagements (siehe etwa [BSI 100-4]) in einer sogenannten „Business Impact“-Analyse (Schadensfolgeanalyse) üblich ist. Sollte eine solche priorisierte Zusammenstellung der Prozesskritikalität bereits vorliegen, kann sie jedoch selbstverständlich auch für die IT-Risikoanalyse hinzugezogen werden.

Hinweise

Sorgfältige Auswahl der kritischen Prozesse
Als unkritisch eingestufte Prozesse werden im Verlauf der Untersuchung nicht weiter betrachtet. Die Auswahl kritischer Prozesse ist daher mit viel Sorgfalt vorzunehmen, damit im Fortgang der Untersuchung keine kritischen IT-Abhängigkeiten übersehen werden. Hierzu gehört auch, dass die verwendeten Auswahlkriterien eindeutig definiert sind, zwischen den Beteiligten und auch mit der Krankenhausleitung abgestimmt werden und zusammen mit den aus ihnen erfolgten Entscheidungen dokumentiert werden.

3 Im Leitfaden des BBK [BBK-LF], Seite 38) werden in ähnlicher Weise aus den Schutzzielen abgeleitete Fragestellungen für die Bestimmung der Prozesskritikalität empfohlen.

Behandlung von Zweifelsfällen
Wenn im Rahmen der Kritikalitätsanalyse ein Prozess aufgrund der gewählten Kriterien als unkritisch eingestuft wird und Zweifel bestehen, ob diese Einstufung auch tatsächlich richtig ist, ist es zulässig den Prozess als kritisch einstufen. Der Ausschluss eines als kritisch eingestuften Prozesses aus dem Fortgang der IT-Risikoanalyse sollte hingegen vermieden werden und ist allenfalls nur nach Rücksprache mit den fachlich Verantwortlichen und mit Zustimmung des Risikomanagements zulässig. Es gilt als Grundsatz, dass es besser ist, einen kritischen Prozess zu viel in der IT-Risikoanalyse zu betrachten als einen zu wenig.

Information und Kommunikation
Die Mitarbeiter sind ausreichend darüber zu informieren, dass die Einstufung eines Prozesses als kritisch oder unkritisch keine Aussage über die Wertschätzung des betreffenden Prozesses und der Aufgaben der an ihm beteiligten Mitarbeiter ist.

Einbeziehung bestehender Ergebnisse
Unter Umständen wurde für den Untersuchungsbereich bereits eine Untersuchung der Kritikalität von Prozessen durchgeführt, beispielsweise im Rahmen einer früheren Risikoanalyse. In einem solchen Fall können deren Ergebnisse für die IT-Risikoanalyse übernommen werden. Hierbei ist jedoch zu prüfen, ob die Untersuchung noch aktuell ist und die Kriterien zur Auswahl kritischer Prozesse mit den Schutzzielen der IT-Risikoanalyse übereinstimmen und zu vergleichbaren Ergebnissen führen würden. Gegebenenfalls sind Anpassungen erforderlich.

So gehen Sie vor

Ausgangspunkt ist die Prozessübersicht zu dem Untersuchungsbereich.

- Definieren Sie geeignete Kriterien für die Auswahl kritischer Prozesse. Orientieren Sie sich bei der Formulierung dieser Kriterien an den übergeordneten Schutzzielen der Einrichtung.
- Wenn im Rahmen einer übergeordneten Risikoanalyse, des Notfallmanagements oder anderer Planungen eine Zusammenstellung kritischer Prozesse bereits vorgenommen wurde, übernehmen Sie diese Ergebnisse für die IT-Risikoanalyse. Prüfen Sie aber auf jeden Fall die Aktualität und Eignung der Untersuchung und nehmen Sie erforderliche Anpassungen vor.
- Falls eine solche Untersuchung noch nicht durchgeführt wurde, bewerten Sie die Kritikalität der Prozesse anhand der vorab definierten Kriterien.
- Prüfen Sie abschließend alle Entscheidungen auf Plausibilität und nehmen Sie erforderliche Korrekturen vor.

Ergebnis ist eine Zusammenstellung der kritischen Prozesse im festgelegten Untersuchungsbereich.

Beispiel

In der MUSTERKLINIK werden die kritischen Prozesse in einem Workshop des Projektteams ausgewählt.

Ausgehend von dem übergeordneten Schutzziel „Schutz der Patienten“ einigt sich das Projektteam darauf, als Auswahlkriterium die folgende Frage zu verwenden:

Wirkt sich der Ausfall des jeweils betrachteten Prozesses bereits nach kurzer Zeit (spätestens nach zwei Stunden) so auf die Patientenversorgung aus, dass gesundheitliche Folgen für die Patienten drohen?

Aufgrund dieses Kriteriums werden unter anderem die Kernprozesse „Intensivbehandlung“, „Stationäre Behandlung“, „Notaufnahme“, „Radiologische Diagnostik“ und „Laboruntersuchung“ sowie Unterstützungsprozesse wie „Pflege/Wartung Medizintechnik“ und „Haustechnik“ als kritisch eingestuft.

Zu den Prozessen, die als unkritisch eingestuft und daher in der Folge nicht mehr weiter untersucht werden, gehört unter anderem der Prozess „Verpflegung“, der in der Organisationseinheit „Küche“ angesiedelt ist. Tabelle 5 enthält einen Auszug aus den Ergebnissen des Workshops.

Organisations-einheit	*Prozess*	*Kritikalität (Ja, Nein)*	*Begründung*
Intensivstation	Aufnahme	Ja	Verzögerungen können sich schon nach kurzer Zeit gravierend auf die Gesundheit eines Patienten auswirken.
	Behandlung	Ja	Verzögerungen können sich schon nach kurzer Zeit gravierend auf die Gesundheit eines Patienten auswirken.
	Verlegung/Entlassung	Nein	Verzögerungen im Rahmen des festgelegten Kriteriums wirken sich nicht kritisch auf die Gesundheit eines Patienten aus.
Radiologie	Radiologische Diagnostik	Ja	Verzögerungen können sich schon nach kurzer Zeit gravierend auf die Gesundheit eines Patienten auswirken.
Chirurgische Station	Stationäre Behandlung	Ja	Verzögerungen können sich schon nach kurzer Zeit gravierend auf die Gesundheit eines Patienten auswirken.
Notaufnahme	Notaufnahme	Ja	Verzögerungen können sich schon nach kurzer Zeit gravierend auf die Gesundheit eines Patienten auswirken.
Küche	Verpflegung	Nein	Auch längere Ausfälle können leicht überbrückt werden, da im Notfall erforderliche Verpflegung extern angeliefert werden kann.

Tabelle 5: Beispiel für die Bewertung der Prozesskritikalität in der MUSTERKLINIK

3.2 IT-Unterstützung ermitteln

Aufgabe:	Ermitteln der IT-Unterstützung für die kritischen Prozesse
Input:	Liste der kritischen Prozesse des Untersuchungsbereichs
Ergebnis:	Zusammenstellung der in den kritischen Prozessen eingesetzten IT-Anwendungen
Beteiligte:	Prozessverantwortliche, Prozessbeteiligte, IT-Verantwortliche
Hilfsmittel:	Fragen zur Ermittlung der IT-Unterstützung in Abschnitt H 1: Fragenkatalog

Für die in Kapitel 3.1 identifizierten kritischen Prozesse wird in einem mehrstufigen Verfahren ermittelt, welche IT-Anwendungen für ihre Funktionsfähigkeit erforderlich sind. Um ein für die weitere IT-Risikoanalyse verwertbares Ergebnis zu erzielen, müssen dabei zwei Sichten auf die prozessunterstützende IT zusammengeführt werden:

- die **Anwendersicht**, die Aufschluss darüber gibt, welche **IT-Anwendungen** und Teilfunktionen dieser IT-Anwendungen für welche Aufgaben benutzt werden und wie kritisch diese IT-Unterstützung für die jeweiligen Aufgaben ist (siehe hierfür Kapitel 3.3), sowie
- die **IT-Sicht** , die aufzeigt, welche **IT-Komponenten** nötig sind, damit die IT-Anwendungen korrekt funktionieren können (siehe hierfür Kapitel 3.4).

Die folgende Abbildung 3 veranschaulicht die Zusammenhänge zwischen Krankenhausprozessen, IT-Anwendungen und IT-Komponenten.

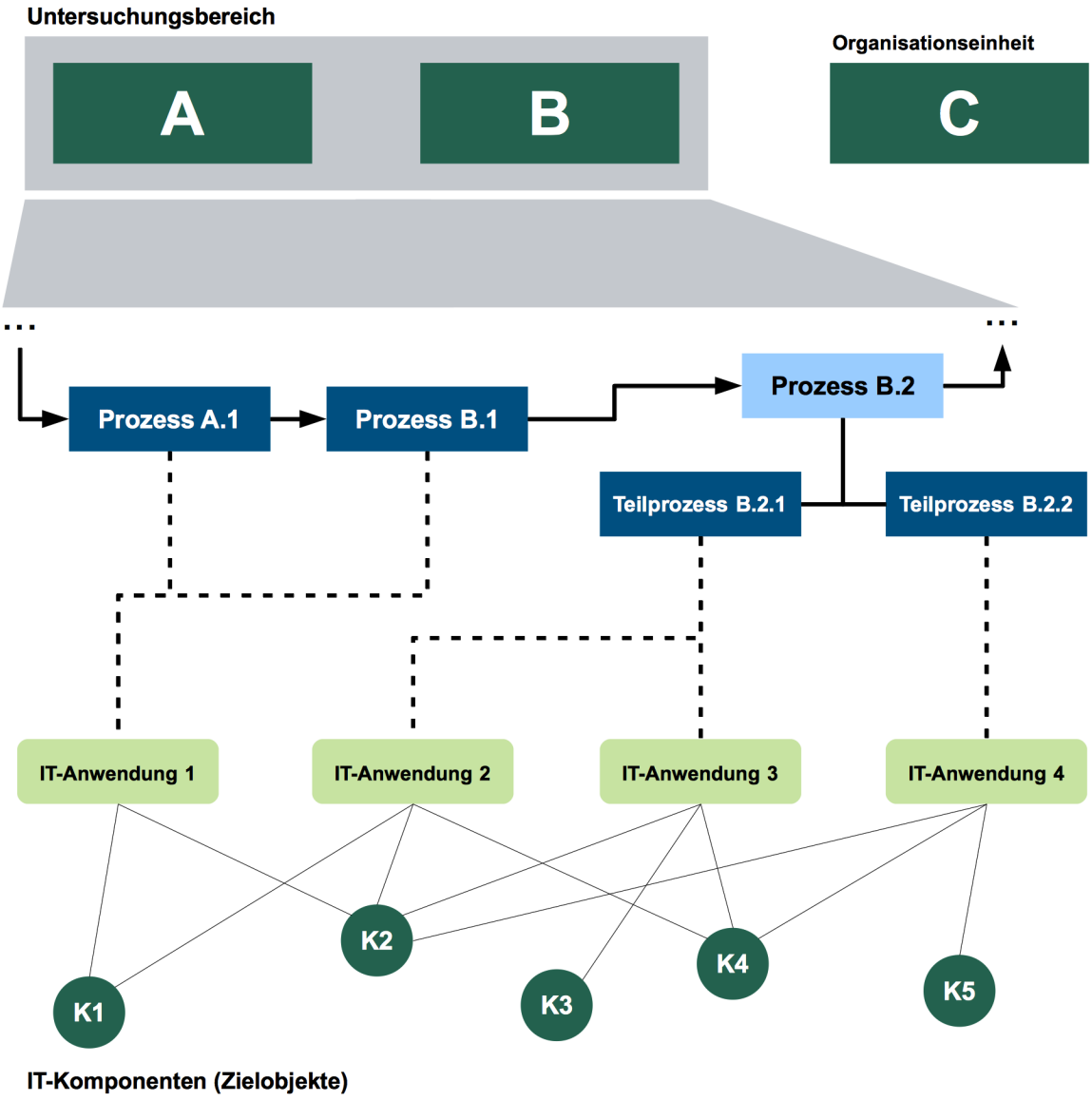

Abbildung 3: Zusammenhänge Untersuchungsbereich, Organisationseinheiten, Prozesse und IT

In diesem Teilschritt werden zunächst Informationen zur IT-Unterstützung aus Anwendersicht ermittelt. Hierfür kann neben der Auswertung bestehender Dokumentationen der Prozessabläufe die **Durchführung von Interviews** dienen.

Eine Begleitung der Interviews durch die IT-Verantwortlichen ist ratsam, da den Anwendern oft nicht im Detail bekannt ist, welche konkreten IT-Anwendungen oder Teile größerer Anwendungen für bestimmte Aufgaben (beispielsweise zur Behandlungsdokumentation) eingesetzt werden.

Es ist davon auszugehen, dass im Rahmen der Interviews und gegebenenfalls einer Begehung vor Ort bereits zahlreiche lokale IT-Komponenten (beispielsweise Arbeitsstationen, Terminals, Monitore an Betten) mit minimalem Mehraufwand erfasst werden können. Diese sollten zumindest übersichtsweise für den jeweiligen Prozess, besser aber anwendungsbezogen dokumentiert werden, um deren Berücksichtigung im Schritt 8 (siehe Kapitel 3.4) sicherzustellen.

Idealerweise sind die im nächsten Schritt (siehe Kapitel 3.3) verwendeten Kriterien für die Bewertung der Kritikalität der IT-Anwendungen bereits vor der Erhebung der IT-Unterstützung bekannt. In diesem Fall sollten zur Vorbereitung bereits alle hierfür notwendigen Informationen im Verlauf der Interviews gezielt erfasst werden. Falls nicht, bietet es sich dennoch an, Angaben wie die tolerierbare Ausfallzeit oder minimal

notwendige Anforderungen an die Performanz einer IT-Anwendung schon vorab zu erfassen. Alternativ kann diese Erhebung selbstverständlich auch in einer späteren, zweiten Gesprächsrunde durchgeführt werden.

So gehen Sie vor

Ausgangspunkt ist die Übersicht der kritischen Prozesse des Untersuchungsbereichs.

- Führen Sie Interviews mit den Prozessbeteiligten durch, um herauszufinden, welche IT-Anwendungen für welche Aufgaben verwendet werden. Als Muster hierfür können Sie die diesbezüglichen Fragen in Abschnitt H 1: Fragenkatalog verwenden.
- Sofern bereits Kriterien zur Bewertung der Kritikalität der IT-Anwendungen in Kapitel 3.3 definiert wurden, sollten die Interviews ebenfalls zur Erhebung der hierfür notwendigen Informationen genutzt werden.
- Stellen Sie die Information, die Sie in den Interviews zur IT-Unterstützung der Prozesse aus Sicht der Anwender gewonnen haben, beispielsweise tabellarisch zusammen.

Ergebnis ist eine Zusammenstellung der in den kritischen Prozessen eingesetzten IT-Anwendungen.

Hinweis

Alternative Vorgehensweisen
Die in den Kapiteln 3.2 bis 3.4 dargestellte Vorgehensweise stellt eine Empfehlung für ein schrittweises Vorgehen dar. Es ist jedoch durchaus möglich und kann im Einzelfall trotz des dadurch gegebenenfalls entstehenden Mehraufwands sinnvoll sein, die in Kapitel 3.4 beschriebene Ermittlung der IT-Komponenten direkt mit der Ermittlung der IT-Anwendungen zu verbinden.

Beispiel

In der MUSTERKLINIK werden zur Ermittlung der IT-Unterstützung für die kritischen Prozesse Interviews mit den Prozessbeteiligten durchgeführt. Im Verlauf der Interviews werden auch bereits Informationen für die anschließende Kritikalitätsbewertung erfasst (siehe Beispiel im Folgekapitel 3.3). Hierzu gehören unter anderem Angaben zur Dauer der maximal zulässigen Ausfallzeit der IT, die zur Bewertung der Kritikalität hinsichtlich der Verfügbarkeit herangezogen werden soll. Die gesammelten Informationen werden tabellarisch dokumentiert.

Tabelle 6 zeigt als Auszug aus dieser Zusammenstellung für die kritischen Prozesse der Intensivstation, der Radiologie und des Labors die eingesetzten IT-Anwendungen

- Krankenhausinformationssystem (KIS),
- Patientendatenmanagementsystem (PDMS),
- Radiologieinformationssystem (RIS),
- Bildarchivierungssystem (PACS = Picture Archiving and Communication System),
- Laborinformationssystem (LIS)

und deren maximal zulässige Ausfallzeit.

Organisations-einheit	*Prozess*	*IT-Unterstützung*	*Maximal zulässige Dauer des IT-Ausfalls in Stunden*
Intensivstation	Aufnahme	KIS, PDMS	2
	Behandlung	PDMS	2
Radiologie	Radiologische Diagnostik	KIS, RIS, PACS	6
Labor	Probenbestätigung	KIS, LIS	4
	Probenverteilung	LIS	4
	Befundrückmeldung	LIS	4
	Blutkonservenbereitstellung	LIS	0,5

Tabelle 6: Beispiel für IT-Anwendungen und zulässige Ausfallzeiten in kritischen Prozessen der MUSTERKLINIK

3.3 Kritikalität der IT-Unterstützung bestimmen

Aufgabe:	Identifikation der kritischen IT-Anwendungen
Input:	Zusammenstellung der in den kritischen Prozessen eingesetzten IT-Anwendungen
Ergebnis:	Liste kritischer IT-Anwendungen
Beteiligte:	Prozessverantwortliche, Prozessbeteiligte, IT-Verantwortliche
Hilfsmittel:	Musterkriterien zur Bestimmung der IT-Kritikalität (siehe Tabelle 7); Fragen zur Bewertung der Kritikalität in Abschnitt H 1: Fragenkatalog

Ausgehend von den kritischen Prozessen und deren IT-Unterstützung wird in diesem Schritt untersucht, wie kritisch die Abhängigkeiten dieser Prozesse von den eingesetzten IT-Anwendungen tatsächlich sind.

Zunächst sind **Kriterien festzulegen**, anhand derer die Kritikalität der IT-Abhängigkeit bewertet werden kann. Diese Kriterien werden mit Hilfe der IT-Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit definiert – Tabelle 7 zeigt ein Beispiel. Von zentraler Bedeutung ist die Verfügbarkeit. Hierfür kann zur Einschätzung der Kritikalität die maximal tolerierbare Ausfallzeit der IT-Anwendung herangezogen werden.

Grundsätzlich kann die Kritikalität zwar für jedes Kriterium beliebig fein beschrieben werden, in der Regel genügen jedoch wie in Tabelle 7 drei Kategorien („Normal“, „Hoch“ und „Sehr hoch“) zur Charakterisierung der Kritikalität einer IT-Anwendung.

Für die **Bewertung der IT-Abhängigkeit** sind Interviews mit den Anwendern zweckmäßig, in denen diese ihre Einschätzungen zur Dringlichkeit einer IT-Anwendung und den möglichen Folgen von Ausfällen oder Störungen äußern. Falls die hierfür notwendigen Informationen nicht bereits im Schritt 6 (siehe Kapitel 3.2) erhoben wurden, müssen weitere Interviews mit den Prozessbeteiligten durchgeführt werden, die ebenfalls durch entsprechende Fragestellungen vorstrukturiert sein sollten. Abschnitt H 1: Fragenkatalog enthält hierzu Vorschläge.

Hinweis

Überprüfung der Ergebnisse
Auch wenn keine weiteren Interviews durchzuführen sind, ist es unter Umständen sinnvoll, die durchgeführte Bewertung einer Qualitätssicherung durch die Prozessbeteiligten zuzuführen.

So gehen Sie vor

Ausgangspunkt ist die Zusammenstellung der kritischen Prozesse des Untersuchungsbereichs und der von ihnen benutzten IT-Anwendungen.

- Definieren Sie Kriterien, anhand derer Sie gemeinsam mit den Anwendern die Kritikalität der IT-Anwendungen beurteilen können. Hierfür können Sie das Muster in Tabelle 7 als Grundlage nehmen und gegebenenfalls variieren.
- Erheben Sie anschließend die erforderlichen Informationen in Interviews mit den Prozessbeteiligten.

Ergebnis ist eine Liste der kritischen IT-Anwendungen für die kritischen Geschäftsprozesse des Untersuchungsbereichs.

Beispiel

In der MUSTERKLINIK werden zur Bewertung der Kritikalität der IT-Unterstützung folgende Kriterien basierend auf den IT-Schutzzielen definiert.

Kategorie	***Verfügbarkeit (maximal tolerierbare Ausfallzeit)***	***Integrität***	***Vertraulichkeit***
Sehr hoch	Weniger als 4 Stunden Ausfallzeit sind tolerierbar.	Kompromittierung betrifft Behandlungs- und lebensnotwendige Daten und/oder IT-Systeme.	Vertraulichkeitsverluste betreffen behandlungs- und lebensnotwendige Daten und/oder IT-Systeme.
Hoch	Zwischen 4 und 24 Stunden Ausfallzeit sind tolerierbar.	Kompromittierung betrifft Behandlungs- aber nicht lebensnotwendige Daten und/oder IT-Systeme.	Vertraulichkeitsverluste betreffen behandlungs-, aber nicht lebensnotwendige Daten und/oder IT-Systeme.
Normal	Ausfallzeiten von mehr als 24 Stunden sind tolerierbar.	Kompromittierung betrifft allgemeine, nicht behandlungs- oder lebensnotwendige Daten und/oder IT-Systeme.	Vertraulichkeitsverluste betreffen allgemeine, nicht behandlungs- oder lebensnotwendige Daten und/oder IT-Systeme.

Tabelle 7: Beispiel für die Definition der Kriterien für die Kritikalität der IT

Das Projektteam einigt sich darauf, die Bewertung der Kritikalität der IT-Unterstützung anhand der definierten Kriterien für die Verfügbarkeit zu bestimmen. Auf Basis der bereits im Rahmen der IT-Unterstützung erfassten Informationen zur maximalen Ausfallzeit der IT und mit Hilfe der definierten Kriterien für die Verfügbarkeit werden beispielsweise die kritischen Prozesse der Intensivstation (ITS), der Radiologie und des Labors wie in Tabelle 8 dargestellt bewertet.

Die Übersicht zeigt, dass alle in 3.2 ermittelten IT-Anwendungen

- Krankenhausinformationssystem (KIS),
- Patientendatenmanagementsystem (PDMS),
- Radiologieinformationssystem (RIS),
- Bildarchivierungssystem (PACS = Picture Archiving and Communication System),
- Laborinformationssystem (LIS)

zu den kritischen IT-Anwendungen des Untersuchungsbereichs zählen.

Organisations-einheit	*Prozess*	*IT-Unterstützung*	*Maximal zulässige Dauer des IT-Ausfalls in Stunden*	*Kritikalität*
Intensivstation	Aufnahme	KIS, PDMS	2	Sehr hoch
	Behandlung	PDMS	2	Sehr hoch
Radiologie	Radiologische Diagnostik	KIS, RIS, PACS	6	Hoch
Labor	Probenbestätigung	KIS (Laborauftrag), LIS	4	Hoch
	Probenverteilung	LIS	4	Hoch
	Befundrückmeldung	LIS	4	Hoch
	Blutkonservenbereitstellung	LIS	0,5	Sehr hoch

Tabelle 8: Beispiel für die Bewertung der Kritikalität der IT-Anwendungen für kritische Prozesse in der MUSTERKLINIK

3.4 Kritische IT-Komponenten ermitteln

Aufgabe:	Identifizieren der IT-Komponenten, von deren korrektem Funktionieren die kritischen IT-Anwendungen abhängig sind
Input:	Liste kritischer IT-Anwendungen (ggf. ergänzt um lokale IT-Komponenten)
Ergebnis:	Liste kritischer IT-Komponenten
Beteiligte:	IT-Verantwortliche
Hilfsmittel:	Keine weiteren Hilfsmittel

In diesem Arbeitsschritt werden durch Auswertung von Dokumenten aus der IT-Abteilung (z. B. eines Netzplans) und in Gesprächen mit IT-Verantwortlichen diejenigen IT-Komponenten zusammengestellt, auf deren korrektem Funktionieren die kritischen IT-Anwendungen angewiesen sind. Diese IT-Komponenten werden **Zielobjekte** des in Kapitel 4 beschriebenen Aufgabenblocks, der Identifikation und Bewertung der IT-Risiken.

Für diese Aufgabe dient die Liste der kritischen IT-Anwendungen sowie – sofern diese in Schritt 6 (siehe Kapitel 3.2) bereits erhoben wurden – der lokalen IT-Komponenten als Ausgangspunkt. Zusätzlich kann es sinnvoll sein, weitere Komponenten zu erfassen und zu dokumentieren, die zwar nicht unmittelbar für eine IT-Anwendung, wohl aber für den Betrieb einer relevanten IT-Komponente erforderlich sind. Vor dem Hintergrund später zu berücksichtigender Maßnahmen könnten so bereits bestehende, direkt oder indirekt für die Ausfallsicherheit und Störungsfreiheit der kritischen IT-Anwendungen wichtige Komponenten aufgenommen werden (beispielsweise eine USV zur kurzfristigen Überbrückung von Stromausfällen).

Zu den Angaben, für die auf jeden Fall der Rückgriff auf das Wissen der IT-Verantwortlichen erforderlich ist, gehören die **Informationen zum Krankenhausnetz** und dessen Segmentierung (zum Beispiel in ein medizinisches Netz und in ein Datennetz). Netzsegmente, die für unterschiedliche Zwecke gebildet wurden und die eigene Schutzzonen darstellen, sollten auf jeden Fall gesondert dokumentiert werden.

Um die Informationen zu den unterstützenden Clients, Servern, Peripheriegeräten und Netzkomponenten zu strukturieren, können diese durch die Angabe eines **IT-Komponententyps** charakterisiert werden. Zur Kennzeichnung dieses Typs kann die folgende Einteilung dienen:

- PC, Laptop, Terminalclient,
- Terminalserver, Applikationsserver, Authentifizierungsserver, Kommunikationsserver, Datenbankserver, Virtualisierungsserver,
- Drucker, Speicher (Storage),

- Zugangsssysteme (Firewall), Netz.

Zur Reduktion der Anzahl der in der IT-Risikoanalyse zu berücksichtigenden IT-Komponenten sollten diese zudem **sinnvoll gruppiert** werden. Eine solche Gruppenbildung, die es erlaubt, mehrere IT-Komponenten in der IT-Risikoanalyse als ein einziges Zielobjekt zu behandeln, ist allerdings nur für solche IT-Komponenten zulässig, die in ihrem Typ, der Art und der Kritikalität der Dienste, die von ihnen unterstützt werden, den Sicherheitsmechanismen, mit denen sie ausgestattet sind, und gegebenenfalls weiteren Faktoren übereinstimmen. Die Gruppierung von Zielobjekten sollte daher sorgfältig vorgenommen werden.

Hinweise

Zu betrachtende IT-Komponenten
In der Regel sollten alle IT-Komponenten, die zur Funktionsfähigkeit einer kritischen Anwendung beitragen, selbst als kritisch angesehen werden. Im Einzelfall können jedoch IT-Komponenten ausgeschlossen werden, wenn deren Nichtverfügbarkeit oder Verletzungen ihrer Integrität die Funktionsfähigkeit einer IT-Anwendung nicht nennenswert beeinträchtigen.

Granularität und Umfang der zu erfassenden Informationen
Wie detailliert die IT-Komponenten zu erfassen sind, ist der jeweiligen Einrichtung überlassen, ebenso der Umfang der zu einer IT-Komponente zu erhebenden Informationen. Es sollten zu einer IT-Komponente zumindest immer so viele Informationen erfasst werden, wie für deren eindeutige Identifizierung erforderlich sind.

So gehen Sie vor

Ausgangspunkt ist die Zusammenstellung der kritischen Prozesse des Untersuchungsbereichs und der von ihnen benutzten IT-Anwendungen.

- Ergänzen Sie diese Zusammenstellung um die IT-Komponenten (Clients, Server, Netzkomponenten), die zur Ausführung dieser IT-Anwendungen erforderlich sind und eingesetzt werden. Werten Sie hierfür Dokumente zur IT-Infrastruktur (zum Beispiel Netzpläne) aus und führen Sie Gespräche mit IT-Verantwortlichen.
- Berücksichtigen Sie insbesondere auch IT-Komponenten, die von anwendungsübergreifender Bedeutung für die IT sind (zum Beispiel das Netzwerk), und solche IT-Komponenten, die indirekt für eine IT-Anwendung bedeutsam sein können.
- Fassen Sie, wenn möglich, die identifizierten kritischen IT-Komponenten sinnvoll in Gruppen zusammen, um den Aufwand der Risikoanalyse zu minimieren. Achten Sie darauf, dass IT-Komponenten mit unterschiedlicher Kritikalität und funktionaler Bedeutung nicht in einer Gruppe zusammengefasst werden.

Als Ergebnis erhalten Sie eine Zusammenstellung von IT-Komponenten, deren Risiken in den Folgeschritten identifiziert und bewertet werden.

Beispiel

Wie in Kapitel 3.3 beschrieben, wurde in der MUSTERKLINIK das Patientendatenmanagementsystem (PDMS) als kritische IT-Anwendung für die Intensivbehandlung identifiziert. Im Rahmen der Interviews zur Ermittlung der IT-Unterstützung wurden bereits die lokalen IT-Komponenten ermittelt, beispielsweise die Client-PCs an den Patientenbetten. Mithilfe eines Netzplans und in Gesprächen mit Experten aus der IT-Abteilung werden die zentralen IT-Komponenten ermittelt, die für das korrekte Funktionieren des PDMS und somit für die Intensivbehandlung des Patienten benötigt werden.

Im Ergebnis werden folgende kritischen IT-Komponenten und Gruppen von IT-Komponenten als Zielobjekte für die nachfolgenden Schritte der IT-Risikoanalyse identifiziert:

- PDMS-Server, auf dem die Patientendaten gespeichert sind,
- PDMS-Clients an den Patientenbetten, die Schnittstellen zu den zugeordneten Medizingeräten haben (z. B. Patientenüberwachungssystemen, Beatmungs- und Dialysegeräten oder solchen zur Regulierung der Flüssigkeitszufuhr) und deren Ergebnisse importieren können,
- PDMS-Clients in den Arztzimmern und Pflegediensträumen, über die von zentraler Stelle aus Informationen über einen Patienten abgerufen sowie bei Bedarf – vergleichbar mit üblichen Krankenhausinformationssystemen – auch zusätzliche Daten eingegeben oder Auswertungen und weitere Funktionen angestoßen werden können, sowie eine
- Netzinfrastruktur zur Übertragung der Daten zwischen Server und Clients.

4 Risiken identifizieren und bewerten

Im letzten Schritt wurden diejenigen IT-Komponenten bestimmt, von deren korrektem Funktionieren die kritischen IT-Anwendungen und damit die kritischen Prozesse eines Krankenhauses abhängig sind und auf deren Verfügbarkeit folglich ein besonderes Augenmerk liegen sollte. Diese **kritischen IT-Komponenten** – beispielsweise bestimmte Server, aber auch ausgewählte Clients oder einzelne Segmente eines Netzes – sind daher die **Zielobjekte** dieses Aufgabenblocks, der IT-Risikoanalyse im engeren Sinn.

Dieser liegt das folgende Begriffsverständnis zugrunde:

- Der Begriff **Risiko** bezeichnet eine Funktion aus der **Wahrscheinlichkeit** eines unerwünschten Ereignisses für ein zu schützendes Objekt und den aus diesem Ereignis resultierenden (negativen) **Auswirkungen**.
- Die Wahrscheinlichkeit, mit der es zum Eintreten des Ereignisses kommt, ergibt sich wiederum aus den **Bedrohungen**, denen das zu schützende Objekt ausgesetzt ist, und den **Schwachstellen**, die es anfällig (**verwundbar**) gegen eine Bedrohung werden lassen. In einem **Risikoszenario** wird eine sinnvolle Kombination einer Bedrohung mit einer hierzu passenden Schwachstelle zur weiteren Untersuchung zusammengefasst.
- Der **Risikowert** beschreibt die Höhe eines Risikos aufgrund der Bewertungen, die für die Wahrscheinlichkeit und die Auswirkungen eines Ereignisses vorgenommen wurden. Bei der Bestimmung dieses Wertes ist zu unterscheiden, ob bereits umgesetzte Maßnahmen zum Schutz des betrachteten Objekts in die Bewertung eingeflossen sind oder nicht.

Ausgehend von dieser Begrifflichkeit umfasst die IT-Risikoanalyse im engeren Sinne die folgenden Aufgaben (siehe auch Abbildung 4):

- **Schritt 9:** Risikoszenarien ermitteln,
- **Schritt 10:** Eintrittswahrscheinlichkeiten abschätzen,
- **Schritt 11:** Auswirkungen bewerten,
- **Schritt 12:** Risikowert ermitteln,
- **Schritt 13:** bestehende Maßnahmen berücksichtigen.

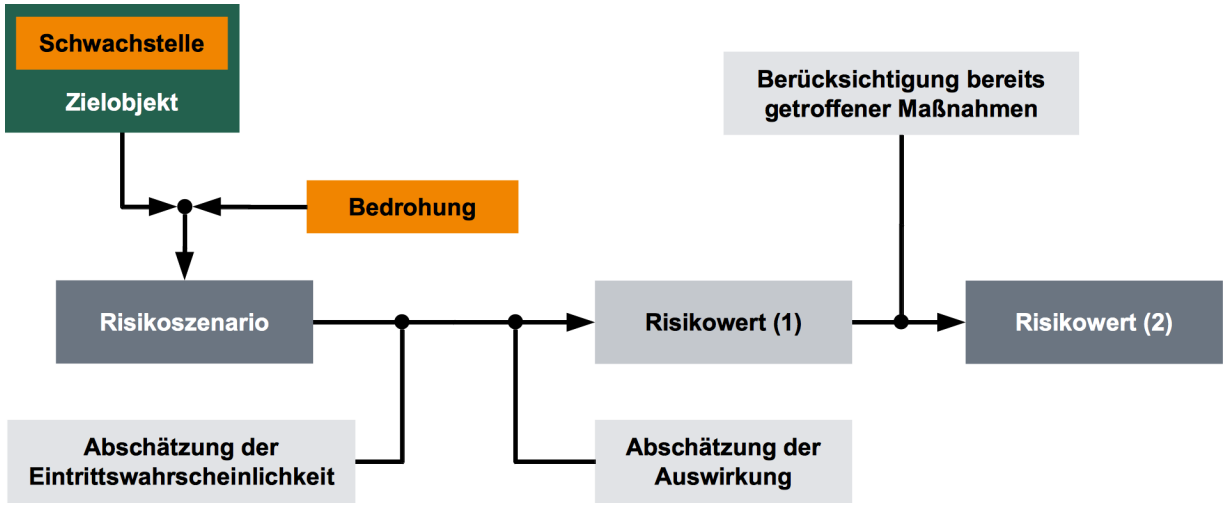

Abbildung 4: Schematische Darstellung der IT-Risikoanalyse

Diese Schrittfolge kann sowohl für jedes einzelne Zielobjekt gesondert durchlaufen werden (Variante 1) als auch in einem Durchgang, bei dem in jedem Teilschritt alle zu untersuchenden Zielobjekte betrachtet werden (Variante 2). Vollständig angewendet führen beide Vorgehensweisen dazu, dass sämtliche Zielobjekte einer IT-Risikoanalyse unterzogen werden. Beide Varianten sind daher im Prinzip gleichrangig. Der nachfolgenden Beschreibung der einzelnen Teilschritte wird die Variante 1 zugrunde gelegt.

Hinweis zur Terminologie

Die hier eingeführte Definition des Risikoszenarios entspricht in etwa dem Begriff der „Gefährdung“ im IT-Grundschutz.[4] Sie unterscheidet sich aufgrund der unterschiedlichen Natur der IT-spezifischen Zielobjekte im Vorgehen aber deutlich von der Methode zur Gefährdungsanalyse und Verwundbarkeitsanalyse des BBK (siehe [BBK-LF], Kapitel 3.2.2). Risikoszenarien sind immer mit einem konkreten Zielobjekt verbunden und können nicht mit dem später auf ein Zielobjekt anzuwendenden „Szenario“ (Gefährdung) gemäß [BBK-LF], Kapitel 3.2.2.1, gleichgesetzt werden. Auch wenn der Begriff der „Bedrohung“ in der IT-Risikoanalyse dem Begriff der „Gefahr“ in [BBK-LF] entspricht und damit ein gemeinsamer Ausgangspunkt existiert, ist eine direkte Übernahme von bereits bestehenden Szenarien oder Ergebnissen der Verwundbarkeitsanalyse gemäß [BBK-LF] nicht möglich. Dies gilt aufgrund der unterschiedlichen Bewertungsabläufe unabhängig von der gewählten Variante dieser Methode.

4.1 Risikoszenarien ermitteln

Aufgabe:	Identifizieren der Bedrohungen und Schwachstellen, die zu einem Risiko für die betrachtete kritische IT-Komponente führen können
Input:	Liste kritischer IT-Komponenten
Ergebnis:	Liste relevanter Risikoszenarien für die kritischen IT-Komponenten
Beteiligte:	IT-Verantwortliche
Hilfsmittel:	Kreuztabelle Bedrohungen – Schwachstellen [RIKRIT-RISIKEN]

Aufgabe der Risikoidentifikation ist es, diejenigen Faktoren zu beschreiben, die zu einem Risiko für ein Zielobjekt führen können. Es ist bei IT-Risikoanalysen üblich (siehe z. B. [ISO 27005]), hierfür die folgenden beiden Bedingungen zugrunde zu legen:

- Das Objekt ist **Bedrohungen** ausgesetzt. Dies können vorsätzliche Handlungen sein, beispielsweise zielgerichtete Angriffe, mit denen der Eigentümer des Objekts geschädigt werden soll. Aber auch Naturereignisse wie Erdbeben oder Überschwemmungen, technisches Versagen aufgrund der Alterung beteiligter Materialien oder von Mängeln bei der Herstellung sowie der unachtsame Umgang mit einem zu schützenden Objekt können dessen Sicherheit gefährden.
- Das bedrohte Objekt oder einer seiner Schutzmechanismen muss eine oder mehrere **Schwachstellen** haben, durch die es für die Bedrohung anfällig wird. Solche Verwundbarkeiten können in der verwendeten Hardware und Software, im Umgang mit beidem, in der umgebenden Infrastruktur oder den organisatorischen Rahmenbedingungen begründet sein.

Für die Identifikation der Risikoszenarien sind folglich zunächst die Bedrohungen zu bestimmen, denen ein Zielobjekt ausgesetzt ist, und ist anschließend zu prüfen, welche Schwachstellen es gegen diese Bedrohungen verwundbar machen. Bei dieser Aufgabe können vorhandene Kataloge als Vorlage und Ausgangspunkt dienen. Als Hilfsmittel zu diesem Leitfaden enthält das Dokument [RIKRIT-RISIKEN] daher eine **Kreuztabelle aus Bedrohungen und Schwachstellen**, die aus dem Katalog G 0: *Elementare Gefährdungen* der

4 „Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.“ Quelle: [GS-KAT]], Glossar.

IT-Grundschutz-Kataloge [GS-KAT][5] und in Anlehnung an eine Übersicht exemplarischer Schwachstellen der Norm ISO 27005 [ISO 27005][6] entwickelt wurde.

Bei der Identifikation von Bedrohungen und Schwachstellen ist es sinnvoll, vom Allgemeinen zum Besonderen vorzugehen, also die erfassten Sachverhalte schrittweise zu verfeinern. Aus diesem Grund sind die Einträge in [RIKRIT-RISIKEN] in zwei Ebenen strukturiert, einer allgemeiner gehaltenen ersten Ebene und einer zweiten Ebene, in der die Einträge detailliert werden.

Angelehnt an die Gliederung der Gefährdungskataloge G 1 bis G 5 der IT-Grundschutz-Kataloge enthält die Tabelle auf der ersten Ebene die folgenden **Bedrohungen**:

- Natürliche Ereignisse,
- Technisches Versagen (von IT-Systemen, Datenspeichern, Netzen oder der Versorgung),
- Menschliche Fehlhandlungen (an IT-Systemen, Software oder Daten),
- Vorsätzliche Handlungen (an IT-Systemen, Software oder Daten),
- Organisatorische Einflüsse (interne, externe).

Mit Ausnahme der in ihren Auswirkungen eher IT-unspezifischen und in einem Gesamtsicherheitskonzept des Krankenhauses zu behandelnden „Natürlichen Ereignisse“ (vgl. [BMI-LF], Anhang IV) werden alle weiteren Bedrohungen in einer zweiten Ebene weiter verfeinert. Tabelle 9 zeigt als Beispiel hierfür die Detaillierung der „Vorsätzlichen Handlungen an Software, Daten und Informationen“.

Bedrohungen		***Betroffene Grundwerte***	***Elementare Gefährdungen***
Ebene 1	***Ebene 2***		
Vorsätzliche Handlungen an Software, Daten und Informationen	Abstreiten von Handlungen	C, I	G 37
	Ausspähen von Informationen/Daten	C	G 14
	Manipulation von Software und Informationen/Daten	C, I, A	G 21, G 22, G 39
	Missbrauch personenbezogener Daten (z. B. von Personen mit besonderem Schutzbedarf)	C	G 36, G 38
	Missbrauch von Berechtigungen	C, I, A	G 32
	Zerstörung von Datenträgern	A	G 24

Tabelle 9: Beispiel für die Detaillierung einer Bedrohung in der Tabelle [RIKRIT-RISIKEN]. Die Buchstaben C, I, A kennzeichnen den betroffenen Grundwert (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

Jede Bedrohung wird ferner – wie in der Tabelle dargestellt – durch die Angabe zusätzlicher Informationen näher charakterisiert:

- die betroffenen Grundwerte sowie
- die Nummern der zugeordneten Gefährdungen im IT-Grundschutz-Katalog G 0 *Elementare Gefährdungen* [GS-KAT].

Die Angabe der elementaren Gefährdungen dient zum einen als Hinweis auf ergänzende Beschreibungen zu einer Bedrohung. Außerdem kann sie im Nachgang der IT-Risikoanalyse die Auswahl von Maßnahmen zur Verringerung eines Risikos unterstützen (siehe hierzu Kapitel 5.2).

5 Die IT-Grundschutz-Kataloge benennen rund 450 teilweise sehr spezifische Einzelgefährdungen, die in die fünf Gefährdungskataloge G 1: *Höhere Gewalt*, G 2: *Organisatorische Mängel*, G 3: *Menschliche Fehlhandlungen*, G 4: *Technisches Versagen* und G 5: V*orsätzliche Handlungen* gegliedert sind. In dem Katalog G 0: *Elementare Gefährdungen* wurden die generellen Aspekte dieser Gefährdungen herausgearbeitet und in 46 elementaren Gefährdungen zusammengefasst.

6 Der Anhang D.1: *Examples of vulnerabilities* der Norm [ISO 27005] benennt Beispiele für mögliche Schwachstellen und gruppiert diese in die Bereiche Hardware, Software, Netz, Personal, bauliche Infrastruktur und Organisation.

In [RIKRIT-RISIKEN] werden ferner die folgenden **Schwachstellen** unterschieden:

- Hardware (z. B. unzureichende Umgebungsbedingungen oder unzureichende Instandhaltung),
- Software (z. B. mangelnder Schutz gegen Malware oder mangelnde Sicherheitsfunktionalität),
- Netz (z. B. fehlende Verschlüsselung oder unsachgemäßes Netzwerkmanagement),
- Personal (z. B. nicht ausreichende Besetzung kritischer Personalressourcen oder unzureichende Anwenderschulung),
- Infrastruktur (z. B. mangelnde Gebäudesicherheit oder unzureichend sichere Stromversorgung),
- Organisation (z. B. unzureichende Prozesse und Verantwortlichkeiten).

Auch die Schwachstellen werden in der Tabelle [RIKRIT-RISIKEN] in einer zweiten Ebene detailliert. Beispielsweise werden zu der Softwareschwachstelle „Mangelnde Sicherheitsfunktionalität“ (Ebene 1) in Ebene 2 die Schwachstellen „Unzureichender Passwortschutz“, „Unzureichende Verschlüsselung“ und „Mangelnder Zugriffsschutz“ unterschieden.

Wenn eine Schwachstelle dazu führt, dass eine Bedrohung zu einer realen Gefährdung für ein Zielobjekt werden kann, ist dies in [RIKRIT-RISIKEN] markiert. Dabei werden **primäre und sekundäre Auswirkungen** unterschieden (siehe den Auszug in Tabelle 10).

„Vorsätzliche Handlungen an Software, Daten und Informationen“: Bedrohungen der Ebene 2	***(Software-)Schwachstellen (Ebene1)***		
	Mangelnder Schutz gegen Malware	***Bekannte Softwarefehler***	***Mangelnde Sicherheits-funktionalität***
Abstreiten von Handlungen			
Ausspähen von Informationen/Daten	P		
Manipulation von Software und Informationen/Daten	P	P	
Missbrauch personenbezogener Daten (z. B. von Personen mit besonderem Schutzbedarf)	P	S	
Missbrauch von Berechtigungen	P		
Zerstörung von Datenträgern			

Tabelle 10: Auszug aus der Kreuzreferenztabelle zu Bedrohungen und Schwachstellen. Ein „P“ kennzeichnet primäre und ein „S“ sekundäre Auswirkungen [RIKRIT-RISIKEN].

Eine Auswirkung ist **primär**, wenn sich eine Bedrohung unmittelbar auf das betrachtete Zielobjekt auswirken kann. Dies gilt etwa für die Schwachstelle „Mangelnder Schutz gegen Malware“, die unmittelbar für den Missbrauch personenbezogener Daten ausgenutzt werden kann, beispielsweise durch Einbringen eines Trojanischen Pferdes in ein unzureichend gegen Schadsoftware geschütztes IT-System.

Eine Auswirkung ist **sekundär**, wenn sich eine Bedrohung indirekt auf das betrachtete Zielobjekt auswirken kann. Dies gilt etwa für die Schwachstelle „Bekannte Softwarefehler“, die zwar unmittelbar zu Manipulationen an Software oder Daten und Informationen führen kann, zum Missbrauch personenbezogener Daten aber erst dann, wenn als Vorbedingung für einen solchen Angriff ein unerlaubter Zugriff auf die Daten hergestellt worden ist.

Es wird empfohlen, zunächst nur die primären Auswirkungen zu betrachten. Im fortgeschrittenen Status kann die Tabelle darüber hinaus auf weitere Kombinationen geprüft und erweitert werden.

Hinweise

Berücksichtigung von Eintrittswahrscheinlichkeiten und bestehenden Maßnahmen
Bei der Identifikation von Risikoszenarien ist zu prüfen, ob Bedrohungen und Schwachstellen für ein Zielobjekt prinzipiell möglich sind. Hierbei sind die Eintrittswahrscheinlichkeiten der Bedrohungen noch nicht zu berücksichtigen. Diese sind erst im nächsten Schritt zu betrachten.

Es empfiehlt sich weiterhin, bei der Beurteilung der Relevanz eines Risikoszenarios Maßnahmen, die eine Einrichtung zum Schutz ihrer IT bereits umgesetzt hat, noch nicht in Betracht zu ziehen. Ansonsten besteht die Gefahr, dass bei der IT-Risikoanalyse eine mangelhafte Umsetzung der Maßnahmen übersehen wird. Wenn die Betrachtung der vorhandenen Sicherheitsmaßnahmen dazu führt, die Relevanz eines Risikoszenarios für die betrachtete IT-Komponente zu bestreiten, ist dies sorgfältig zu dokumentieren.

Großschadensereignisse
In [RIKRIT-RISIKEN] werden Großschadensereignisse, Naturkatastrophen (Feuer, Erdbeben, Überschwemmungen) und andere Ereignisse, die zu einer unmittelbaren Gefährdung des gesamten Krankenhausbetriebs und der Patientenversorgung führen und bei denen IT-Ausfälle nicht mehr das Hauptproblem sind, weniger stark berücksichtigt. Es wird davon ausgegangen, dass diese Ereignisse in einer übergeordneten Risikoanalyse behandelt werden und sich eine IT-Risikoanalyse bei dieser Art von Bedrohungen folglich auf solche Aspekte konzentrieren kann, die spezifische IT-Lösungen erfordern. Hierzu zählen beispielsweise Fragestellungen wie die, ob Serverräume und andere Räumlichkeiten, in denen wichtige IT-Systeme untergebracht sind, hinreichend gegen Hochwasser geschützt sind.

Identifikation weiterer Bedrohungen und Schwachstellen
Die Einträge in [RIKRIT-RISIKEN] sind als Vorschläge zu verstehen, die bei Bedarf an die konkreten Bedingungen des untersuchten Krankenhauses angepasst werden sollten. Mögliche weitere Bedrohungen der Ebene 2 können beispielsweise über die Gefährdungskataloge G 1 bis G 5 der IT-Grundschutz-Kataloge ermittelt werden [GS-KAT].

So gehen Sie vor

Ausgangspunkt ist die Liste kritischer IT-Komponenten, die Zielobjekt einer IT-Risikoanalyse sind. Für jeden Eintrag in dieser Liste bestimmen Sie mit Hilfe der Kreuztabellen in [RIKRIT-RISIKEN] die relevanten Risikoszenarien wie folgt:

- Beginnen Sie als Einstieg die Relevanz der Bedrohungen der Ebene 1 für das betrachtete Zielobjekt zu bestimmen. Bei der Entscheidung, ob eine Bedrohung für ein Zielobjekt in Erwägung zu ziehen ist oder nicht, können die folgenden Fragestellungen helfen:
  - Wurde die eigene IT in der Vergangenheit bereits konkret durch diese Bedrohung gefährdet?
  - Ist eine solche Bedrohung aus anderen Einrichtungen bekannt geworden?
- Ziehen Sie bei Bedarf anschließend die Bedrohungen der Ebene 2 hinzu. Beachten Sie dabei: Wenn Sie eine Bedrohung auf Ebene 1 ausgeschlossen haben, so gilt dies auch für alle Bedrohungen auf Ebene 2. Haben Sie hingegen eine Bedrohung auf Ebene 1 ausgewählt, so müssen Sie auch auf Ebene 2 für jede einzelne Bedrohung entscheiden, ob diese zu beachten ist oder nicht.
- Prüfen Sie anschließend für alle als relevant identifizierten Bedrohungen, welche der angeführten Schwachstellen diesen zugeordnet werden können. Auch hier beginnen Sie wieder mit den Schwachstellen der Ebene 1 und verfeinern Sie die Untersuchung bei Bedarf mit den Schwachstellen der Ebene 2. Bei der Auswahl der Schwachstellen werden Sie durch die mit „P“ und „S“ gekennzeichneten Zuordnungen unterstützt, die in [RIKRIT-RISIKEN] bereits vorgenommen wurden.

- Prüfen Sie abschließend die Liste der identifizierten Risikoszenarien auf Vollständigkeit: Wurden alle relevanten Bedrohungen und Schwachstellen erfasst? Sind gegebenenfalls weitere Bedrohungen und Schwachstellen zu berücksichtigen?

Als Ergebnis dieser Teilschritte erhalten Sie für jedes betrachtete Zielobjekt eine Liste von Risikoszenarien, die Sie in den nachfolgenden Schritten genauer untersuchen müssen.

Beispiel

Zielobjekt ist der PDMS-Server für die Intensivstation. Für diesen Server sollen mit dem Hilfsmittel [RIKRIT-RISIKEN] die relevanten Risikoszenarien identifiziert werden.

Hierfür werden zunächst die Bedrohungen der Ebene 1 betrachtet, darunter die Bedrohung „Vorsätzliche Handlungen an Software, Daten und Informationen“, die auf Ebene 2 in weitere Bedrohungen detailliert wird, beispielsweise in die Bedrohungen „Manipulation von Software und Informationen/Daten“ und „Missbrauch von Berechtigungen“ (siehe Tabelle 9).

Für jede Bedrohung wird anschließend geprüft, welche Schwachstellen für diese relevant sein können. Für die Bedrohung „Manipulation von Software und Informationen/Daten“ sind dies zum Beispiel die als primär gekennzeichneten Schwachstellen „Mangelnder Schutz gegen Malware“ und „Bekannte Softwarefehler“ (siehe Tabelle 10).

Der betreffende Server ist zwar mit einer Virenschutzsoftware ausgestattet, das Projektteam für die IT-Risikoanalyse ist sich aber nicht sicher, ob dieser Schutz tatsächlich ausreicht. Sollte es einem Angreifer gelingen, diese Schwachstelle auszunutzen, ist die Manipulation von Daten im System zu befürchten. Wenn der Angreifer beispielsweise die Angaben zu den verordneten Medikamenten und Durchflussraten für die Infusionsgeräte ändert, droht eine falsche Medikation von Patienten. Es wird daher beschlossen, das aus [RIKRIT-RISIKEN] ableitbare Risikoszenario „Vorsätzliche Handlung an Software, Daten und Informationen aufgrund unzureichendem Schutz gegen Malware“ im Fortgang der IT-Risikoanalyse genauer zu betrachten.

4.2 Eintrittswahrscheinlichkeiten abschätzen

Aufgabe:	Einschätzen der Eintrittswahrscheinlichkeit eines Risikoszenarios
Input:	Liste der kritischen IT-Komponenten mit identifizierten Risikoszenarien
Ergebnis:	Liste der kritischen IT-Komponenten mit eingeschätzten Eintrittswahrscheinlichkeiten für die identifizierten Risikoszenarien
Beteiligte:	IT-Verantwortliche
Hilfsmittel:	Tabellen in Abschnitt H 2: Kriterien zur Bestimmung der Eintrittswahrscheinlichkeit

In diesem Schritt ist zu prüfen, mit welcher Wahrscheinlichkeit die im vorangegangenen Schritt identifizierten Risikoszenarien eintreten und die Schutzziele der betrachteten IT-Komponente tatsächlich verletzt werden können.

Eine solche Einschätzung ist – wie alle Prognosen über zukünftige Ereignisse – naturgemäß nicht einfach. Üblicherweise greift man hierzu auf ähnliche Ereignisse aus der Vergangenheit zurück und leitet hieraus zu erwartende Eintrittshäufigkeiten ab. Dies fällt umso leichter, je mehr Erfahrungen über das Eintreten von Ereignissen vorliegen und je besser diese dokumentiert sind. Aus diesem Grund führen Versicherungsgesellschaften beispielsweise umfangreich und detailliert Buch über Schadensfälle als Grundlage für die Kalkulation ihrer Prämien.

Vergleichbare verlässliche und verallgemeinerbare Statistiken fehlen – bislang zumindest – jedoch im Bereich der Informationssicherheit. Und selbst wenn es sie gäbe, blieben aus ihnen abgeleitete Prognosen mit einem hohen Grad an Unsicherheit behaftet. Um angesichts dieser Schwierigkeiten Entscheidungen zu

Eintrittswahrscheinlichkeiten nicht nur aus einem „Bauchgefühl“ heraus treffen zu können, empfiehlt es sich, auf Faktoren zu schauen, die das Eintreten eines Ereignisses begünstigen oder – umgekehrt betrachtet – es erschweren können. So ist beispielsweise davon auszugehen, dass

- öffentlich zugängliche IT-Systeme (etwa ein Webserver im Internet) eher angegriffen werden als IT-Systeme, auf die nur ein kleiner Personenkreis lokal begrenzt zugreifen kann, und
- erfolgreiche Angriffe umso weniger wahrscheinlich werden, je mehr Spezialkenntnisse für ihre Durchführung erforderlich sind.

Je nach Bedrohungskategorie ergeben sich unterschiedliche Faktoren für die Eintrittswahrscheinlichkeit:

- **Vorsätzliche Angriffe** – hier wird die Wahrscheinlichkeit umso größer sein, je einfacher eine Schwachstelle aufzuspüren ist und je mehr technische Fähigkeiten ein Angreifer hat, diese zu entdecken und auszunutzen. Umgekehrt sinkt die Wahrscheinlichkeit eines erfolgreichen Angriffs, je leichter ein solcher zu entdecken ist.
- **Menschliche Fehlhandlungen** – ob Eingabefehler oder andere Unzulänglichkeiten im Umgang mit Informationstechnik zu einem Schadensereignis führen, hängt zum einen davon ab, wie fehlertolerant ein System ist (je höher die Fehlertoleranz ist, desto geringer ist die Wahrscheinlichkeit eines Schadens), zum anderen von dem Ausmaß, in dem Fehler zur Quelle von Schadensereignissen werden können (mit zunehmendem Ausmaß wächst hier die Wahrscheinlichkeit eines Schadens).
- **Technisches Versagen** – dies ist abhängig vom Zustand der beteiligten Hardware und Software. Die Wahrscheinlichkeit eines solchen Risikoszenarios wird durch das Ausmaß (Anzahl möglicher Störungsquellen, Schweregrad potenzieller Störungen) sowie die Fehlertoleranz bestimmt. Während die Wahrscheinlichkeit mit dem Störungsausmaß steigt, wird sie auch hier durch die Fehlertoleranz gemindert.
- **Natürliche Ereignisse** – die Wahrscheinlichkeit, dass Großschadensereignisse und Naturereignisse zu kritischen Ausfällen führen, hängt zum einen von Standortfaktoren (Exposition) ab, zum anderen von den möglichen Ersatzsystemen bei Ausfällen (Redundanz).
- **Organisatorische Mängel** – diese befördern umso stärker das Eintreten eines Risikoszenarios, je größer die internen und externen Abhängigkeiten von einer fehlerfreien Organisation sind. Eine systematische Ressourcenplanung in einer Organisation trägt ebenfalls dazu bei, die Bedrohung durch organisatorische Mängel zu verringern.

In den Tabellen in Abschnitt H 2: Kriterien zur Bestimmung der Eintrittswahrscheinlichkeit werden die vorstehend erwähnten Faktoren genauer spezifiziert und Kriterien definiert, anhand derer mit Hilfe einer dreistufigen Skala die Relevanz eines Faktors bewertet werden kann. Tabelle 11 zeigt als ein Beispiel für diese Tabellen diejenige für die Bedrohungskategorie „Vorsätzliche Handlungen“.

Hierbei bedeuten die Ziffern in der Spalte „Wert“ folgendes:

- eine „1“, dass nur eine geringe Eintrittswahrscheinlichkeit vorliegt,
- eine „2“ eine mittlere Eintrittswahrscheinlichkeit,
- eine „3“ eine hohe oder sehr hohe Eintrittswahrscheinlichkeit und
- die Angabe „nicht relevant“, dass ein Faktor für die zugehörige Bedrohungskategorie in dem konkreten Anwendungsfall nicht bedeutsam ist.

Die Gesamtwahrscheinlichkeit für das Risikoszenario ergibt sich als Mittelwert der Einzelbewertungen.

Faktor	*Bewertung*	*Wert*
Schwachstellenentdeckung: Wie leicht ist die Schwachstelle zu erraten?	Nur mit Insider-Wissen	1
	Mit veröffentlichtem Basiswissen	2
	Mithilfe verfügbarer Werkzeuge	3
	Nicht relevant	--
Fähigkeit: Welche technischen Fähigkeiten setzt ein erfolgreicher Angriff voraus?	Tiefgehende Kenntnisse (Netzwerk, Programmierung, Sicherheitsmechanismen)	1
	Erfahrene Anwenderkenntnisse	2
	Wenige technische Kenntnisse	3
	Nicht relevant	--
Angriffsentdeckung: Wie schnell kann ein Angriff entdeckt werden?	Kurzfristig (durch Echtzeitsysteme, regelmäßige Prüfung von Logdateien)	1
	Mittelfristig (Logging ohne regelmäßige Prüfung der Logdateien)	2
	Langfristig (kein Logging; Abweichungen vom normalen Systembetrieb)	3
	Nicht relevant	--

Tabelle 11: Faktoren der Wahrscheinlichkeit bei vorsätzlichen Handlungen

Hinweise

Anpassbarkeit der Vorschläge
Die in den Tabellen in Abschnitt H 2: Kriterien zur Bestimmung der Eintrittswahrscheinlichkeit genannten Faktoren sind auf Störungen und Ausfälle von IT-Objekten, also von Hardware, Software, Anwendungen oder Daten, hin ausgerichtet. Bei ihnen handelt es sich zudem um Vorschläge. Die Methode ist offen für Ergänzungen: Anwender können weitere Faktoren hinzufügen oder vorhandene anpassen.

Zur Terminologie
Die in diesem Schritt vorgenommene Bewertung der Eintrittswahrscheinlichkeit von Risikoszenarien entspricht inhaltlich nicht der in der Methode des BBK ([BBK-LF], Kapitel 3.2.2.1) bestimmten Eintrittswahrscheinlichkeit im Rahmen der Gefährdungsanalyse. Letztere findet Anwendung auf das nach [BBK-LF] noch von konkreten Zielobjekten unabhängige Szenario (Gefährdung), ein Risikoszenario ist dagegen stets mit dem betrachteten Zielobjekt verbunden.

So gehen Sie vor

Ausgangspunkt sind die Risikoszenarien, die Sie im vorangegangenen Schritt der IT-Risikoanalyse für ein Zielobjekt ermittelt haben. Führen Sie für jedes Risikoszenario die folgenden Teilschritte aus:

- Wählen Sie aus Abschnitt H 2: Kriterien zur Bestimmung der Eintrittswahrscheinlichkeit diejenige Tabelle aus, die zu der übergeordneter Bedrohungskategorie des Risikoszenarios passt.
- Bewerten Sie jedes in der Tabelle angeführte und als relevant anzusehende Kriterium mit Hilfe der angeführten Beschreibungen mit „1“, „2“ oder „3“.
- Bilden Sie zur Bestimmung der Eintrittswahrscheinlichkeit für ein Risikoszenario den Mittelwert aus den getroffenen Einzelentscheidungen.

Ergebnis ist eine Übersicht zu den bewerteten Eintrittswahrscheinlichkeiten für die identifizierten Risikoszenarien des betrachteten Zielobjekts.

Beispiele

Bei der Bewertung der Eintrittswahrscheinlichkeit des Risikoszenarios „Vorsätzliche Handlung an Software, Daten und Informationen aufgrund unzureichendem Schutz gegen Malware“ für den als Zielobjekt betrachteten PDMS-Server erwägt das Projektteam für die IT-Risikoanalyse die Möglichkeit, dass der Mitarbeiter einer Fremdfirma das IT-System vorsätzlich während der Wartung mit Schadsoftware infiziert, die gespeicherte und eingegebene Daten ausspäht. Unter der Annahme, dass die Systemereignisse zwar protokolliert werden, die Protokolldateien jedoch nicht regelmäßig geprüft werden, beurteilt das Team die Wahrscheinlichkeit des Risikoszenarios mit Hilfe der in Tabelle 11 dargestellten Kriterien wie folgt:

- Die Schwachstelle „Unzureichender Schutz gegen Malware“ ist nur mit Insider-Wissen zu erraten (Schwachstellenentdeckung: 1).
- Sie erfordert nur geringe technische Kenntnisse (Fähigkeit: 3).
- Der Angriff wird höchstens mittelfristig entdeckt (Angriffsentdeckung: 2).

Als Mittelwert der Bewertungen für die Eintrittswahrscheinlichkeit ergibt sich damit 2,0.

Nachfolgend werden drei weitere Beispiele zur Anwendung der Tabellen in Abschnitt H 2: Kriterien zur Bestimmung der Eintrittswahrscheinlichkeit erläutert.

Beispiel für die Kategorie „Menschliche Fehlhandlungen“
Ein System arbeitet mit Informationen über Messdaten von Patienten. Die Software verfügt über eine komplexe Eingabemaske. Bei der Eingabe von Daten wird nicht überprüft, ob die eingegebenen Daten gültig sind, beispielsweise nur Ziffern enthalten, so dass Systemabstürze möglich sind.

Bewertung: Die Möglichkeit eines Zusammenbruchs des Systems durch Falscheingaben allein ist bereits eine schwerwiegende Fehlerquelle (Ausmaß: 2). Wegen der Komplexität der Anwendung ist aber auch zu erwarten, dass es möglicherweise viele solche Fehlerquellen gibt. Das Ausmaß wird damit mit „3“ höher bewertet. Das Systemverhalten ist instabil (Fehlertoleranz: 3). Der Mittelwert der Bewertungen ist 3,0.

Beispiel für die Kategorie „Natürliche Ereignisse“
Das Dokumentationssystem für die Intensivmedizin ist in den zum Rechenzentrum umfunktionierten Kellerräumen aufgestellt. Durch einen falschen Feueralarm im darüber befindlichen Geschoss wird die Sprinkleranlage ausgelöst, Löschwasser dringt durch die Geschossdecke in die Kellerräume und der zugehörige Server wird überschwemmt. Ein zweiter Server mit identischer Funktionalität ist in einer anderen Lokation zwar vorhanden, dieser muss aber erst eingeschaltet werden.

Bewertung: Es existiert ein identisches Ersatzsystem, das erst im Falle einer Störung oder eines Ausfalls eingeschaltet wird und dann alle Funktionen des Primärsystems ausführt (Redundanz: 2). Aufgrund seiner Lage im Keller und unterhalb von Räumen mit wasserführenden Leitungen sowie Decken, die unzureichend gegen Wasserdurchlass geschützt sind, ist der Standort des Servers kritisch (Exposition: 3). Der Mittelwert der Bewertungen ist 2,5.

Beispiel für die Kategorie „Organisatorische Mängel“
Das Bild-Archivierungs- und Kommunikationssystem (PACS) wird extern bei einem Dienstleister betrieben. Wegen eines Ausfalls der Kommunikationsverbindung zum Dienstleister können keine Bilder (z. B. digitale Röntgenaufnahmen) mehr bereitgestellt werden.

Bewertung: Es besteht eine hohe externe Abhängigkeit (Externe Abhängigkeit: 3). Andere Faktoren haben keinen Einfluss. Der Mittelwert der Bewertungen ist folglich 3,0.

4.3 Auswirkungen bewerten

Aufgabe:	Einschätzen der Auswirkungen bei Eintreten eines Risikoszenarios
Input:	Liste der kritischen IT-Komponenten mit eingeschätzten Eintrittswahrscheinlichkeiten für die identifizierten Risikoszenarien
Ergebnis:	Liste der kritischen IT-Komponenten mit eingeschätzten Eintrittswahrscheinlichkeiten und Schadensauswirkungen für die identifizierten Risikoszenarien
Beteiligte:	IT-Verantwortliche
Hilfsmittel:	Kriterien zur Bewertung von Auswirkungen (siehe Tabelle 12)

Bei der Bewertung der Auswirkungen eines Risikoszenarios sind dessen Folgen für die kritischen Prozesse unter dem Blickwinkel der Schutzziele der Einrichtung zu betrachten. Beispielsweise ist daher bei entsprechend gewähltem Schutzziel auf die möglichen Beeinträchtigungen für die Behandlung und Pflege der Patienten und zusätzliche Risiken für deren Gesundheit ein besonderes Augenmerk zu richten. Als Maßstab zu Bestimmung der Auswirkungen kann – wie in Tabelle 12 dargestellt – der Grad dienen, in dem beim Eintreten eines Risikoszenarios die Grundwerte Vertraulichkeit, Verfügbarkeit und Integrität verletzt werden. Zur Kennzeichnung dieses Grads sieht diese Tabelle folgende dreistufige Bewertungsskala vor:

- „1“ = geringe Auswirkungen,
- „2“ = mittlere Auswirkungen,
- „3“ = starke Auswirkungen.

Faktoren	*Bewertung*	*Wert*
Verfügbarkeit: Wie stark ist die Beeinträchtigung der Verfügbarkeit	Die betroffenen IT-Anwendungen sind im Funktionsumfang eingeschränkt, die wesentlichen Bestandteile sind weiterhin nutzbar.	1
	Die betroffenen IT-Anwendungen sind erheblich beeinträchtigt aber noch eingeschränkt nutzbar.	2
	Die betroffenen IT-Anwendungen sind vollständig ausgefallen.	3
	Das Schutzziel Verfügbarkeit ist nicht relevant.	--
Integrität: Bis zu welchem Grad könnten Daten kompromittiert und/oder verloren sein?	Nicht behandlungsnotwendige Daten sind kompromittiert oder verloren.	1
	Für die Behandlung notwendige Daten sind kompromittiert oder verloren.	2
	Lebensnotwendige Daten sind kompromittiert oder verloren.	3
	Das Schutzziel Integrität ist nicht relevant.	--
Vertraulichkeit: Welcher Art sind die von einem Verlust der Vertraulichkeit betroffenen Daten?	Daten, deren unbefugte Einsichtnahme keine Auswirkungen auf die Verfügbarkeit und Integrität anderer IT-Anwendungen, IT-Systeme oder Behandlungsprozesse hat	1
	Daten, deren unbefugte Einsichtnahme die Behandlungsprozesse stören kann, allerdings ohne lebensbedrohliche Folgen oder bleibende schwere Schäden bei Betroffenen	2
	Daten, deren unbefugte Einsichtnahme die Behandlungsprozesse derart stören kann, dass lebensbedrohlichen Folgen oder bleibende schwere Schäden bei Betroffenen drohen	3
	Das Schutzziel Vertraulichkeit ist nicht relevant.	--

Tabelle 12: Kriterien zur Bewertung der Auswirkungen eines Schadensereignisses

Hinweis

Anpassbarkeit der Vorschläge
Die Kriterien zur Bewertung der Auswirkungen sind ein Vorschlag, der gegebenenfalls an die spezifischen Gegebenheiten des Untersuchungsbereichs angepasst werden sollte. Beispielsweise könnte man bei dem Faktor „Verfügbarkeit“ auch die Anzahl der nicht verfügbaren IT-Anwendungen als Kriterium verwenden. Bei der Definition der Kriterien ist darauf zu achten, dass diese mit den formulierten IT-Schutzzielen harmonieren.

So gehen Sie vor

Ausgangspunkt sind die Risikoszenarien, die Sie in den vorangegangenen Schritten für das betrachtete Zielobjekt ermittelt und bezüglich ihrer Eintrittswahrscheinlichkeit eingestuft haben. Für jedes Risikoszenario

- prüfen Sie anhand der Kriterien in Tabelle 12, welche Auswirkungen es für das Krankenhaus hat, wenn die Grundwerte Verfügbarkeit, Integrität und Vertraulichkeit für das betrachtete Zielobjekt verletzt werden, und
- bilden Sie anschließend den Mittelwert aus den getroffenen Einzelentscheidungen.

Ergebnis ist eine Übersicht, in der für die Risikoszenarien, die Sie für ein Zielobjekt identifiziert haben, die daraus resultierenden Auswirkungen bewertet sind.

Beispiel

Bei der Bewertung der Auswirkungen des Risikoszenarios „Vorsätzliche Handlung an Software, Daten und Informationen aufgrund unzureichendem Schutz gegen Malware“ für den als Zielobjekt betrachteten PDMS-Server der Intensivstation geht das Projektteam für die IT-Risikoanalyse weiterhin davon aus, dass dieses IT-System von einem Mitarbeiter einer Fremdfirma während der Wartung mit Schadcode infiziert wird, der nicht nur gespeicherte und eingegebene Daten ausspähen, sondern auch wichtige Systemdateien modifizieren und damit schwerwiegende Funktionsstörungen bewirken kann.

Die Anwendung der Kriterien in Tabelle 12 führt zu folgender Bewertung:

- Die Schadensauswirkungen werden im Hinblick auf die beiden IT-Schutzziele Integrität und Verfügbarkeit als „Sehr hoch“ eingestuft und folglich mit „3“ bewertet, da das korrekte Funktionieren des Servers für den Behandlungsprozess von fundamentaler Bedeutung ist.
- Hingegen werden mögliche Verluste an Vertraulichkeit zwar als drohend, aber als weniger kritisch eingeschätzt (Vertraulichkeit: 2).

Als Mittelwert der Bewertungen für die Auswirkungen ergibt sich damit 2,7.

4.4 Risikowert ermitteln

Aufgabe:	Bewerten der Risiken auf Grundlage der Einschätzungen zu Eintrittswahrscheinlichkeiten und Schadensauswirkungen ohne Berücksichtigung bereits umgesetzter Maßnahmen zur Risikominderung
Input:	Liste der kritischen IT-Komponenten mit eingeschätzten Eintrittswahrscheinlichkeiten und Schadensauswirkungen für die identifizierten Risikoszenarien
Ergebnis:	Risikomatrix oder Risikomatrizen mit den bewerteten Risiken für die kritischen IT-Komponenten **ohne** Berücksichtigung bereits umgesetzter Maßnahmen zur Risikominderung
Beteiligte:	IT-Verantwortliche
Hilfsmittel:	Metrik und Matrix als Muster für eine Risikobewertung (siehe Tabelle 13, Tabelle 14)

In diesem Schritt, der **Ermittlung des Risikowerts**, sind die als relevant identifizierten Risikoszenarien auf Basis der zuvor ermittelten Werte für Eintrittswahrscheinlichkeiten und Auswirkungen zu bewerten. Es ist zu beachten, dass der Risikowert zunächst festgelegt wird, ohne dass die bereits umgesetzten und für das jeweilige Zielobjekt relevanten Sicherheitsmaßnahmen berücksichtigt werden.

Bei dieser Aufgabe sind vorbereitete Schemata mit definierten Kategorien, anhand derer Eintrittswahrscheinlichkeiten und Auswirkungen eingestuft und Risikowerte dargestellt werden können, zweckmäßige Hilfsmittel. Tabelle 13 zeigt einen Vorschlag für ein solches Schema. In dieser Bewertungsmetrik sind fünf Stufen zwischen „Sehr niedrig“ und „Sehr hoch“ definiert. Der zur quantitativen Beschreibung gewählte Wertebereich von 1,0 bis 3,0 ist auf diese Stufen gleichmäßig abgebildet.

Bewertung	***Stufen der Wahrscheinlichkeit***	***Stufen der Auswirkung***
1,0 bis 1,4	Sehr niedrig	Sehr niedrig
> 1,4 bis 1,8	Niedrig	Niedrig
> 1,8 bis 2,2	Mittel	Mittel
> 2,2 bis 2,6	Hoch	Hoch
> 2,6 bis 3,0	Sehr hoch	Sehr hoch

Tabelle 13: Bewertungsmetrik Wahrscheinlichkeit und Auswirkung

Diese Werte können in eine **Risikomatrix** übertragen werden, die als Hilfsmittel zur zusammenfassenden Darstellung des Risikowerts dient. Tabelle 14 enthält einen Vorschlag für eine solche Darstellungsform mit Festlegungen dazu, wie ein Risiko bei ermittelten Bewertungen für Eintrittswahrscheinlichkeiten und Auswirkungen insgesamt zu bewerten ist. Auch für die Beschreibung des resultierenden Risikowerts wird ein fünfstufiges Schema von „Sehr niedrig“ bis „Sehr hoch“ zugrunde gelegt.

Auswirkung	*Wahrscheinlichkeit*				
	Sehr niedrig	***Niedrig***	***Mittel***	***Hoch***	***Sehr hoch***
Sehr hoch	Niedrig	Mittel	Hoch	Sehr hoch	Sehr hoch
Hoch	Niedrig	Mittel	Hoch	Hoch	Sehr hoch
Mittel	Sehr niedrig	Niedrig	Mittel	Hoch	Hoch
Niedrig	Sehr niedrig	Niedrig	Niedrig	Mittel	Mittel
Sehr niedrig	Sehr niedrig	Sehr niedrig	Sehr niedrig	Niedrig	Niedrig

Tabelle 14: Matrix zur Bewertung von Risiken

Hinweise

Anpassbarkeit der Vorschläge
Sowohl das in Tabelle 13 dargestellte fünfstufige Bewertungsschema als auch die Risikomatrix in Tabelle 14 sind Muster, die bei Bedarf angepasst werden sollten. Wurde in einem Krankenhaus beispielsweise im Rahmen des allgemeinen Risikomanagements bereits ein Schema zur Bewertung von Risiken eingeführt, ist es in der Regel zweckmäßig, dieses auch den Risikobewertungen der IT-Risikoanalyse zugrunde zu legen.

Dokumentation der Risikowerte
Für die Darstellung der Risikowerte sind verschiedene Varianten möglich, beispielsweise

- eine einzige Risikomatrix für alle Risiken aller betrachteten Zielobjekte,
- für jedes Risiko eine eigene Risikomatrix mit den Risikowerten der jeweils betroffenen Zielobjekte,
- für jedes Zielobjekt eine eigene Risikomatrix mit den zugehörigen Risiken.

Die Ergebnisse sollten so übersichtlich dargestellt werden, dass Sie auch von Dritten ohne großen Aufwand leicht zu interpretieren sind.

So gehen Sie vor

Grundlage für die Ermittlung und Beschreibung des Risikowerts ist ein Bewertungsschema, das für alle Zielobjekte und Risiken einheitlich sein und zu Ihrer Einrichtung passen sollte. Prüfen Sie daher vorab, ob die Vorschläge in Tabelle 13 und Tabelle 14 für die von Ihnen betrachteten Untersuchungsbereich geeignet sind und passen Sie diese bei Bedarf an.

- Wenden Sie anschließend das in Tabelle 13 vorgeschlagene und gegebenenfalls von Ihnen angepasste Bewertungsschema auf die einzelnen Risiken an, die Sie für das betrachtete Zielobjekt identifiziert haben.
- Tragen Sie die Ergebnisse in eine Risikomatrix gemäß der gegebenenfalls von Ihnen angepassten Vorlage in Tabelle 14 ein.

Als Ergebnis erhalten Sie für das betrachtete Zielobjekt eine Zusammenstellung der Risikowerte für das betrachtete Zielobjekt, bei der die bereits umgesetzten Sicherheitsmaßnahmen noch nicht berücksichtigt sind.

Beispiel

Für das in den vorangegangenen Schritten untersuchte Risikoszenario „Vorsätzliche Handlung an Software, Daten und Informationen aufgrund unzureichendem Schutz gegen Malware“ wird für den betrachteten PDMS-Server aufgrund der zuvor vorgenommenen Bewertungen von

- 2,0 für die Eintrittswahrscheinlichkeit und
- 2,7 für die Auswirkungen des Schadens

sowie des gewählten Schemas zur Risikoklassifikation der Risikowert als „Hoch“ bestimmt und wie in Tabelle 15 dargestellt mit der Bezeichnung „Schadsoftware auf Server“ in die Risikomatrix eingeordnet.

Bei dieser Bewertung wird nicht berücksichtigt, dass auf dem betrachteten Server bereits Virenschutzsoftware installiert und in Betrieb ist.

Auswirkung	***Wahrscheinlichkeit***				
	Sehr niedrig	***Niedrig***	***Mittel***	***Hoch***	***Sehr hoch***
Sehr hoch	Niedrig	Mittel	**Hoch: Schadsoftware auf Server**	Sehr hoch	Sehr hoch
Hoch	Niedrig	Mittel	Hoch	Hoch	Sehr hoch
Mittel	Sehr niedrig	Niedrig	Mittel	Hoch	Hoch
Niedrig	Sehr niedrig	Niedrig	Niedrig	Mittel	Mittel
Sehr niedrig	Sehr niedrig	Sehr niedrig	Sehr niedrig	Niedrig	Niedrig

Tabelle 15: Risikomatrix mit Beispiel für eine Risikobewertung

4.5 Bestehende Maßnahmen berücksichtigen

Aufgabe:	Berücksichtigen bereits umgesetzter Sicherheitsmaßnahmen bei den vorgenommenen Risikobewertungen
Input:	Risikomatrix oder Risikomatrizen mit den bewerteten Risiken für die kritischen IT-Komponenten **ohne** Berücksichtigung bereits umgesetzter Maßnahmen zur Risikominderung
Ergebnis:	Risikomatrix oder Risikomatrizen mit den bewerteten Risiken für die kritischen IT-Komponenten **mit** Berücksichtigung der bereits umgesetzten Maßnahmen zur Risikominderung
Beteiligte:	IT-Verantwortliche
Hilfsmittel:	Metrik und Matrix als Muster für eine Risikobewertung (siehe Tabelle 13, Tabelle 14)

In der Regel hat eine Einrichtung bereits Vorkehrungen getroffen, um den Risikowert herabzusetzen, also die Eintrittswahrscheinlichkeit von Schadensereignissen abzusenken oder deren Auswirkungen zu verringern. Werden die bereits eingeführten Sicherheitsmaßnahmen berücksichtigt, führt dies in der Regel zu einer anderen Risikobewertung als bei einer Betrachtung der Risiken ohne umgesetzte Schutzmaßnahmen.

Hinweise

Informationsquellen
Bei der Ermittlung der umgesetzten Maßnahmen und deren Wirksamkeit im Hinblick auf die untersuchten Risikoszenarien können Informationen aus den Interviews, die im Rahmen der Kritikalitätsanalyse geführt wurden (siehe Kapitel 3.3), vorhandene Dokumente (zum Beispiel das Sicherheitskonzept eines Krankenhauses oder Auditberichte) oder auch weitere Gespräche mit der IT-Administration hilfreich sein.

Keine Berücksichtigung von Notfallmaßnahmen
In diesem Schritt der Risikobewertung sind Maßnahmen zu berücksichtigen, mit denen Ausfällen und Störungen der IT vorgebeugt werden solle, nicht aber Ersatzverfahren im Rahmen der Notfallvorsorge, mit denen IT-Ausfälle überbrückt werden sollen und die der Wiederherstellung normaler Betriebsabläufe dienen.

So gehen Sie vor

Ausgangspunkt sind die im vorangegangenen Schritt vorgenommenen Risikobewertungen für das betrachtete Zielobjekt.

- Prüfen Sie für jedes Risikoszenario, ob und inwiefern bereits umgesetzte Sicherheitsmaßnahmen die zuvor vorgenommenen Bewertungen der Eintrittswahrscheinlichkeiten (siehe Kapitel 4.2) oder der Auswirkungen (siehe Kapitel 4.3) verändern oder ob die zuvor getroffenen Bewertungen beibehalten werden können.
- Weisen Sie den Eintrittswahrscheinlichkeiten und Auswirkungen eines Risikoszenarios die passende Kategorie gemäß den gegebenenfalls von Ihnen angepassten Kategorien aus Tabelle 13 zu.
- Tragen Sie anschließend die Ergebnisse in eine Risikomatrix gemäß der gegebenenfalls von Ihnen angepassten Vorlage in Tabelle 14 ein.

Als Ergebnis erhalten Sie für das betrachtete Zielobjekt eine Zusammenstellung der Risikowerte für die identifizierten Risiken unter Berücksichtigung der bereits umgesetzten Sicherheitsmaßnahmen.

Beispiel

Da auf dem betrachteten PDMS-Server Virenschutzsoftware in Betrieb ist, geht das Projektteam für die IT-Risikoanalyse in der MUSTERKLINIK davon aus, dass die Eintrittswahrscheinlichkeit eines Schadens durch Schadsoftware bei einer Berücksichtigung dieser Maßnahme deutlich sinken würde. Allerdings stellt das Team bei einer genaueren Untersuchung des betrachteten Servers fest, dass die installierte Virenschutzsoftware veraltet ist und bereits seit längerer Zeit keine aktuellen Virensignaturen mehr eingespielt werden. Ursache hierfür ist eine zu restriktive Konfiguration der Firewall, die bewirkt, dass eine Verbindung zu dem Server des Herstellers, auf dem die Aktualisierungen der Software und der Virensignaturen bereitgestellt werden, verhindert wird.

Das Projektteam ändert aufgrund dieser Feststellungen die zuvor vorgenommene Bewertung für die Eintrittswahrscheinlichkeit des Risikoszenarios „Vorsätzliche Handlung an Software, Daten und Informationen aufgrund unzureichendem Schutz gegen Malware“ für den betrachteten Server wie folgt:

- Der vorhandene Virenschutz ist zwar unzureichend, würde aber gleichwohl tiefere Kenntnisse über Sicherheitsmechanismen voraussetzen, um den Schutz umgehen zu können, als wenn überhaupt keine Schutzsoftware installiert wäre – die Bewertung zur erforderlichen Fähigkeit sinkt von „3“ auf „2“.
- Angesichts des unzureichenden Virenschutzes wird die Bewertung des Kriteriums Angriffsentdeckung (eine „2“) beibehalten.

Die Einstufung der Schadensauswirkungen eines erfolgreichen Angriffs bleibt unverändert bei „Sehr hoch“.

Die Gesamtbewertung für die Eintrittswahrscheinlichkeit sinkt damit auf „Mittel“ (2,0). Das verbleibende Risiko wird daher bei Berücksichtigung der tatsächlich vorhandenen Sicherheitsmaßnahmen ebenfalls mit „Mittel“ bewertet (siehe Tabelle 16, Szenario „Schadsoftware auf partiell geschütztem Server“).

Auswirkung	***Wahrscheinlichkeit***				
	Sehr niedrig	***Niedrig***	***Mittel***	***Hoch***	***Sehr hoch***
Sehr hoch	Niedrig:	**Mittel: Schadsoftware auf partiell geschütztem Server**	*Hoch: Schadsoftware auf ungeschütz-tem Server*	Sehr hoch	Sehr hoch
Hoch	Niedrig	Mittel	Hoch	Hoch	Sehr hoch
Mittel	Sehr niedrig	Niedrig	Mittel	Hoch	Hoch
Niedrig	Sehr niedrig	Niedrig	Niedrig	Mittel	Mittel
Sehr niedrig	Sehr niedrig	Sehr niedrig	Sehr niedrig	Niedrig	Niedrig

Tabelle 16: Reduziertes Risiko bei vorhandenem, aber unzureichendem Schutz gegen Schadsoftware

5 Risiken behandeln

Ergebnis der IT-Risikoanalyse ist eine Übersicht über die bewerteten Risikoszenarien für die betrachteten IT-Komponenten. Diese Risikowerte geben Hinweise auf das Gefährdungspotenzial eines Risikoszenarios und sind daher ein wichtiger Indikator für die im Nachgang der IT-Risikoanalyse vorzunehmenden Entscheidungen zur Behandlung der Risiken (**Schritt 14**, siehe Kapitel 5.1) und die Auswahl von Maßnahmen zur Umsetzung dieser Entscheidungen (**Schritt 15**, siehe Kapitel 5.2).

5.1 Behandlung der Risiken entscheiden

Aufgabe:	Entscheiden, wie die Risiken für die kritischen IT-Komponenten zu behandeln sind
Input:	Risikomatrix oder Risikomatrizen mit den bewerteten Risikoszenarien für die kritischen IT-Komponenten **mit** Berücksichtigung der bereits umgesetzten Maßnahmen zur Risikominderung
Ergebnis:	Zusammenstellung der Entscheidungen zur Risikobehandlung für die kritischen IT-Komponenten
Beteiligte:	Risikomanagement, Prozessverantwortliche, Krankenhausleitung
Hilfsmittel:	Keine weiteren Hilfsmittel

Grundsätzlich gibt es unterschiedliche Möglichkeiten, mit Risiken umzugehen:

- **Vermeidung:** Sofern dies der Anwendungszweck zulässt, können mögliche Schäden durch Verzicht auf die risikobehaftete Situation vermieden werden, beispielsweise indem riskante Technik außer Betrieb genommen wird.
- **Reduktion:** Diese Option empfiehlt sich, wenn der Anwendungszweck es nicht zulässt, Risiken zu vermeiden. Durch die Umsetzung zusätzlicher oder stärker wirksamer Sicherheitsmaßnahmen soll dafür gesorgt werden, dass die Eintrittswahrscheinlichkeit oder die Auswirkungen eines Schadensereignisses verringert werden. Diese Handlungsoption ist sinnvoll, wenn grundsätzlich geeignete Maßnahmen zur Risikoreduktion möglich sind und der mit ihrer Umsetzung verbundene Aufwand in einem (auch in wirtschaftlicher Hinsicht) angemessenen Verhältnis zum Schutzzweck steht.
- **Transfer:** Wenn Risiken nicht vermieden werden können, ein Krankenhaus aber nicht in der Lage ist, mit eigenen Mitteln für hinreichende Sicherheit zu sorgen, können Risiken auf andere Institutionen verlagert werden. Finanziellen Risiken kann beispielsweise durch den Abschluss einer ausreichenden Versicherung begegnet werden. Ist eine Einrichtung nicht in der Lage, in Eigenregie bestimmte Prozesse sicher zu gestalten, kann überlegt werden, die zugehörigen Aufgaben an geeignete Dienstleister auszulagern. In beiden Fällen entbindet dies ein Krankenhaus jedoch nicht von der grundsätzlichen Verantwortung für das sichere und ordnungsmäßige Funktionieren der IT und seiner Prozesse. Die Option „Risikotransfer“ sollte zudem nur dann gewählt werden, wenn sich dies mit den Schutzzielen eines Krankenhauses vereinbaren lässt.
- **Übernahme:** Wenn alle anderen Möglichkeiten nicht infrage kommen oder ausgeschöpft sind, müssen die verbliebenen Restrisiken getragen werden.

Bei der Entscheidung, ob ein Risiko vermieden, verringert, verlagert oder übernommen wird, ist dessen Risikowert zu berücksichtigen. Ziel muss sein, durch wirtschaftlich angemessene und zu den Prozessen eines Krankenhauses passende Maßnahmen das zu tragende Restrisiko auf ein vertretbares Maß zu senken.

Hinweise

Integration in den Risikomanagementprozess
Alle Entscheidungen zur Behandlung von Risiken sind sorgfältig abzuwägen, müssen dokumentiert sowie von der zuständigen Leitungsebene verantwortet und unterstützt werden. Für die regelmäßige Durchführung von IT-Risikoanalysen und den angemessenen Umgang mit IT-Risiken im Rahmen des allgemeinen Risikomanagements eines Krankenhauses ist daher ein entsprechender Prozess zu etablieren, sofern er nicht bereits im Rahmen der übergeordneten Risikoanalyse (beispielsweise im Sinne des Leitfadens des BBK [BBK-LF]) eingerichtet wurde.

Übertragung der Ergebnisse in eine übergeordnete Risikoanalyse
Wird die IT-Risikoanalyse im Rahmen der allgemeinen Risikoanalyse im Sinne des Leitfadens des BKK [BBK-LF] oder eines anderen Rahmenwerks zum Risikomanagement durchgeführt, so müssen die Ergebnisse (die identifizierten Risikoszenarien und ihre Bewertungen) dorthin zurückübertragen werden und in die dort zu treffenden Gesamtbewertungen einfließen. Daher sind Prozesse, Verantwortlichkeiten und Schnittstellen zu definieren, um den erforderlichen Informationsfluss zu gewährleisten.

So gehen Sie vor

Ausgangspunkt sind die Risikoszenarien, die Sie für das betrachtete Zielobjekt zusammengestellt und bewertet haben.

- Wählen Sie für jedes Risikoszenario eine angemessene Option zu dessen Behandlung. Berücksichtigen Sie dabei die getroffenen Risikobewertungen:
  - Sehr geringe oder geringe Risiken können Sie unter Umständen akzeptieren und erfordern dann keine weiteren Maßnahmen mehr zur Verringerung des Risikowerts – eine solche Entscheidung sollten Sie jedoch stichhaltig begründen.
  - Liegt der Risikowert im mittleren Bereich, sollten Sie sorgfältig prüfen, welche Option (Vermeidung, Reduktion oder Transfer) zur Behandlung der Risiken angemessen ist und zu der gewählten Strategie passende und wirtschaftlich vertretbare Maßnahmen umsetzen.
  - Sehr hohe oder hohe Risikowerte erfordern auf jeden Fall Vorkehrungen zur Verringerung des Risikowertes. Sollte es nicht möglich oder nicht sinnvoll sein, ein Risiko zu vermeiden, sind auf jeden Fall Maßnahmen umzusetzen, die es auf ein vertretbares Maß senken können.
- Dokumentieren Sie die getroffenen Entscheidungen.

Als Ergebnis erhalten Sie eine auf das betrachtete Zielobjekt bezogene Zusammenstellung der Entscheidungen zur Risikobehandlung.

Beispiel

Für das Beispielszenario „Vorsätzliche Handlung an Software, Daten und Informationen aufgrund unzureichendem Schutz gegen Malware“ würden die vier Handlungsoptionen für den als kritisch identifizierten PDMS-Server folgendes bedeuten:

- Die Option „Risikovermeidung“ hätte die Abschaltung des Servers als Konsequenz, was aufgrund der durch ihn bereitgestellten Dienste für die Behandlungsprozesse nicht sinnvoll wäre.
- Die Option „Risikoreduktion“ würde bedeuten, Maßnahmen zur Absicherung zu treffen. Eine naheliegende Maßnahme ist es, ein geeignetes Schutzprogramm gegen Schadsoftware auszuwählen, zu installieren und zu pflegen. Wenn dies nicht praktikabel ist, wie beispielsweise bei manchen Systemen, die in Echtzeit funktionieren müssen, könnten die Maßnahmen darin bestehen, die Schnittstellen des Systems (externe Laufwerke, USB-Steckplätze, Netzanbindung) weitgehend zu verringern und stark zu kontrol-

lieren. Im dargestellten Beispiel (unzureichend gewartete Virenschutzsoftware) sind Maßnahmen zur Gewährleistung einer kontinuierlichen und zeitnahen Aktualisierung der Schutzsoftware naheliegend.

- Da für den betrachteten Server wirksame Sicherheitsmaßnahmen mit einem geringen Aufwand umsetzbar sind, scheidet die Option „Risikotransfer“ aus, beispielsweise der ohnehin eher nur theoretisch mögliche Abschluss einer Versicherung gegen die Auswirkungen einer Infektion mit Schadsoftware.
- Die Option „Risikoübernahme“ wäre angesichts der Höhe des Risikos und des geringen Aufwandes für dessen Reduktion ebenfalls unvertretbar.

Das Projektteam für die IT-Risikoanalyse in der MUSTERKLINIK entscheidet sich folglich dafür, das betrachtete Risiko durch geeignete Sicherheitsmaßnahmen zu verringern.

5.2 Präventive Maßnahmen bestimmen und Ersatzverfahren vorsehen

Aufgabe:	Auswählen und konkretisieren passender Maßnahmen für alle Risiken, die durch zusätzliche Sicherheitsmaßnahmen minimiert werden sollen
Input:	Zusammenstellung der Entscheidungen zur Risikobehandlung für die kritischen IT-Komponenten; Übersicht der Prozesse mit kritischer IT-Abhängigkeit
Ergebnis:	Zusammenstellung von Maßnahmen zur Absicherung der Verfügbarkeit der kritischen IT-Komponenten und der Prozesse mit kritischer IT-Abhängigkeit
Beteiligte:	IT-Administration, je nach Maßnahme weitere Fachverantwortliche (z. B. Haus- und Gebäudetechnik, Personalrat, Datenschutz), Krankenhausleitung (Bereitstellung der notwendigen Ressourcen und Unterstützung bei der Umsetzung von Maßnahmen)
Hilfsmittel:	Zusammenstellung Bedrohungen – Maßnahmen – IT-Komponentengruppen [RIKRIT-BMTAB]; IT-Grundschutz-Kataloge [GS-KAT]

Im Rahmen der Risikobehandlung wurde unter anderem entschieden, welche Risiken durch zusätzliche Sicherheitsmaßnahmen verringert werden sollen. Für die betroffenen Zielobjekte – und damit letztlich die von ihnen unterstützten kritischen Krankenhausprozesse – sind folglich Maßnahmen festzulegen, um diese Handlungsoption umzusetzen. Hierfür sind grundsätzlich zwei sich ergänzende Arten von Maßnahmen zu berücksichtigen: zum einen **Maßnahmen zur Erhöhung der Ausfallsicherheit** der kritischen IT-Komponenten, zum anderen als Teil der Notfallvorsorge eines Krankenhauses **Ersatzmaßnahmen**, mit denen die Funktionsfähigkeit der kritischen Prozesse aufrechterhalten werden kann, wenn die benötigte IT-Infrastruktur trotz der vorgenommenen Schutzmaßnahmen ausfällt oder gravierend gestört ist.

Es gilt grundsätzlich, dass die Vorbereitung von Ersatzmaßnahmen kein Ersatz für präventive Maßnahmen zur Erhöhung der Ausfallsicherheit ist. In gleicher Weise gilt umgekehrt, dass auch noch so aufwendige präventive Schutzmaßnahmen Notfallvorsorgeplanungen nicht überflüssig werden lassen.

Präventive Maßnahmen zur Erhöhung der Ausfallsicherheit

Bei der Auswahl von Maßnahmen zur Absicherung der kritischen IT-Komponenten können existierende Standards und „Best Practice“-Empfehlungen hilfreich sein. Nachfolgend einige Beispiele:

- Verschiedene **internationale Normen** beschreiben einen allgemeinen Rahmen für Informationssicherheit und empfehlen zugehörige Maßnahmen. Beispielsweise enthält die Norm **ISO 27002** insgesamt 135 generisch beschriebene technische und organisatorische Maßnahmen für die Gewährleistung von Informationssicherheit [ISO 27002]. Die Norm **ISO 27999** [ISO 27999] passt diese Empfehlungen an die besonderen Bedingungen eines Krankenhauses an. Der technische Standard **IEC 80001-1** [IEC 80001] enthält Vorgaben für die Integration medizintechnischer Geräte in das IT-Netz eines Krankenhauses.

- Die **IT-Grundschutz-Kataloge** [GS-KAT] beschreiben sehr konkret technische und organisatorische Maßnahmen für eine Basissicherheit, die bei höheren Schutzbedarfsanforderungen gegebenenfalls durch zusätzliche, wirksamere Maßnahmen verstärkt werden muss. Den Kern der IT-Grundschutz-Kataloge bilden die in die fünf Schichten „Übergreifende Aspekte“, „Infrastruktur“, „IT-Systeme“, „Netze“ und „Anwendungen“ gegliederten Bausteine. Sie sind typischen Aufgabenbereichen der Informationssicherheit gewidmet, beispielsweise Querschnittsthemen wie Sicherheits-, Notfall- oder Hardware- und Softwaremanagement, infrastrukturellen Aspekte wie der räumlichen Absicherung von Informationen und IT sowie dem Schutz von IT-Systemen, Netzen und Anwendungen. Jeder Baustein benennt charakteristische Gefährdungen für den beschriebenen Sachverhalt und enthält Verweise auf Maßnahmen, mit denen diesen Gefährdungen begegnet werden kann.
- Der **Leitfaden Informationssicherheit** des BSI [LF-IS] gibt einen kompakten Überblick über grundlegende Sicherheitsmaßnahmen. Die insgesamt fünfzig beschriebenen Maßnahmen sind in die Bereiche „Systematisches Herangehen an Informationssicherheit“, „Sicherheit von IT-Systemen“, „Vernetzung und Internet-Anbindung“, „Faktor Mensch: Kenntnis und Beachtung von Sicherheitsanforderungen“, „Wartung von IT-Systemen: Umgang mit sicherheitsrelevanten Updates“, „Verwendung von Sicherheitsmechanismen: Umgang mit Passwörtern und Verschlüsselung“ sowie „Schutz vor Katastrophen und Elementarschäden“ gruppiert. Im Mittelpunkt der Darstellung stehen organisatorische Regelungen, auf technische Details wird bewusst verzichtet.

Die Auswahl von Sicherheitsmaßnahmen ist eine Konsequenz aus der IT-Risikoanalyse, ist aber selbst nicht mehr Bestandteil dieser Untersuchung. Daher kann im Rahmen der in diesem Leitfaden beschriebenen Vorgehensweise nur ein möglicher Einstieg in ein systematisches Verfahren zur Behandlung von Risiken skizziert werden.

Zur Unterstützung der Anwender bei der Auswahl passender Sicherheitsmaßnahmen wurde unter Rückgriff auf die IT-Grundschutz-Kataloge [GS-KAT] eine Zusammenstellung von Bedrohungen und möglichen Gegenmaßnahmen entwickelt ([RIKRIT-BMTAB][7]), die es erlaubt, für die in Schritt 9 identifizierten Risikoszenarien (siehe Kapitel 4.1) geeignete Sicherheitsmaßnahmen zu bestimmen.

Die Zusammenstellung enthält die folgenden drei Tabellenblätter:

- **Abbildungskette Ebene 1**: Dieses Tabellenblatt enthält eine Zuordnung von elementaren IT-Grundschutz-Maßnahmen zu den Bedrohungen der Ebene 1.
- **Abbildungskette Ebene 2:** Diese Tabellenblatt enthält einer Zuordnung von elementaren IT-Grundschutz-Maßnahmen zu den Bedrohungen der Ebene 2.[8]
- **Map Maßnahmen zu IT-Komponente:** In dieser Tabelle werden die in den beiden ersten Tabellenblättern aufgeführten Maßnahmen den verschiedenen Typen zugeordnet, die zur Strukturierung der typischen IT-Komponenten eines Krankenhauses verwendet wurden (siehe Kapitel 3.2 und 3.3).[9]

Die drei Tabellenblätter erlauben es damit, zu einer Bedrohung und der betroffenen IT-Komponente passende Maßnahmen zu bestimmen. Es ist dabei jedoch zu berücksichtigen, dass die Tabellen nur eine begrenzte Auswahl von IT-Grundschutz-Maßnahmen der Siegelstufe A enthalten und noch keine hinreichende Sicherheit garantieren. Da die kritischen IT-Komponenten (zumindest in dem Grundwert Verfügbarkeit) einen hohen oder sehr hohen Schutzbedarf haben, ist die Erfordernis weiterer Maßnahmen – auch über den IT-Grundschutz hinaus – sorgfältig zu prüfen.

Ersatzverfahren bei IT-Ausfällen

Präventive Maßnahmen zielen darauf ab, die Wahrscheinlichkeit von Ausfällen und Störungen der IT-Anwendungen in einem Krankenhaus abzusenken sowie die drohenden Auswirkungen zu begrenzen.

7 Das Dokument kann unter https://www.kritis.bund.de heruntergeladen werden.
8 Zu den beiden Ebenen siehe Kapitel 4.1.
9 Die folgenden Typen werden betrachtet: Client PC, Laptop, Terminal Client, Terminal Server, Application Server, Authentifizierungsserver, Kommunikationsserver, Datenbankserver, Drucker, Storage, Virtualisierungsserver, Zugangssysteme (Demilitarisierte Zone – DMZ), Netz, sowie Übergreifende Aspekte, Organisation und Gebäude.

Jedoch können auch bei noch so umfassend umgesetzten Sicherheitsmaßnahmen IT-Ausfälle niemals vollständig ausgeschlossen werden. Damit aus den verbleibenden **Restrisiken** keine schwerwiegenden Folgen für die Patienten und das Krankenhaus entstehen, sollten zum einen Pläne für einen **hinreichend schnellen Wiederanlauf** der IT-Systeme und -Anwendungen vorbereitet werden, zum anderen geeignete **Ersatzverfahren** geplant werden, um auch ohne die standardmäßig genutzten IT-Anwendungen und bis zu deren vollständigem Wiederanlauf eine ausreichende Patientenversorgung und das Funktionieren weiterer kritischer Prozesse des Krankenhauses zu gewährleisten.

Generell können als alternative Maßnahmen bei einem Ausfall der IT manuelle oder mündliche Prozesse, papiergebundene Dokumentationen und Checklisten sowie vorgedruckte Formulare und Etiketten eingesetzt werden. Den Einsatz von Telefon, Fax oder Kurierdiensten kann dazu beitragen, auch bei einem Ausfall der Computernetze einen notwendigen Informationsaustausch aufrechtzuerhalten. Aber auch IT-bezogene Ersatzverfahren sind möglich. Diese Handlungsalternativen können in System- und Daten- oder Informationsredundanz eingeteilt werden:

- **Systemredundanz** kann mittels Ersatzsystemen hergestellt werden,
- **Daten- oder Informationsredundanz** wird durch Speicherung von Daten oder Informationen auf externen Speichermedien (z. B. CD, DVD, USB-Stick) erreicht.

Eine bevorzugte Handlungsalternative ist es, Ersatzsysteme vorzuhalten, die im Bedarfsfall schnell verfügbar sind. Eine solche Redundanz für IT-Systeme kann beispielsweise durch zusätzliche Einzelplatz-PCs als Ersatz für die primären IT-Systeme und gegebenenfalls auf externen Speichermedien bereitgestellte Daten erreicht werden. Für medizintechnische Geräte, die an das IT-Netzes angeschlossen sind und Patientendaten in die IT-Anwendungen und -Systeme einfließen lassen, müssen als Alternative manuelle Verfahren für das Erfassen und Übertragen der Daten vorgesehen werden.

In Bezug auf die Materialwirtschaft ist zu berücksichtigen, dass das Lager so gefüllt ist, dass eine Versorgung für einen hinreichend langen Zeitraum (z. B. für mindestens 72 Stunden) gesichert ist. Zusätzlich muss das Lager auch datenredundant ausgelegt sein, die Lagerorte des Materials müssen also nicht nur über eine IT-Anwendung, sondern auch manuell bestimmt werden können (z. B. durch Beschriftung der Regale mittels Etiketten).

Die Leitfäden des BBK ([BBK-LF], Kapitel 3.4.2 und 4) und des BMI ([BMI-LF], Kapitel 3.4) enthalten weitere Hinweise und Empfehlungen zum Notfall- und Krisenmanagement.

Hinweise

Zusammenhang mit dem übergeordneten Risikomanagement
Die auf den Schutz kritischer IT-Komponenten bezogenen Sicherheitsmaßnahmen sind mit den Maßnahmen zu harmonisieren, die gegebenenfalls im Rahmen eines übergeordneten Risikomanagements ergriffen wurden oder ergriffen werden sollen. Letztere tragen üblicherweise als umfassend auf die Sicherheit der Prozesse eines Krankenhauses bezogene Maßnahmen auch zur IT-Sicherheit bei. Dies gilt beispielsweise für Vorkehrungen zur Verbesserung der Versorgungssicherheit (z. B. Strom) ebenso wie für solche zur Absicherung gegen Naturereignisse (z. B. Blitzschutz, Schutz gegen Hochwasser) oder zur physischen Absicherung von Gebäuden und Räumlichkeiten.

Konkretisierung der Maßnahmen
In Regelwerken mit „Best Practice“-Empfehlungen zur Informationssicherheit werden Maßnahmen üblicherweise generisch und ohne Berücksichtigung des konkreten Anwendungsumfeldes beschrieben. Es ist daher darauf zu achten, dass Maßnahmen so geplant und umgesetzt werden, dass sie auch tatsächlich in das jeweilige Krankenhausumfeld und dessen Erfordernisse passen. Beispielsweise verbieten sich zu restriktive Vorkehrungen zum Zutritts-, Zugangs- und Zugriffsschutz für ein IT-System, wenn diese dazu führen, dass der Zugriff auf Daten, die für eine angemessene medizinische Behandlung der Patienten zwingend erforderlich sind, unvertretbar verzögert oder eingeschränkt wird.

Testen und Einüben von Ersatzverfahren
Die Funktionsfähigkeit der beabsichtigten Ersatzverfahren muss vorab getestet werden. Damit der Übergang auf ein Ersatzverfahren im Bedarfsfall reibungslos funktioniert, sind außerdem die an einem Prozess beteiligten Personen ausreichend im Umgang mit den geplanten Verfahren zu schulen.

So gehen Sie vor

Ergebnis des in Kapitel 5.1 beschriebenen Schritts ist eine Zusammenstellung der Entscheidungen zur Behandlung der identifizierten Risiken für die kritischen IT-Komponenten des betrachteten Untersuchungsbereichs.

- Für diejenigen Risiken, die durch zusätzliche Sicherheitsmaßnahmen reduziert werden können und sollen, finden Sie in den ergänzenden Hilfsmitteln zu diesem Leitfaden wie folgt Beispiele für geeignete Maßnahmen:
  - In der Tabelle [RIKRIT-RISIKEN] ist zusätzlich zu einer Bedrohung vermerkt, welche elementaren Gefährdungen des Katalogs G 0 der IT-Grundschutz-Kataloge ihr zugeordnet werden können.
  - Diese Angabe können Sie verwenden, um mithilfe der Tabellen in [RIKRIT-BMTAB] für diesen Zielobjekt-Typus und das betrachtete Risikoszenario passenden IT-Grundschutz-Maßnahmen auszuwählen.
- Erstellen Sie insbesondere für solche kritischen Prozesse, die eine hohe oder sehr hohe Abhängigkeit von einer funktionierenden IT haben, Wiederanlaufpläne, um hinreichend zügig die benötigten IT-Anwendungen wieder in Betrieb nehmen zu können.
- Stellen Sie sicher, dass alle Informationen, die für einen reibungslosen Behandlungsprozess und alle weiteren kritischen Prozesse eines Krankenhauses erforderlich sind, auch bei einem Ausfall der regulären IT noch verfügbar sind.
- Ersatzverfahren können beispielsweise über redundant vorgehaltene IT oder aber auch ganz ohne IT-Unterstützung realisiert werden, beispielsweise durch zusätzliche Pflege und Bereitstellung einer papiergebundenen Patientenakte. Welches Verfahren Sie wählen, hängt von der Art des unterstützten Prozesses, den finanziellen Möglichkeiten und der Ausstattung mit Personal und anderen Ressourcen Ihres Krankenhauses ab.
- Bei der Planung der Ersatzverfahren können Sie auch von den Erfahrungen und Konzepten anderer Krankenhäuser lernen. Suchen Sie daher den Erfahrungsaustausch mit anderen Einrichtungen.

Als Resultat dieses Schritts erhalten Sie zum einen eine Zusammenstellung von Maßnahmen zur Reduktion der Risiken für die kritischen IT-Komponenten und zur Notfallvorsorge im Falle von IT-Ausfällen im betrachteten Untersuchungsbereich.

Beispiel

Zur Reduktion des Risikos, das aus dem unzureichenden Virenschutz für den PDMS-Server der Intensivstation resultiert, korrigieren die IT-Zuständigen der MUSTERKLINIK zunächst einmal die Konfiguration der Firewall des Krankenhausnetzes, sodass eine zeitnahe Aktualisierung der Virenschutzsoftware und der von dieser verwendeten Signaturen möglich wird. Zur **Verbesserung des Schutzes gegen Schadsoftware** ziehen sie zusätzlich die beiden in der Tabelle [RIKRIT-BMTAB] aufgeführten übergreifenden IT-Grundschutz-Maßnahmen M 2.154: *Erstellung eines Sicherheitskonzeptes gegen Schadprogramme* und M 2.157: *Auswahl eines geeigneten Viren-Schutzprogramms* hinzu. Nach Auswertung dieser Maßnahmen entscheiden sich die IT-Verantwortlichen dafür, durch ein zentrales Monitoring die Aktualität der auf den IT-Systemen des Krankenhausnetzes installierten Virenschutzsoftware zu überwachen.

Die Betrachtung weiterer IT-Risiken bestärkt das Risikomanagement der MUSTERKLINIK darin, dass es zusätzlich erforderlich ist, das Gesamtrisiko für die Patientenversorgung aufgrund von Ausfällen und Störungen der IT durch ein **umfassendes Ersatzverfahren** zu reduzieren. Dieses Ersatzverfahren zielt darauf ab, bei

einem Ausfall der Systeme, in denen die Patientendaten gepflegt werden, möglichst rasch eine papiergebundene Fassung der erforderlichen Informationen zu den Patienten zu erhalten. Dieses Ersatzverfahren regelt also nicht nur den Umgang mit den elektronischen Informationen des auf der Intensivstation eingesetzten Patientendatenmanagementsystems.

Zu diesem Zweck werden alle wichtigen Patientendaten in PDF-Dateien auf einem separaten System vorgehalten, um bei einem Ausfall der elektronischen Systeme – beispielsweise des PDMS – einen ununterbrochenen Zugriff auf die für die Behandlung der Patienten benötigten Daten zu gewährleisten. Durch entsprechende technische Verfahren wird hierfür sichergestellt, dass die Patientendaten mindestens stündlich auf einem Ersatzsystem gespeichert werden, das den kurzfristigen Ausdruck der Patientendokumentation mittels eines lokal installierten Hochleistungsdruckers ermöglicht.

6 Grundlegende Maßnahmen zur IT-Sicherheit

Eine IT-Risikoanalyse schafft Voraussetzungen für einen angemessenen Schutz gegen die Risiken, denen ein Krankenhaus aufgrund der zunehmenden IT-Durchdringung seiner Prozesse ausgesetzt ist. Für die Nachhaltigkeit der Ergebnisse der IT-Risikoanalyse ist es erforderlich, diese Untersuchung und die ihr zugrunde liegenden Dokumente (z. B. die Prozessübersicht) regelmäßig zu aktualisieren und mit einem übergreifenden, also nicht nur IT-Risiken adressierenden Risikomanagement des Krankenhauses zu verzahnen. Die IT-Risikoanalyse liefert daher einen wichtigen Beitrag zu einer umfassenden Absicherung der Krankenhausprozesse.

Zu dieser umfassenden Absicherung gehört auch, dass dem Schutz der IT-Infrastruktur in einem Krankenhaus aufgrund der großen Abhängigkeit von einer störungsfrei funktionierenden IT eine hohe Priorität zugewiesen wird. Dieses Kapitel skizziert einige wichtige Handlungsfelder und Maßnahmen, mit deren Umsetzung ein Krankenhaus diesem hohen Stellenwert gerecht werden kann und die als Einstieg in ein umfassendes Management der Informationssicherheit dienen können.

Die beschriebenen Handlungsfelder und Maßnahmen erheben nicht den Anspruch der Vollständigkeit und sollen – in Verbindung mit weiterführenden Quellen (siehe hierzu Kapitel 6.4) – als Denkansatz und Ausgangspunkt zur Steigerung des IT-Sicherheitsniveaus in einer Einrichtung dienen. In der Praxis ersetzt die Umsetzung von Maßnahmenkatalogen zudem niemals ein anhand der konkreten Gegebenheiten eines Krankenhauses entwickeltes und auf diese Einrichtung zugeschnittenes Sicherheitskonzept.

6.1 Organisation der Informationssicherheit und Notfallmanagement

Zur umfassenden Absicherung der Prozesse eines Krankenhauses gegen die Risiken kritischer IT-Abhängigkeiten gehören sowohl Vorkehrungen zum Schutz der IT-Infrastruktur als auch Vorsorgemaßnahmen für den Fall, dass es trotz aller Sicherheitsmaßnahmen zu kritischen IT-Ausfällen kommt.

Informationssicherheitsmanagement aufbauen

Um dem Stellenwert der Informationssicherheit in einem Krankenhaus gerecht werden zu können, muss diese Aufgabe organisatorisch verankert werden. Hierzu gehört, dass die Leitung durch Ernennung eines **IT-Sicherheitsbeauftragten** eine zentrale Zuständigkeit für die Koordination der zugehörigen Aktivitäten schafft. Weiterhin ist es erforderlich, dass in einem Krankenhaus ausreichende Ressourcen für das Management der Informationssicherheit und die Umsetzung und den Betrieb der zugehörigen technischen und organisatorischen Sicherheitsmaßnahmen bereitgestellt werden.

Erläuterungen zu den Aufgaben des IT-Sicherheitsbeauftragten und weitere Hinweise zu den organisatorischen Vorkehrungen für Informationssicherheit bieten beispielsweise die folgenden IT-Grundschutz-Maßnahmen:

- M 2.1 *Festlegung von Verantwortlichkeiten und Regelungen,*
- M 2.193 *Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit,*
- M 2.335 *Festlegung der Sicherheitsziele und Strategie.*

Eine umfassende Einführung in das **Management der Informationssicherheit** enthält BSI-Standard 100-1: *Managementsysteme für Informationssicherheit (ISMS)* [BSI 100-1].

Sicherheitskonzepte entwickeln

Ein mithilfe der in BSI-Standard 100-2 [BSI 100-2] beschriebenen IT-Grundschutz-Vorgehensweise entwickeltes Sicherheitskonzept trägt zu einer ganzheitlichen Sicherheit bei. Wichtige Elemente eines solchen Konzepts sind Regelungen unter anderem zu den folgenden Themenbereichen:

- **Schulung und Sensibilisierung** von Ärzten, medizinischem und administrativem Personal für das Thema Informationssicherheit (siehe hierzu insbesondere die Maßnahmen M 2.198 *Sensibilisierung der Mitarbeiter für Informationssicherheit* und M 2.312 *Konzeption eines Schulungs- und Sensibilisierungsprogramms für Informationssicherheit*),
- Einsatz von **Fremdpersonal** und das **Outsourcing** von IT-Dienstleistungen (siehe hierzu insbesondere die Maßnahme M 2.226 *Regelungen für den Einsatz von Fremdpersonal* und die Maßnahmen des Bausteins B 1.11 *Outsourcing*),
- sicherer **Betrieb von Netzen und IT-Systemen** mit Detailkonzepten unter anderem
  - zum **Schutz vor Schadsoftware** (siehe M 2.154 *Erstellung eines Sicherheitskonzeptes gegen Schadprogramme*, M 4.3 *Einsatz von Viren-Schutzprogrammen*),
  - zum **Einsatz kryptographischer Verfahren** für die Sicherung der Vertraulichkeit und Integrität von Informationen (siehe M 2.161 *Entwicklung eines Kryptokonzepts*),
  - zur **Einrichtung von Client-Server-Netzen** (siehe M 2.321 *Planung des Einsatzes von Client-Server-Netzen,* M 2.322 *Festlegen einer Sicherheitsrichtlinie für ein Client-Server-Netz*),
  - zum **Betrieb von Netzkomponenten** (siehe M 2.279 *Erstellung einer Sicherheitsrichtlinie für Router und Switches*),
  - zur sicheren **Grundkonfiguration von IT-Systemen** (siehe M 4.237 *Sichere Grundkonfiguration eines IT-Systems*),
  - zur sicheren **Aussonderung von IT-Systemen und Löschung von Daten**, um den unkontrollierten Abfluss von Daten zu verhindern (siehe M 2.13 *Ordnungsgemäße Entsorgung von schützenswerten Betriebsmitteln*, M 2.431 *Regelung der Vorgehensweise für die Löschung oder Vernichtung von Informationen*),
  - zum **Patch- und Änderungsmanagement** (siehe M 2.221 *Änderungsmanagement*, M 2.273 *Zeitnahes Einspielen sicherheitsrelevanter Patches und Updates*, M 4.78 *Sorgfältige Durchführung von Konfigurationsänderungen*).

Eine wichtige Voraussetzung für strukturierte und an den realen Gegebenheiten eines Krankenhauses orientierte Sicherheitskonzepte und die Umsetzung der in diesen vorgesehenen Sicherheitsmaßnahmen ist ein vollständiges und fortlaufend aktualisiertes **Inventar der eingesetzten IT-Systeme**, in dem Einsatzzweck, Softwareausstattung (Betriebssystem- und Anwendungssoftware), Art der Netzanbindung (einschließlich ihrer externen Erreichbarkeit) aller im Krankenhausnetz betriebenen Server und Clients dokumentiert sind.

Einige weitere wichtige Aspekte, die in einem Sicherheitskonzept eines Krankenhauses zu regeln sind, werden in den folgenden Kapiteln skizziert.

Informationssicherheit in das Notfall- und Krisenmanagement integrieren

Weil der Ausfall von IT-Anwendungen sich gravierend auf die Krankenhausprozesse auswirken kann, müssen – wie in Kapitel 5.2 beschrieben – die organisatorischen und technischen Maßnahmen zum Schutz der IT-Infrastruktur durch Maßnahmen ergänzt werden, mit denen die Handlungsfähigkeit eines Krankenhauses auch bei Ausfällen und Störungen der IT gesichert werden kann. Hierfür sind zum einen Vorkehrungen für die Überbrückung solcher Notfallsituationen zu treffen, zum anderen Pläne zur Wiederaufnahme des regulären IT-Betriebs zu entwickeln. So muss auch bei Ausfall des Krankenhausinformations- oder des Bildarchivierungssystems der Zugriff auf Informationen, die für die Behandlung der Patienten erforderlich sind, möglich bleiben. Um dies sicherzustellen, können beispielsweise Vorkehrungen getroffen werden, damit bei einem IT-Ausfall eine papiergebundene Patientenakte hinreichend schnell zur Verfügung steht. Neben dem Rückgriff auf „herkömmliche“ Verfahren können aber auch IT-gestützte Maßnahmen sinnvoll sein, etwa die Vorhaltung von redundanten Ersatzsystemen. Unabhängig von der Art des gewählten Ver-

fahrens ist darauf zu achten, dass die Funktionsfähigkeit der vorgesehenen Ersatzverfahren vorab getestet und ihre Inbetriebnahme eingeübt wird.

Angesichts der starken IT-Abhängigkeiten der Krankenhausprozesse muss darüber hinaus die Behandlung von Risiken für die IT-Infrastruktur ein unerlässlicher Bestandteil des **Notfall- und Krisenmanagements** eines Krankenhauses sein. Für den Aufbau und Betrieb eines Notfallmanagementsystems mit angemessenen Vorkehrungen für die Notfallvorsorge und Notfallbewältigung enthalten der BSI-Standard 100-4: *Notfallmanagement* [BSI 100-4] und der Maßnahmenkatalog M 6 *Notfallvorsorge* der IT-Grundschutz-Kataloge umfangreiche und detaillierte Empfehlungen.

6.2 Absicherung des Krankenhausnetzes

Aufgrund der Kritikalität der betriebenen IT-Anwendungen hat der Schutz des Krankenhausnetzes als Schlüsselsystem der IT-Infrastruktur eine hohe Priorität. So muss zum einen durch redundante Auslegung der Netzkomponenten und Verbindungswege sowie Mechanismen zur automatischen Umschaltung der Wege bei Ausfällen dafür gesorgt werden, dass das Netz hohen Verfügbarkeitsanforderungen genügt. Zum anderen ist das Netz durch geeignete Sicherheitsmaßnahmen gegen Angriffe durch Hacker oder die Infiltration von Schadsoftware zu schützen. Hierfür ist insbesondere auf die Absicherung der externen Schnittstellen und eine am Schutzbedarf orientierte Segmentierung des Netzes sowie den sicheren Betrieb der eingesetzten Netztechnik (z. B. WLAN und VPN) zu achten.

Externe Schnittstellen absichern

Das Internet wird auch von Krankenhäusern immer stärker für den Austausch von Informationen, die Abwicklung von Transaktionen mit externen Stellen (Verwaltungen, Ärzten, anderen Krankenhäusern etc.) oder auch die Fernwartung von IT-Systemen und Medizinprodukten genutzt. Zur Absicherung gegen die daraus resultierenden Risiken sind die externen Schnittstellen des Krankenhausnetzes durch ein **zentrales Sicherheitsgateway** zu schützen. Zur Konzeption und zum Betrieb eines solchen Gateways geben beispielsweise die folgenden IT-Grundschutz-Maßnahmen detaillierte Empfehlungen:

- M 2.70 *Entwicklung eines Konzepts für Sicherheitsgateways*,
- M 2.71 *Festlegung einer Policy für ein Sicherheitsgateway*,
- M 2.299 *Erstellung einer Sicherheitsrichtlinie für ein Sicherheitsgateway*,
- M 2.73 *Auswahl geeigneter Grundstrukturen für Sicherheitsgateways*,
- M 2.74 *Geeignete Auswahl eines Paketfilters*,
- M 2.75 *Geeignete Auswahl eines Application-Level-Gateways,*
- M 2.78 *Sicherer Betrieb eines Sicherheitsgateways,*
- M 4.47 *Protokollierung der Sicherheitsgateway-Aktivitäten*.

Besondere Sorgfalt erfordern darüber hinaus **Server, die in das Sicherheitsgateway zu integrieren** sind. Hierzu zählen Server, über die externe Zugänge in das Krankenhausnetz ermöglicht werden sollen (z. B. für die Fernwartung von IT-Systemen), Mail- und Webserver. Für Empfehlungen zur Absicherung dieser IT-Systeme siehe die IT-Grundschutz-Maßnahme M 2.77 *Integration von Servern in das Sicherheitsgateway*.

Es ist sicherzustellen, dass der zentrale Schutz des Netzübergangs durch ein Sicherheitsgateway nicht umgangen wird, etwa indem von einem Client des Netzes aus Internetverbindungen via UMTS-Stick (UMTS = Universal Mobile Telecommunications System) aufgebaut werden.

Die BSI-Standards zur Internet-Sicherheit enthalten eine Vielzahl an Empfehlungen zur Netzsicherheit. In diesem Zusammenhang sind insbesondere die folgenden Module zu nennen:

- *Sichere Anbindung von lokalen Netzen an das Internet* [ISi LANA],
- *Sicherer Fernzugriff auf das interne Netz* [ISi FERN].

Krankenhausnetz gemäß Schutzbedarf segmentieren

Das interne Netz eines Krankenhauses muss dem Schutzbedarf der jeweils angeschlossenen IT-Systeme und der auf diesen gespeicherten und bearbeiteten Daten entsprechend in **Schutzzonen** aufgeteilt werden. Beispielsweise empfiehlt sich eine Segmentierung in ein klinisches Datennetz mit für die Patientenversorgung unmittelbar kritischen IT-Anwendungen und ein allgemeines Krankenhausnetz mit ausschließlich weniger kritischen IT-Anwendungen.

Grundsätzlich gilt, dass Netzsegmente mit besonders hohem Schutzbedarf (zum Beispiel solche mit Medizinprodukten und sensiblen Patientendaten) besonders restriktiv zu konfigurieren und vom übrigen Netz zu trennen sind. Zu dieser restriktiven Konfiguration tragen Einzelmaßnahmen bei wie

- die grundsätzliche Sperrung von externen Laufwerken und USB-Schnittstellen (USB = Universal Serial Bus) an den in das betreffende Netzsegment integrierten IT-Systemen und
- die Einrichtung spezieller Arbeitsstationen mit aktiviertem Virenschutz für den gesicherten Austausch von Daten mit dem ansonsten abgeschotteten Netzsegment.

Als technisches Verfahren für einen solchen Datenträgeraustausch wurde im Auftrag des BSI die „Janus Wechseldatenträgerschleuse“ entwickelt, welche beispielsweise dazu dienen kann, das lokale Einspielen eines Softwareupdates im Rahmen der Wartung eines Medizinprodukts oder auch den Import von Patientendaten über externe Datenträger abzusichern.

WLANs sicher an das Krankenhausnetz anbinden

Bestandteil des Krankenhausnetzes sind immer stärker auch Funknetze (WLAN = Wireless Local Area Network). Diese ermöglichen beispielsweise flexible Zugriffe auf ein Krankenhausinformationssystem mithilfe mobiler IT-Systeme, erfordern aber angesichts der Eigenheiten dieser drahtlosen Netztechnik eine gründliche Absicherung. Empfehlungen hierfür geben die IT-Grundschutz-Maßnahmen

- M 2.381 *Festlegung einer Strategie für die WLAN-Nutzung,*
- M 2.382 *Erstellung einer Sicherheitsrichtlinie zur WLAN-Nutzung,*
- M 2.383 *Auswahl eines geeigneten WLAN-Standards,*
- *M 2.385 Geeignete Auswahl von WLAN-Komponenten,*
- *M 4.297 Sicherer Betrieb der WLAN-Komponenten,*
- M 5.139 *Sichere Anbindung eines WLANs an ein LAN*

sowie der BSI-Standard zur Internet-Sicherheit (ISi-Reihe)

- *Sichere Nutzung von WLAN* [ISi WLAN].

Virtuelle Private Netze (VPN) sicher einsetzen

Zur Absicherung ansonsten ungeschützter Kommunikationsverbindungen haben sich Virtuelle Private Netze (VPN) etabliert. Mit ihrer Hilfe können beispielsweise externe Standorte eines Krankenhauses angebunden und Fernwartungszugänge geschützt oder Zugriffe von mobilen Geräten auf die IT-Anwendungen im Krankenhausnetz per WLAN abgesichert werden. Empfehlungen für den sicheren Betrieb eines VPN geben die IT-Grundschutz-Maßnahmen

- M 2.415 *Durchführung einer VPN-Anforderungsanalyse,*
- M 2.416 *Planung des VPN-Einsatzes,*

- M 2.418 *Erstellung einer Sicherheitsrichtlinie zur VPN-Nutzung,*
- M 4.320 *Sichere Konfiguration eines VPNs,*
- M 4.321 *Sicherer Betrieb eines VPNs*

sowie der BSI-Standard zur Internet-Sicherheit (ISi-Reihe)

- *Virtuelles privates Netz* [ISi VPN].

6.3 Absicherung der IT-Systeme

Eine Vielzahl unterschiedlicher IT-Systeme kann Bestandteil des Krankenhausnetzes sein. So können in jedem Raum, in dem medizinische Leistungen erbracht und dokumentiert oder administrative Aufgaben erledigt werden müssen, Client-PCs anzutreffen sein, so in Stations- und Ärztezimmern, speziellen Funktionsräumen, aber auch – beispielsweise auf der Intensivstation – an den Patientenbetten. Immer häufiger finden sich auch Laptops, Tablets und andere mobile Geräte als Bestandteil der IT-Infrastruktur von Krankenhäusern. Ebenso vielfältig ist auch die Serverlandschaft eines modernen Krankenhauses: Krankenhausinformationssysteme werden als verteilte Client-Server-Anwendung betrieben, die auf Datenbankservern für die Verwaltung unter anderem der Patientendaten zurückgreifen. In größeren Umgebungen werden zusätzlich Applikationsserver eingesetzt, die mit den Datenbankservern kommunizieren und die Anfragen der Clients verarbeiten. Spezielle Kommunikationsserver tragen dazu bei, den insgesamt erforderlichen Kommunikationsaufwand der IT-Anwendungen zu optimieren. Auch das Prinzip der Virtualisierung findet in der Krankenhaus-IT immer mehr Anwendung.

Sicherheitskonzepte für die Krankenhaus-IT müssen folglich einer unter Umständen ausgesprochen komplexen IT-Infrastruktur mit hohen Sicherheitsanforderungen gerecht werden.

IT-Systeme und IT-Anwendungen zentral administrieren

Die **zentrale Verwaltung von IT-Anwendungen und IT-Systemen** (einschließlich der mobilen Endgeräte) verringert Administrationsaufwände und erleichtert es, die Einhaltung von Sicherheitsrichtlinien zu kontrollieren und durchzusetzen. Virenschutzprogramme oder Betriebssystem- und Anwendungssoftware können leichter gewartet und die Aktualität und Konfiguration dieser Software leichter kontrolliert werden. Auch die Konfiguration von Routern und Switches wird effizienter: Die lokale Administration aktiver Netzkomponenten verlängert beispielsweise die Reaktionszeiten bei Störungen, da unter Umständen längere Wege bis zum Standort der Komponente zurückzulegen sind.

Die Administratoren eines Krankenhaus-Netzes müssen nahezu täglich damit rechnen, dass neue Schwachstellen in der eingesetzten Betriebssystem- und Anwendungssoftware bekannt werden. Daraus folgt, dass **Patches und Updates zeitnah** eingespielt oder andere Verfahren umgesetzt werden müssen, um zu verhindern, dass eine Schwachstelle für Angriffe auf das Krankenhausnetz ausgenutzt wird. Eine zentrale Administration ist ein wichtiges Instrument zur Unterstützung dieser Aufgabe.

Client-Server-Anwendungen schützen

Die Vielfalt der **Anwendungssysteme in Krankenhäusern** lässt sich grob in die folgenden Gruppen aufteilen:

- Kernanwendungen (Planung und Steuerung, Abrechnung, Dokumentation, Kommunikation),
- Berichtswesen (Auswertung und internes Reporting),
- Betriebswirtschaft (Materialwirtschaft und Finanzbuchhaltung),
- medizinische Subsysteme.

Neben dem zentralen Krankenhausinformationssystem (KIS) gehören dazu beispielsweise Anwendungen für die Arbeitsablaufsteuerung, die Planung von Operationen, die Leistungsstellung, die Erfassung von Diagnosen, die Befundschreibung, die Erfassung von Berichten beispielsweise an die Berufsgenossenschaft, Kosten- und Leistungsrechnung, Kostenträgerrechnung, um nur einige Anwendungen für die ersten drei Kategorien zu nennen.

Das Krankenhaus-Informationssystems (KIS) ist die zentrale Anwendung für die Unterstützung der administrativen (Planung, Abrechnung und Controlling) sowie medizinischen (Medizinische Dokumentation – elektronische Patientenakte, Pflegedokumentation, Auftragsmanagement) Prozesse eines Krankenhauses mit der Patientendatenbank als Kernbestandteil. In der Radiologie werden die abteilungsspezifischen Abläufe und die Verwaltung der Patientendaten durch das Radiologie-Informationssystem (RIS) übernommen. Dazu gehören auch Dokumentation, Abrechnung und Statistik. Das RIS wiederum steuert unter anderem das digitale Bilddatenarchivierungs- und Kommunikationssystem (PACS). Es verwaltet alle anfallenden medizinischen Bilder und bildbezogenen Daten (Ultraschall, Endoskopie usw.) sowie Befunde und dient der gesetzeskonformen Archivierung.

Alle wichtigen Krankenhausanwendungen werden als Client-Server-Anwendung betrieben, können miteinander vernetzt sein und haben Schnittstellen zu Datenbanken, Speicher und Archivsystemen. Die Sicherheit dieser IT-Anwendungen und des Netzes hängt damit wesentlich von der **Absicherung der beteiligten IT-Komponenten** ab, also den Servern, über die diese Dienste bereitgestellt werden, den Clients, mit denen die Dienste genutzt werden und den Datenbanken und Speichersystemen, in denen die wichtigen Daten abgelegt werden. Zur Absicherung dieser IT-Komponenten können die folgenden Maßnahmen beitragen:

- Grundsätzlich sind für **Server** alle Maßnahmen zu ergreifen, die deren Schutz über den gesamten Lebenszyklus von der Anschaffung bis zur Außerbetriebnahme gewährleisten. Siehe hierzu die IT-Grundschutz-Maßnahmen
  - M 2.315 *Planung des Servereinsatzes*,
  - M 2.316 *Festlegen einer Sicherheitsrichtlinie für einen allgemeinen Server*,
  - M 2.318 *Sichere Installation eines Servers*,
  - M 4.239 *Sicherer Betrieb eines Servers*,
  - M 2.320 *Geregelte Außerbetriebnahme eines Servers.*
- IT-Anwendungen, die auf **Datenbanken** sowie **Speicher- und Archivsystemen basieren**, sind in besonderem Maße zu schützen und werden durch eine Vielzahl von Maßnahmen aus dem IT-Grundschutz adressiert. Diese Maßnahmen sind insbesondere in den folgenden drei Bausteinen zusammengestellt:
  - B 5.7 *Datenbanken*,
  - B 1.4 *Datensicherungskonzept,*
  - B 1.12 *Archivierung*.

Virtualisierung

Auch in der Krankenhaus-IT setzt sich das Prinzip der Virtualisierung immer stärker durch. Hierbei werden ein oder mehrere IT-Systeme virtuell auf einem physischen IT-System, dem sogenannten Virtualisierungsserver, betrieben. Beispielsweise kann ein Krankenhausträger das Krankenhausinformationssystem oder das Bildarchivierungssystem mehreren angeschlossenen Krankenhäusern virtualisiert in einem zentralen Rechenzentrum zur Verfügung stellen. Für den sicheren Betrieb virtueller IT-Systeme enthält der IT-Grundschutz-Baustein

- B 3.304 *Virtualisierung*

umfangreiche Maßnahmenempfehlungen.

Schutz von stationären und mobilen Clients

Der Schutz aller Endgeräte sollte über den gesamten Lebenszyklus von der Anschaffung bis zur Außerbetriebnahme sichergestellt sein. Hinweise hierzu bieten

- die IT-Grundschutz-Maßnahme M 4.241 *Sicherer Betrieb von Clients* sowie
- das Modul *Absicherung eines PC-Clients* [ISi Client] aus der ISi-Reihe des BSI.

Es ist insbesondere zu verhindern, dass an den Endgeräten zentrale Schutzvorkehrungen ausgehebelt werden, beispielsweise indem mittels UMTS-Stick oder ungesichertem WLAN das Sicherheitsgateway an der Schnittstelle zum Internet umgangen wird. Eine besondere Herausforderung bedeutet in dieser Hinsicht die Absicherung von Laptops, Smartphones, Tablets und anderen mobilen IT-Systemen. Sicherheitsempfehlungen für diese Art von IT-Systemen enthalten beispielsweise die folgenden IT-Grundschutz-Maßnahmen:

- M 2.303 *Festlegung einer Strategie für den Einsatz von PDAs*,
- M 2.304 *Sicherheitsrichtlinien und Regelungen für die PDA-Nutzung*,
- M 2.309 *Sicherheitsrichtlinien und Regelungen für die mobile IT-Nutzung*,
- M 5.122 *Sicherer Anschluss von Laptops an lokale Netze*,
- M 1.33 *Geeignete Aufbewahrung tragbarer IT-Systeme bei mobilem Einsatz*,
- M 1.34 *Geeignete Aufbewahrung tragbarer IT-Systeme im stationären Einsatz*,
- M 4.228 *Nutzung der Sicherheitsmechanismen von PDAs*,
- M 4.27 *Zugriffsschutz am Laptop*,
- M 1.61 *Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes*.

Internet-Nutzung auf Endgeräten absichern

Beim Anschluss eines Krankenhausnetzes an das Internet muss der Schutz der Patientendaten und der für die Behandlungsprozesse kritischen IT-Anwendungen höchste Priorität haben. Einerseits bietet das Internet einem Krankenhaus vielfältige Möglichkeiten für die Erhöhung der Effizienz seiner Prozesse. Andererseits führt die Anbindung an das Internet aber auch zu hohen Risiken für die Daten und IT-Anwendungen in einem Krankenhausnetz. Um diese Risiken zu begrenzen, ist neben einer Absicherung der Schnittstelle des internen Netzes zum Internet und einer am Schutzbedarf orientierten Strukturierung dieses Netzes in Sicherheitszonen auch auf eine sorgfältige Konfiguration der Endgeräte zu achten, mit denen E-Mail, das WWW und andere Internet-Dienste genutzt werden. Zusätzlich sind Richtlinien für einen sicheren Umgang mit diesen Endgeräten und die Internet-Nutzung festzulegen.

Umsetzungsempfehlungen finden sich in den folgenden IT-Grundschutz-Maßnahmen:

- M 2.234 *Konzeption von Internet PCs*,
- M 2.235 *Richtlinien für die Nutzung von Internet-PCs*,
- M 5.46 *Einsatz von Stand-alone-Systemen zur Nutzung des Internets*,
- M 5.69 *Schutz vor aktiven Inhalten*,
- M 5.91 *Einsatz von Personal Firewalls für Internet-PCs*,
- M 5.93 *Sicherheit von WWW-Browsern bei der Nutzung von Internet-PCs*,
- *M 5.94 Sicherheit von E-Mail-Clients bei der Nutzung von Internet-PCs*.

Grundlegende Empfehlungen zur Absicherung von Web-Clients sind darüber hinaus in dem Modul

- *Sichere Nutzung von Web-Clients* [ISi WebClient]

der ISi-Reihe des BSI zusammengestellt.

Die Verwendung eines sogenannten **Remote Controlled Browser Systems** (ReCoBS) bietet sich an, um auf solchen Clients einen sicheren Zugang zum WWW zu ermöglichen, die aufgrund der Kritikalität der Daten und IT-Anwendungen, die mit ihnen bearbeitet werden, einen hohen Schutzbedarf haben. Hierbei läuft der Webbrowser nicht auf dem Client-PC, sondern auf einem gesicherten Terminalserver-System als Bestandteil eines Sicherheitsgateways außerhalb des internen Netzes. Auf den Client-PC gelangen daher ausschließlich grafische Informationen, die Ausführung von aktiven Inhalten und damit von potenziell schädlichem Code auf den Clients ist damit nicht mehr möglich. Weitere Informationen zu dieser technischen Sicherheitsmaßnahme können auf den Internetseiten des BSI gefunden werden.

Sichere Authentisierung und Autorisierung

Medizinische IT-Anwendungen verfügen häufig über eigene Datenbanken zur Verwaltung der Zugangskennungen und Berechtigungen ihrer Benutzer, sodass Ärzte und das Pflegepersonal sich unter Umständen mehrmals täglich mit unterschiedlichen Kennwörtern und Benutzernamen an den von ihnen benötigten Anwendungen anmelden müssen. Dies stört nicht nur den medizinischen Arbeitsablauf, sondern befördert auch einen fahrlässigen Umgang mit Kennwörtern, beispielsweise durch die Auswahl schwacher Passworte.

Hier helfen Verzeichnisdienste insbesondere dann, wenn die Anwendungssysteme Single Sign-On (SSO) unterstützen. Die Benutzer müssen sich nur einmal anmelden und haben Zugriff auf die ihrer Berechtigung entsprechenden IT-Systeme und IT-Anwendungen. In Verbindung mit einem Heilberufsausweis (z. B. dem elektronischen Arztausweis) kann die einmalige Identifizierung kombiniert mit Eingabe der zugehörigen PIN sehr einfach und sicher erfolgen und damit die Anmeldung mit Passwort und Benutzername ablösen.

Verzeichnisdienste sind in einem Krankenhaus-Netz eine Kernkomponente. Sie verwalten in hierarchischen Strukturen Objekte wie Benutzer, Zugangsinformationen, Berechtigungen, Gruppen, Server, Clients, Dateifreigaben, Drucker, Scanner und andere Geräte und deren Eigenschaften. Aufgrund dieser zentralen Stellung für die Sicherheit eines Krankenhausnetzes ist auf die Sicherheit des Verzeichnisdienstes ein besonderes Augenmerk zu richten. Hinweise hierzu geben die folgenden IT-Grundschutz-Maßnahmen:

- M 4.307 *Sichere Konfiguration von Verzeichnisdiensten*,
- M 4.308 *Sichere Installation von Verzeichnisdiensten*,
- M 4.311 *Sicherer Betrieb von Verzeichnisdiensten*.

6.4 Weitere Informationsquellen

Die in den vorangegangenen Abschnitten angeführten Informationsquellen entstammen insbesondere den folgenden Publikationen bzw. Gruppen von Publikationen:

- den **IT-Grundschutz-Katalogen** ([GS-KAT], http://www.bsi.bund.de/IT-Grundschutz-Kataloge), in denen Standardsicherheitsmaßnahmen für ein breites Spektrum an typischen IT-Einsatzszenarien beschrieben werden, deren Umsetzung ein normalen Schutzbedarfsanforderungen genügendes Sicherheitsniveau bietet, das auch für höhere Sicherheitsanforderungen ausbaufähig ist,
- den **BSI-Standards zur Internet-Sicherheit (ISi-Reihe)**, die thematisch und zielgruppenspezifisch modularisiert eine an individuelle Gegebenheiten anpassbare Grundarchitektur für einen wirksamen Schutz gegen Gefährdungen aus dem Internet vorstellen. Die Studie *Internet-Sicherheit: Einführung, Grundlagen, Vorgehensweise* [ISi-E] gibt einen Überblick über die gesamte Reihe, deren Module kostenfrei unter https://www.bsi.bund.de/ISi-Reihe bezogen werden können.

Im Bereich der Informationssicherheit ist von einer sich kontinuierlich wandelnden Bedrohungslage auszugehen. Für die Nachhaltigkeit der organisatorischen und technischen Maßnahmen zur Absicherung der IT-Infrastruktur eines Krankenhauses ist es daher unerlässlich, dass die IT-Verantwortlichen sich ebenso kontinuierlich über neue Entwicklungen sowohl zur aktuellen Gefährdungslage als auch über zweckmäßige Sicherheitsmaßnahmen informieren und bei kritischen Informationen unverzüglich erforderliche Sicherheitsmaßnahmen einleiten.

Wichtige **Informationsquellen** können beispielsweise sein:

- die Warn- und Informationsmeldungen eines etablierten Computer Emergency Response Teams (CERT), beispielsweise des CERT-Bund, des Computer-Notfallteams des BSI (https://www.cert-bund.de), oder des CERTs des Deutschen Forschungsnetzes DFN (http://www.dfn-cert.de),
- Lageberichte wie die regelmäßig publizierten Lageberichte zur IT-Sicherheit in Deutschland des BSI (https://www.bsi.bund.de/Lageberichte) oder anderer Sicherheitsdienstleister,
- Mitteilungen, Warnungen und Sicherheitsempfehlungen der Hersteller der eingesetzten Betriebssystem- und Anwendungssoftware und medizintechnischen Geräte,
- das Informationsangebot des BSI zur Cyber-Sicherheit (https://www.bsi.bund.de/cyber-sicherheit),
- das Informationsangebot der Allianz für Cyber-Sicherheit (https://www.allianz-fuer-cybersicherheit.de).

Als wichtige Informationsquelle für angemessene und wirksame Sicherheitsmaßnahmen können auch die Erfahrungen anderer Krankenhäuser dienen. Die **Zusammenarbeit und der Informationsaustausch** mit anderen Krankenhäusern und Krankenhausbetreibern zur Informationssicherheit wie auch zu anderen Fragestellungen des Risikomanagements ist daher zu empfehlen.

7 Ausblick: Sicherheit aufrechterhalten und weiterentwickeln

Sorgfältig durchgeführte IT-Risikoanalysen helfen dabei, an den Schutzzielen ausgerichtete und der Bedrohungslage angepasste Sicherheitskonzepte für die IT-Infrastruktur eines Krankenhauses zu entwickeln. Damit die bei diesen Untersuchungen getroffenen Entscheidungen von Dritten und zu späteren Zeitpunkten leicht nachvollzogen werden können, sind sie hinreichend zu **dokumentieren**. Die Dokumentation sollte insbesondere auch die Begründungen für die gewählten Optionen zur Risikobehandlung einschließen.

Eine gute Dokumentation erleichtert die Qualitätssicherung und Weiterentwicklung des Risikomanagements. Sie hilft bei den hierfür notwendigen Überprüfungen der Sicherheitskonzepte auf deren Umsetzungsstand, Aktualität und Wirksamkeit. Es empfiehlt sich, diese Kontrollen in den Evaluationsprozess für das allgemeine Risikomanagement eines Krankenhauses einzubinden. Solche **Evaluationen**, die alle Phasen und Aspekte des Risikomanagementprozesses einschließen müssen, sollten regelmäßig durchgeführt werden – zum Beispiel jährlich, spätestens jedoch nach fünf Jahren – und können mit der Überprüfung anderer Vorsorgemaßnahmen verknüpft werden, etwa der Krankenhausalarmplanung (siehe [BBK-LF], Seite 67).

Besondere Ereignisse oder Situationen erfordern daneben auch fallweise Evaluierungen, beispielsweise wenn

- sich etwa infolge einer Reorganisation die Geschäftsprozesse eines Krankenhauses geändert haben und die Analyse zur Kritikalität der Prozesse angepasst werden muss,
- sich die IT-Infrastruktur eines Krankenhauses verändert hat, beispielsweise durch neuartige IT-Anwendungen, zusätzliche Server oder eine geänderte Netzstruktur, und geprüft werden muss, ob die Einschätzungen zur Kritikalität der IT-Komponenten noch aktuell sind,
- sich die Gefährdungslage geändert hat, beispielsweise neuartige Bedrohungen bekannt geworden sind, und die Risikoanalyse entsprechend zu ergänzen ist,
- sich durch aktuelle Schadensereignisse, aber auch als Ergebnis einer Übung oder eines Tests, Mängel in den vorhandenen Sicherheitsmaßnahmen gezeigt haben.

Sowohl für die periodischen als auch die außerplanmäßigen Evaluationen gilt, dass sie nicht nur Mängel in den vorhandenen Risikoanalysen und bei der Umsetzung geplanter Maßnahmen identifizieren, sondern auch Möglichkeiten zur Verbesserung des Risikomanagements aufzeigen sollten. Sie können sowohl intern als auch mit Hilfe externer Dienstleister durchgeführt werden. Hilfestellungen für die systematische Durchführung solcher Überprüfungen bietet der Leitfaden IS-Revision des BSI (siehe [LF-IS-REV]).

Hilfsmittel

H 1: Fragenkatalog

Im Folgenden werden Beispiele für die Fragestellungen zur Prozesserhebung, zur Auswahl kritischer Prozesse und zur Ermittlung kritischer IT-Abhängigkeiten beispielhaft beschrieben.

Fragen zur Prozesserhebung (siehe Kapitel 2.3)

1. Welche Aufgaben erfüllt dieser Prozess?
2. Welche Vorgängerprozesse hat er, welche Nachfolger?
3. Welchen Input liefert der Vorgänger, welche Lieferung erfolgt an den Nachfolgeprozess?

Fragen zur Bestimmung der Kritikalität von Prozessen (siehe Kapitel 3.1)

1. Warum ist dieser Prozess wichtig?
2. Welche Ausfallzeit dieses Prozesses ist im Hinblick auf die übergeordneten Schutzziele maximal tolerierbar?
3. Welche Abhängigkeiten existieren zu anderen Prozessen?

Fragen zur IT-Unterstützung eines Prozesses (siehe Kapitel 3.2)

1. Welche IT-Anwendungen und/oder Medizingeräte werden im Prozess genutzt?
   Beispiele: Krankenhausinformationssystem – KIS, Laborinformationssystem – LIS, Radiologieinformationssystem – RIS, Medizinische Überwachungssysteme, Patientendatenmanagementsystem, Bürosoftware.
2. Welche Informationen sind für die Ausführung des Prozesses erforderlich?
   Beispiele: Laborwerte, Befunde, Medikation, Patientenakte.
3. Welche Informationen werden im Prozess erzeugt?
   Beispiele: Arztbriefe, Pflegedokumentation, Befunde, Operationsberichte, Medikamentendokumentation.

Fragen zur Kritikalität der IT-Anwendungen (siehe Kapitel 3.3)

1. Welche Auswirkungen hat ein IT-Ausfall?
   Beispiele: kein Zugriff auf Befunde, keine Neuaufnahme Externer möglich, kein Zugriff auf administrative Patientendaten, keine Abschlussdokumentation, Medikation problematisch.
2. Welche Ausfallzeit ist ohne Risiko für den Patienten maximal tolerierbar?
3. Welche Ersatzverfahren sind für den Fall eines IT-Ausfalls etabliert und wie hoch ist der geschätzte Aufwand für den Umstieg?
   Beispiele: Papierakte, telefonische Kommunikation, Datenträger (z. B. USB-Stick, CD, DVD).
4. Welche Auswirkungen haben fehlerhaft erfasste, verarbeitete, übertragene oder gespeicherte Daten für den oder die Patienten?
5. Sind behandlungs- und/oder lebensnotwendige Daten betroffen?
6. Welche Schutzmaßnahmen sind bereits umgesetzt, um fehlerhafte Informationen und IT-Anwendungen zu erkennen?

7. Welche Auswirkungen hat das Bekanntwerden vertraulicher Informationen auf die Gesundheit und das Leben von Patienten?
8. Welche Auswirkungen hat das Bekanntwerden vertraulicher Informationen auf die Verfügbarkeit und die Integrität der übrigen IT-Anwendungen und IT-Systeme?
9. Welche Schutzmaßnahmen existieren, um Verletzungen der Vertraulichkeit zu erkennen?

H 2: Kriterien zur Bestimmung der Eintrittswahrscheinlichkeit

Faktor	*Bewertung*	*Wert*
Schwachstellenentdeckung: Wie leicht ist die Schwachstelle zu erraten?	Nur mit Insider-Wissen	1
	Mit veröffentlichtem Basiswissen	2
	Mithilfe verfügbarer Werkzeuge	3
	Nicht relevant	--
Fähigkeit: Welche technischen Fähigkeiten setzt ein erfolgreicher Angriff voraus?	Tiefgehende Kenntnisse (Netzwerk, Programmierung, Sicherheitsmechanismen)	1
	Erfahrene Anwenderkenntnisse	2
	Wenige technische Kenntnisse	3
	Nicht relevant	--
Angriffsentdeckung: Wie schnell kann ein Angriff entdeckt werden?	Kurzfristig (durch Echtzeitsysteme, regelmäßige Prüfung von Logdateien)	1
	Mittelfristig (Logging ohne regelmäßige Prüfung der Logdateien)	2
	Langfristig (kein Logging; Abweichungen vom normalen Systembetrieb)	3
	Nicht relevant	--

Tabelle 17: Faktoren der Wahrscheinlichkeit bei vorsätzlichen Handlungen

Faktor	*Bewertung*	*Wert*
Ausmaß: Welches Ausmaß (in Anzahl und Schweregrad) ist für die Kompromittierung des Zielobjekts durch die potenziellen Fehlerquellen zu erwarten?	Nur wenige und nicht schwerwiegende Fehlerquellen	1
	Entweder viele oder schwerwiegende Fehlerquellen	2
	Viele und schwerwiegende Fehlerquellen	3
	Nicht relevant	--
Fehlertoleranz: Wie reagiert das Zielobjekt auf Fehlhandlungen?	Sicher und korrekt	1
	Systembetrieb sicher, aber Leistung vermindert	2
	Instabiles Systemverhalten	3
	Nicht relevant	--

Tabelle 18: Faktoren der Wahrscheinlichkeit bei menschlichen Fehlhandlungen

Faktor	*Bewertung*	*Wert*
Ausmaß: Welches Ausmaß (in Anzahl und Schweregrad) ist für die Kompromittierung des Zielobjekts durch die potenziellen Fehlerquellen zu erwarten?	Nur wenige und nicht schwerwiegende Fehlerquellen	1
	Entweder viele oder schwerwiegende Fehlerquellen	2
	Viele und schwerwiegende Fehlerquellen	3
	Nicht relevant	--
Fehlertoleranz: Wie reagiert das Zielobjekt auf Fehlhandlungen?	Sicher und korrekt	1
	Systembetrieb sicher, aber Leistung vermindert	2
	Instabiles Systemverhalten	3
	Nicht relevant	--

Tabelle 19: Faktoren der Wahrscheinlichkeit bei technischem Versagen

Faktor	*Bewertung*	*Wert*
Redundanz: Welche Vorkehrungen wurden getroffen, um auf ein Ersatzsystem umzusteigen?	Es existiert wenigstens ein identisches Ersatzsystem, das alle Funktionen des Primärsystems parallel ausführt.	1
	Es existiert ein identisches Ersatzsystem, das erst im Falle einer Störung oder eines Ausfalls eingeschaltet oder bereitgestellt wird und dann alle Funktionen des Primärsystems ausführt.	2
	Es existiert kein Ersatzsystem.	3
	Nicht relevant	--
Exposition: In welchem Maß ist das System durch seine räumliche Lage einer potenziellen Bedrohung durch ein natürliches Ereignis ausgesetzt?	Gering, da das System unter normalen Bedingungen an einer nicht exponierten Stelle aufgestellt und betrieben wird (zum Beispiel oberhalb des Erdgeschosses, weit entfernt von Flüssen oder Erdbebengebieten)	1
	Die Umgebung des Aufstellungsortes des Systems war bereits in der Vergangenheit beinahe in Mitleidenschaft gezogen worden oder es kann nicht ausgeschlossen werden, dass das System an einer exponierten Stelle betrieben wird (eventuell wechselnde Einsatzorte).	2
	Der Aufstellungsort des Systems war bereits in der Vergangenheit von natürlichen Ereignissen betroffen oder das System ist dauerhaft solchen Gegebenheiten ausgesetzt aufgrund seiner Funktion oder seines Einsatzgebietes.	3
	Nicht relevant	--

Tabelle 20: Faktoren der Wahrscheinlichkeit bei natürlichen Ereignissen

Faktor	*Bewertung*	*Wert*
Interne Abhängigkeiten: Ist Ersatzpersonal in ausreichendem Maße vorhanden?	Es stehen permanent mehrere Personen für die Erfüllung von Aufgaben zur Verfügung.	1
	Es kommt zu Engpässen, wenn Personal durch Krankheit ausfällt.	2
	Das Personal ist permanent unterbesetzt.	3
	Nicht relevant	--
Externe Abhängigkeiten: Wie stark ist der Betrieb der Systeme von externen Diensten abhängig?	Gering (nur für die Grundversorgung)	1
	Mäßig (Grundversorgung sowie Wartung und Support)	2
	Hoch (Grundversorgung, Wartung und Support sowie Betrieb von Systemen)	3
	Nicht relevant	--
Planungssicherheit: Wird der Einsatz von Ressourcen geplant und überwacht?	Ressourcen werden regelmäßig geplant und überwacht.	1
	Ressourcen werden geplant, aber nicht auf tatsächlichen Einsatz überprüft.	2
	Es findet keine Ressourcenplanung statt.	3
	Nicht relevant	--

Tabelle 21: Faktoren der Wahrscheinlichkeit bei organisatorischen Mängeln

Glossar

Begriff	*Beschreibung*
Bedrohung	Umstand oder Ereignis, durch den oder das ein Schaden an einem Zielobjekt (IT-Komponente) und eine Beeinträchtigung der Verfügbarkeit entstehen können. Bedrohungen können sich aus Einwirkungen durch höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen ergeben. Anmerkung: Der Begriff „Bedrohung“ entspricht dem Begriff der „Gefahr“ in [BBK-LF].
Behandlungsprozess	Der Behandlungsprozess beschreibt auf einer abstrahierten Ebene den Durchlauf eines Patienten im Krankenhaus während seiner Behandlung. Der Prozess beginnt mit der Aufnahme und endet mit der Entlassung bzw. der Verlegung des Patienten.
Eintrittswahrscheinlichkeit	Ein Kriterium der Risikobewertung. Der Wert, der die Wahrscheinlichkeit des Eintretens eines Risikoszenarios beschreibt.
Gefahr	Der Begriff „Gefahr“ wird in diesem Leitfaden synonym zum Begriff „Bedrohung“ verwendet.
Gefährdung	Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Zielobjekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Zielobjekt. (Quelle: [GS-KAT])
Grundwerte	Andere Bezeichnung für die Schutzziele der Informationssicherheit. Die drei elementaren Grundwerte sind Verfügbarkeit, Integrität und Vertraulichkeit.
Integrität	Schutzziel, das die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen bezeichnet.
IT-Anwendung	Anwendungssystem zur Unterstützung der klinischen und medizinischen Abläufe (z. B. Krankenhausinformationssystem, Bildarchivierungssystem, Bürosoftware). IT-Anwendungen, von deren Verfügbarkeit die Funktionsfähigkeit kritischer Prozesse in besonderem Maße abhängig ist, werden als kritische IT-Anwendungen bezeichnet.
IT-Komponente	Technische Komponente (Hardware, Software, Kommunikationsverbindung), die für den Betrieb einer IT-Anwendung erforderlich ist. IT-Komponenten, die zur Funktionsfähigkeit einer kritischen Anwendung beitragen, können selbst als kritisch bezeichnet werden.

Begriff	*Beschreibung*
Kritikalität	Maß für die Bedeutsamkeit eines Prozesses oder einer Ressource in Bezug auf die Patientenversorgung und die Funktionsfähigkeit des Krankenhauses.
Kritische Infrastruktur	Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden. (Quelle: [KRITIS_STRAT])
Prozess	Summe der Tätigkeiten und Bearbeitungsschritte in einem Krankenhaus zur Erbringung einer Dienstleistung.
Risiko	Produkt aus der Eintrittswahrscheinlichkeit und der Auswirkungen eines Schadens.
Risikoanalyse	Systematisches Verfahren zur Identifikation und Bewertung von Risiken.
Risikobewertung	Verfahren zur Feststellung, ob ein Risiko vermieden, verringert, verlagert oder akzeptiert werden kann.
Risikomanagement	Prozess bzw. Verfahren zum planvollen Umgang mit Risiken.
Risikomatrix	Mit der Risikomatrix wird der Risikowert dargestellt. Dabei werden die Eintrittswahrscheinlichkeit und Schadensauswirkung angegeben.
Risikoszenario	Sinnvolle Kombination einer Bedrohung mit einer hierzu passenden Schwachstelle (synonym zu „Gefährdung“).
Risikowert	Maß zur Bewertung eines Risikos aufgrund von Einschätzungen zur Eintrittswahrscheinlichkeit und den Auswirkungen eines Schadensereignisses.
Schutzbedarf	Beschreibung, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist. (Quelle: [GS-KAT])
Schutzziel, übergeordnet	Beschreibung eines herbeizuführenden Sollzustandes bezüglich zu schützender Bereiche (Prozesse) eines Krankenhauses. Schutzziele enthalten generelle, strategische Festlegungen über das anzustrebende Niveau der Ausfallsicherheit des Krankenhauses und seiner Organisationseinheiten. Die übergeordneten Schutzziele werden zur Ermittlung kritischer Prozesse herangezogen. (Quelle: [BBK-LF])

Begriff	*Beschreibung*
Schutzziel, Informationstechnik	Konkretisierung der übergeordneten Schutzziele für den Bereich der Informationstechnik. Sie dienen als Maßstab für die Ermittlung kritischer IT-Abhängigkeiten und die Risikobewertung. Für die Definition werden die Grundwerte der Informationssicherheit (Verfügbarkeit, Integrität, Vertraulichkeit) herangezogen.
Schwachstelle	Fehler eines Objekts oder einer Institution, der dazu führen kann, dass eine Bedrohung wirksam wird und Schaden verursacht.
Verfügbarkeit	Schutzziel, das den Grad der Gewährleistung des Zugriffs auf Prozesse und Ressourcen bezeichnet.
Vertraulichkeit	Schutzziel, das den Schutz vor unbefugter Preisgabe von Informationen bezeichnet.
Verwundbarkeit	Der Begriff „Verwundbarkeit“ wird in diesem Leitfaden synonym zum Begriff „Schwachstelle“ verwendet und weicht somit von der Begriffsdefinition in [BBK-LF] ab.
Zielobjekt	Zielobjekte sind im Kontext der Risikoanalyse Krankenhaus-IT alle kritischen IT-Komponenten des Untersuchungsbereichs.

Literaturverzeichnis

BBK-LF	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.): Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus. Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens, 2008, https://www.kritis.bund.de.
BBK-RM-KH	Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.): Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus; Praxis im Bevölkerungsschutz Band 2, 2008, https://www.kritis.bund.de.
BMI-LF	Bundesministerium des Innern (Hrsg.): Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Ein Leitfaden für Unternehmen und Behörden, 2008, https://www.kritis.bund.de.
BSI 100-1	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), 2008, https://www.bsi.bund.de/Standards.
BSI 100-2	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, 2008, https://www.bsi.bund.de/Standards.
BSI 100-4	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): BSI-Standard 100-4: Notfallmanagement, 2008, https://www.bsi.bund.de/Standards.
GS-KAT	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): IT-Grundschutz-Kataloge, fortlaufend aktualisiert, https://www.bsi.bund.de/IT-Grundschutz-Kataloge.
IEC 80001	International Electrotechnical Committee (Hrsg.): IEC 80001. Application of risk management for IT-networks incorporating medical devices, 2010/12.
ISi Client	Bundesamt für Sicherheit in der Informationstechnik: Absicherung eines PC-Clients (Leitlinie, Studie und Checklisten), 2011, https://www.bsi.bund.de/ISi-Reihe.
ISi FERN	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Sicherer Fernzugriff auf das interne Netz (Leitlinie, Studie und Checklisten), 2010, https://www.bsi.bund.de/ISi-Reihe.
ISi LANA	Bundesamt für Sicherheit in der Informationstechnik: Sichere Anbindung von lokalen Netzen an das Internet (Leitlinie, Studie und Checklisten), 2012, https://www.bsi.bund.de/ISi-Reihe.
ISi VPN	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Virtuelles Privates Netz (Leitlinie), 2009, https://www.bsi.bund.de/ISi-Reihe.
ISi WebClient	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Sichere Nutzung von Web-Clients (Leitlinie, Studie und Checklisten), 2008/12, https://www.bsi.bund.de/ISi-Reihe.
ISi WLAN	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Sichere Nutzung von WLAN (Leitlinie), 2009, https://www.bsi.bund.de/ISi-Reihe.
ISi-E	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Internet-Sicherheit: Einführung, Grundlagen, Vorgehensweise, 2011, https://www.bsi.bund.de/ISi-Reihe.
ISO 27002	International Organization for Standardization (Hrsg.): ISO/IEC 27002:2005. Information technology -- Security techniques -- Code of practice for information security management, 2005.
ISO 27005	International Organization for Standardization (Hrsg.): ISO/IEC 27005:2011. Information technology -- Security techniques -- Information security risk management, 2011.
ISO 27999	International Organization for Standardization (Hrsg.): ISO 27799:2008. Health informatics -- Information security management in health using ISO/IEC 27002, 2008.
ISO 9001	Deutsches Institut für Normung (Hrsg.): DIN EN ISO 9001:2008. Qualitätsmanagementsysteme - Anforderungen, 2008.
KRITIS-STRAT	Bundesministerium des Innern (Hrsg.): Nationale Strategie zum Schutz Kritischer Infrastrukturen, 2009, http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf.
LF-IS	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Leitfaden Informationssicherheit, 2012, https://www.bsi.bund.de/Publikationen.

LF-IS-REV	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Leitfaden IS-Revision, 2010, https://www.bsi.bund.de/is-revision.
RIKRIT-BMTAB	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Zusammenstellung Bedrohungen – Maßnahmen – IT-Komponentengruppen, 2013, https://www.kritis.bund.de.
RIKRIT-RISIKEN	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Kreuztabelle Bedrohungen – Schwachstellen, 2013, https://www.kritis.bund.de.
RiKrIT-ÜB	Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT – Management-Kurzfassung, 2013, https://www.kritis.bund.de.