Bundesamt
für Sicherheit in der
Informationstechnik

Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT

Management-Kurzfassung

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

IT-Risiken im Gesundheitswesen

Krankenhäuser erbringen als eine der tragenden Säulen unseres Gesundheitswesens vielfältige medizinische und pflegerische Dienstleistungen und zählen daher zu den Kritischen Infrastrukturen unserer Gesellschaft. Dabei ist die Funktionsfähigkeit dieser Einrichtungen selbst wiederum nicht nur von weiteren externen Kritischen Infrastrukturen, wie beispielsweise der Strom- und Wasserversorgung, abhängig, sondern auch bereits in hohem Maße von der vor Ort eingesetzten Informationstechnologie. Diese findet sich in zahlreichen Formen von Anwendungen zur Behandlungsdokumentation über Inventar- und Bestellsysteme bis hin zu medizintechnischen Geräten wieder. Sie unterstützt bei bisher papiergebundenen Arbeitsabläufen und erleichtert Diagnose- und Behandlungsprozesse oder macht diese sogar erst möglich.

Neben der Möglichkeit zur Optimierung und Effizienzsteigerung von Prozessen birgt die zunehmende IT-Unterstützung aber auch neue Risiken, denen im Rahmen des Risikomanagements entsprechend begegnet werden muss. Bisher standen hier vor allem Risiken im Bereich des Datenschutzes, beispielsweise bei der Einführung elektronischer Patientenakten, im Fokus von Untersuchungen zur Sicherheit der Krankenhaus-IT. Aus dem Blickwinkel Kritischer Infrastrukturen, welcher auf die Aufrechterhaltung der Verfügbarkeit der medizinischen Versorgung abzielt, treten solche Überlegungen jedoch in den Hintergrund.

Der effektive Umgang mit IT-Risiken erfordert in jedem Fall eine strukturierte Vorgehensweise, in welcher der IT-Risikoanalyse als wichtigem Werkzeug zur Identifikation der relevanten Risiken eine zentrale Rolle zukommt. Die IT-Risikoanalyse unterstützt damit bestehende Ansätze zum Informationssicherheits- und Risikomanagement und erleichtert sowohl Priorisierung als auch Auswahl der umzusetzenden Maßnahmen. Dabei ersetzt die IT-Risikoanalyse aber in keinem Fall die zwingend notwendige organisatorische Verankerung des Themas „IT-Sicherheit“ oder eine umfassende Sicherheitskonzeption nach gängigen Standards.

Diese Broschüre bietet allen Interessierten einen ersten Überblick über eine branchenspezifische Methode zur IT-Risikoanalyse. Die Methode wurde im Rahmen des Projekts „Risikoanalyse Krankenhaus-IT“ (RiKrIT) im Auftrag des *Bundesamts für Sicherheit in der Informationstechnik* (BSI) in Zusammenarbeit mit dem *Bundesamt für Bevölkerungsschutz und Katastrophenhilfe* (BBK), der *Senatsverwaltung für Gesundheit und Soziales* (SenGS) Berlin und dem *Unfallkrankenhaus Berlin* (ukb) entwickelt.

Mit der Entwicklung dieser auf IT zugeschnittenen Methode zur Risikoanalyse in Krankenhäusern ergänzt das Projekt bestehende Ansätze zum Risiko- und Krisenmanagement in Krankenhäusern bzw. Kritischen Infrastrukturen und ermöglicht den Brückenschlag zum Thema der Informations- und Cyber-Sicherheit.

Der Leitfaden „Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT“ mit einer ausführlichen Beschreibung zur Anwendung der hier kurz dargestellten Methode und weitere Hilfsmittel stehen auf der Internetseite www.kritis.bund.de zum Download zur Verfügung.

1 Einführung

1 Einführung

Diese Broschüre gibt einen kurzen Überblick über die in dem Leitfaden „Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT“ [LF-RiKrIT] dargestellte Methode zur Untersuchung der Risiken, die mit dem zunehmenden Einsatz von Informationstechnik (IT) in einem Krankenhaus verbunden sind. Die Zielsetzungen und der Nutzen dieser – nachfolgend als IT-Risikoanalyse bezeichneten – Methode für die Verbesserung der IT-Sicherheit in einem Krankenhaus werden beschrieben. Darüber hinaus wird gezeigt, wie sich die IT-Risikoanalyse in das übergreifende Risikomanagement eines Krankenhauses einordnen lässt.

Neben Hinweisen zu Zielen und Nutzen enthält diese Broschüre auch eine kurze Beschreibung der Teilschritte der IT-Risikoanalyse. Diese Darstellung soll die zugehörigen Aufgaben zeigen und eine Einschätzung des Aufwands ermöglichen, der für die Durchführung erforderlich ist. Für detaillierte Handlungsanleitungen wird auf den oben genannten Leitfaden verwiesen, der zusammen mit ergänzenden Hilfsmitteln unter www.kritis.bund.de zum Download angeboten wird.

1.1 Krankenhäuser als Kritische Infrastruktur

Unsere Gesellschaft ist in hohem Maße davon abhängig, dass bestimmte Basisdienste zuverlässig erbracht werden. Beispielsweise muss die Versorgung mit Wasser, Energie und Nahrungsmitteln gesichert sein – gleiches gilt für das Transportwesen, die Informations- und Kommunikationsnetze oder das Gesundheitswesen.

KRITIS-Sektoren	Branchen im Sektor
Energie	
Informationstechnik und Telekommunikation	medizinische Versorgung
Gesundheit	Arzneimittel und Impfstoffe
Wasser	Labore
Ernährung	
Transport und Verkehr	
Finanz- und Versicherungswesen	
Staat und Verwaltung	
Medien und Kultur	

Abbildung 1: Sektoren der Kritischen Infrastrukturen

Diese für das störungsfreie Funktionieren des sozialen Lebens unerlässlichen Dienste bilden die **Kritischen Infrastrukturen** (KRITIS) einer Gesellschaft (siehe Abbildung 1). Hierzu zählen gemäß der im Bund verwendeten Definition der „Nationalen Strategie zum Schutz Kritischer Infrastrukturen“ alle Einrichtungen, „deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen“ nach sich ziehen würde.[1]

Krankenhäuser sind aufgrund ihrer herausragenden Bedeutung für das Wohlergehen der Bevölkerung ein wichtiger Teil dieser Kritischen Infrastrukturen. Sie haben daher eine besondere Verpflichtung, die Verfügbarkeit ihrer Dienstleistungen sicherzustellen. Um dieser Verpflichtung gerecht werden zu können, sollten Krankenhäuser die potenziellen Risiken für die Funktionsfähigkeit ihrer Prozesse kennen und geeignete Strategien zu deren Behandlung entwickeln.

1.2 Risiken durch zunehmende IT-Abhängigkeit

Wie in den meisten Bereichen der modernen Gesellschaft werden auch in heutigen Krankenhäusern Prozesse und Strukturen immer stärker und auf vielfältige Weise durch Informationstechnik geprägt. Dies gilt sowohl für die administrativen Abläufe der Einrichtungen als auch für deren Kernaufgabe, die medizinische Versorgung und Pflege der Patienten: Krankenhausinformationssysteme für administrative Daten und Patientendaten, Spezialanwendungen für Funktionsbereiche wie Labor, Radiologie oder Intensivstation, elektronische Patientenakten und eine umfassende Vernetzung der Anwendungssysteme sind aus modernen Krankenhäusern nicht mehr wegzudenken. Informationstechnik ist zu einer der wichtigsten Ressourcen für die Prozesse dieser Einrichtungen geworden.

Es gibt viele Belege dafür, wie verwundbar Krankenhäuser durch Naturkatastrophen oder durch den Ausfall wichtiger Ressourcen wie Strom oder Wasser sind (siehe beispielsweise die Folgen eines Gewitterregens in Mittelhessen im Jahr 2006[2] oder eines Kurzschlusses in einem Hamburger Krankenhaus im Jahr 2008[3]). Mit zunehmender IT-Durchdringung wächst jedoch die Gefahr, dass Krankenhausprozesse nicht nur durch solche konventionellen Risiken, sondern auch durch Ausfälle oder Störungen der IT erheblich beeinträchtigt werden oder sogar komplett ausfallen können. Dass diese Risiken ernst zu nehmen sind, belegt nicht nur die Vielzahl an bekannt gewordenen IT-Sicherheitsvorfällen und IT-Störungen in Unternehmen und Behörden. Auch Krankenhäuser waren in den letzten

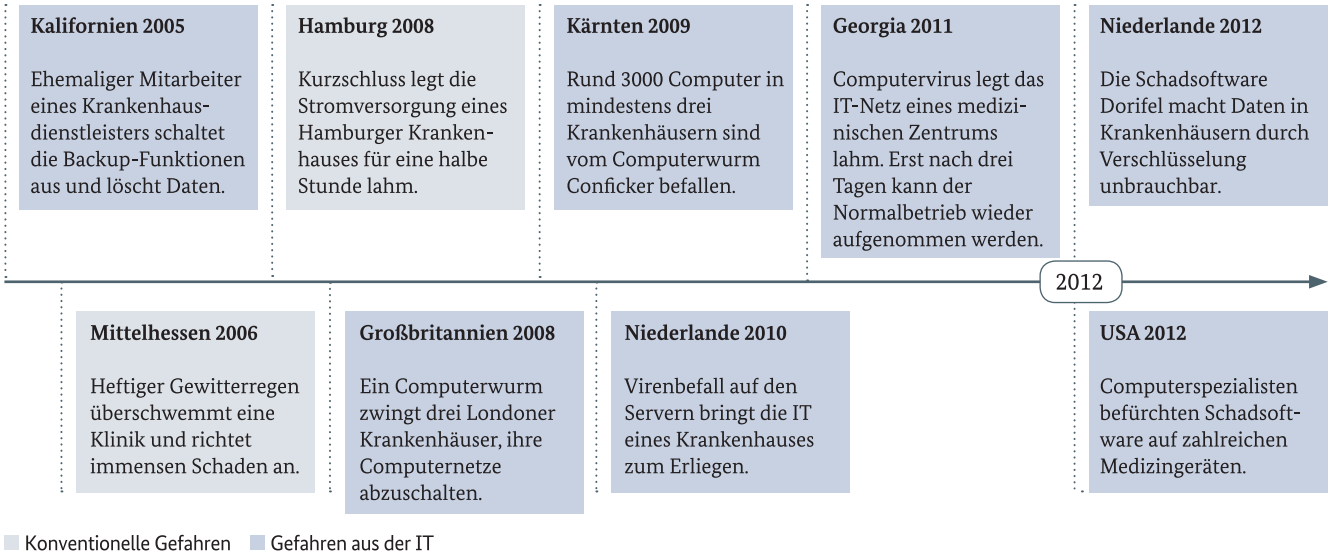


Abbildung 2: Exemplarische Sicherheitsvorfälle

Jahren schon von Ausfällen, Schadsoftware und anderen IT-Sicherheitsvorfällen betroffen, wie beispielsweise Meldungen aus den Vereinigten Staaten (Kalifornien im Jahr 2005[4], Georgia im Jahr 2011[5]), Großbritannien (im Jahr 2008)[6], Österreich (Kärnten im Jahr 2009)[7] sowie den Niederlanden (aus den Jahren 2010[8] und 2012[9]) belegen. Computer-Experten vermuten, dass mittlerweile auch Medizingeräte, die in ein Krankenhausnetz integriert sind, eine besondere Anfälligkeit gegen Computerviren haben.[10] Die Beispiele (siehe Abbildung 2) zeigen einen Ausschnitt der möglichen Bedrohungen und offenbaren Schwachstellen, die das Eintreten von Sicherheitsvorfällen begünstigen, wie etwa veraltete Technik, unzureichende Schutzmechanismen, unterbliebene Tests von Notfallmaßnahmen oder die Unzufriedenheit von Mitarbeitern. In allen angeführten Fällen entstanden in erster Linie Sachschäden und finanzielle Verluste für die betroffenen Krankenhäuser. Nachhaltige Schäden für die Patienten blieben glücklicherweise aus. Gleichwohl verdeutlichen diese Beispiele, wie wichtig der Schutz der IT-Infrastruktur für ein Krankenhaus heutzutage ist.

1.3 IT-Risikoanalyse: Ziele und Einordnung

Die IT-Risikoanalyse trägt dazu bei, angemessene Vorkehrungen zum Schutz der IT-Infrastruktur eines Krankenhauses zu treffen. In einer solchen Untersuchung werden

- Prozesse im Krankenhaus, bei denen der Ausfall der unterstützenden IT-Anwendungen gravierende Folgen hätte,
- Bestandteile der IT-Infrastruktur, die für das störungsfreie Funktionieren dieser IT-Anwendungen unverzichtbar sind, sowie
- Bedrohungen und Schwachstellen, welche die Funktionsfähigkeit dieser kritischen IT-Komponenten gefährden können,

identifiziert und bewertet.

Die IT-Risikoanalyse zeigt damit auf, an welchen Stellen anzusetzen ist, um die Verfügbarkeit der kritischen Prozesse eines Krankenhauses sicherzustellen. Sie hilft dabei, angemessene Entscheidungen zur Auswahl von geeigneten Sicherheitsmaßnahmen zu treffen. Weil sie damit Ergebnisse liefert, die auch für das Informationssicherheits- und das Risikomanagement eines Krankenhauses wichtig sind, sollte sie mit diesen Aktivitäten eng verzahnt werden.

Aufgabe des **Informationssicherheitsmanagements** ist es, durch eine geeignete Organisationsstruktur und definierte Sicherheitsprozesse systematisch und nachhaltig für die Sicherheit der Informationen, Anwendungen und IT-Systeme und damit der Prozesse eines Krankenhauses zu sorgen. Die IT-Risikoanalyse liefert Entscheidungshilfen für Maßnahmen, die darauf abzielen, die Verfügbarkeit der für die Kranken-

hausprozesse unverzichtbaren IT-Infrastruktur zu sichern. Ein etabliertes Informationssicherheitsmanagement erleichtert die Umsetzung solcher Maßnahmen. Andere Aspekte der Informationssicherheit, zum Beispiel auch solche des Datenschutzes, liegen hingegen aufgrund der eingangs skizzierten Aufgabenstellung nicht im primären Fokus der hier vorgestellten IT-Risikoanalyse.

Unter Umständen ist in einem Krankenhaus – etwa aufgrund der Vorgaben des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) – bereits ein **Risikomanagement** (hier: „übergeordnetes Risikomanagement“) eingerichtet, in dem Ausfallrisiken beispielsweise aufgrund von Naturkatastrophen oder Versorgungsengpässen untersucht und Lösungen zu deren Behandlung entwickelt werden. Vorgehensweisen für ein solches Risikomanagement und darüber hinaus das Notfall- und Krisenmanagement finden sich beispielsweise in den folgenden beiden Publikationen:

- „Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Ein Leitfaden für Unternehmen und Behörden“ [LF-BMI] des Bundesministeriums des Innern und
- „Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus“ [LF-BBK] des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe.

In den genannten Leitfäden werden Risiken durch Informationstechnik für die Kritische Infrastruktur Krankenhaus berücksichtigt, jedoch nicht im Detail betrachtet.

Sofern ein solches besteht, sollte die IT-Risikoanalyse in ein übergeordnetes Risikomanagement eingegliedert werden. Dies bedeutet, dass Ergebnisse und Verfahrensweisen der übergeordneten Risikoanalyse übernommen werden sollten. Umgekehrt können Ergebnisse der IT-Risikoanalyse in das übergeordnete Risikomanagement einfließen und die dort durchgeführten Risikoanalysen durch die intensive Betrachtung der wichtigen Ressource „Informationstechnik“ ergänzen.

Ähnliches gilt für ein zum Beispiel auf der Grundlage des BSI-Standards 100-4 eingerichtetes **Notfallmanagement**. Dessen Ziel ist es, die Kontinuität der wichtigen Prozesse einer Einrichtung und damit deren Existenz zu sichern, und zu diesem Zweck Vorkehrungen zur Vorsorge gegen und zum Umgang mit Notfällen zu entwickeln. Grundlage hierfür ist eine intensive Untersuchung der Kritikalität der Prozesse und der von diesen benötigten Ressourcen. Im Blickfeld des Notfallmanagements stehen dabei sämtliche Ressourcen, die für eine Einrichtung wichtig sind, nicht nur die Informationstechnik, also auch die Behandlung von Notfällen, wie den in den obigen Beispielen erwähnten Stromausfällen.

Derzeit bestehen – im Unterschied etwa zu den detaillierten Vorgaben zum Brandschutz – noch kaum IT-spezifische rechtliche Verpflichtungen zur Absicherung der Kritischen Infrastrukturen des Gesundheitswesens. Dennoch ist die Aufrechterhaltung der Funktionsfähigkeit der IT-Infrastruktur aus dem Risikomanagement eines Krankenhauses nicht mehr wegzudenken. Die Anwendung der nachfolgend dargestellten Vorgehensweise zur IT-Risikoanalyse kann hierzu einen wichtigen Beitrag leisten.

2 IT-Risikoanalyse: die Methode RiKrIT

2 IT-Risikoanalyse: die Methode RiKrIT

Die IT-Risikoanalyse umfasst eine Reihe von Teilschritten, die sich zusammen mit den vor- und nachgelagerten Aktivitäten in vier Aufgabenblöcke gliedern lassen:

- Vorbereitende Aktivitäten,
- Kritikalität von Prozessen und IT analysieren,
- Risiken identifizieren und bewerten,
- Risiken behandeln.

Im Folgenden wird der Inhalt dieser Aufgabenblöcke für die hier entwickelte Methode zur „Risikoanalyse Krankenhaus-IT“ im Überblick dargestellt.

2.1 Vorbereitende Aktivitäten

Für den Erfolg der IT-Risikoanalyse ist die Unterstützung der Leitung und anderer Führungsebenen des Krankenhauses unabdingbar. Dies erleichtert es, bereits vor und auch während der Startphase der Untersuchung passende Weichenstellungen für deren effiziente Durchführung vorzunehmen.

Zunächst muss das Vorhaben im Rahmen der **Initialisierung** organisatorisch verankert werden. Es muss entschieden werden, wer für die Durchführung dieser Untersuchung verantwortlich und wer mit welchen Aufgaben daran zu beteiligen ist. Bei der Auswahl der Beteiligten ist darauf zu achten, dass Schlüsselpersonen, etwa die Leitungen der in die Untersuchung einbezogenen Organisationseinheiten oder auch die Mitarbeitervertretung, rechtzeitig einbezogen werden, um sich so deren Unterstützung zu sichern. Bei Ressourcenknappheit oder fehlender Erfahrung mit der IT-Risikoanalyse ist auch zu entscheiden, ob und für welche Aufgaben externe Hilfe in Anspruch genommen werden soll.

Als Maßstab für die Ermittlung kritischer Prozesse und IT-Ressourcen sowie für die Entscheidungen zur Risikobehandlung sind **Schutzziele** zu definieren, die sich an den übergeordneten Zielen der Einrichtung orientieren, beispielsweise an der aus dem Auftrag eines Krankenhauses abzuleitenden Verpflichtung zum Schutz der Gesundheit der Patienten oder dem Interesse an einer Aufrechterhaltung der wirtschaftlichen Existenzfähigkeit der Einrichtung. Für die IT werden die Schutzziele durch die im Rahmen der Informationssicherheit üblichen Grundwerte Verfügbarkeit, Integrität und Vertraulichkeit konkretisiert.

Aufgrund der speziellen Ausrichtung der IT-Risikoanalyse im Kontext Kritischer Infrastrukturen steht die Sicherung der Verfügbarkeit und Integrität der IT-Infrastruktur an oberster Stelle. Das Ziel der Vertraulichkeit wird in die Betrachtung einbezogen, da durch dessen Verletzung sich in der Folge Verletzungen der Verfügbarkeit und der Integrität ergeben können. Eine mögliche Definition der **IT-Schutzziele** lautet beispielsweise wie folgt:

„IT-Störungen dürfen nicht dazu führen, dass

- die medizinischen Versorgungskapazitäten nicht mehr in angemessener Qualität und Quantität aufrechterhalten werden können **(Verfügbarkeit)**,
- Daten verfälscht werden, deren Richtigkeit für die Versorgung eines Patienten unbedingt erforderlich ist **(Integrität)**,

→ Daten, deren Bekanntwerden sekundär die Verfügbarkeit und Integrität der IT-Infrastruktur beeinträchtigen oder die Sicherheit eines Patienten gefährden können, unberechtigten Dritten zugänglich werden **(Vertraulichkeit)**."

Vor Beginn der IT-Risikoanalyse ist ferner deren **Untersuchungsbereich** abzugrenzen und sind – falls eine solche Zusammenstellung noch nicht existiert – die in diesem angesiedelten Prozesse zu erheben und zu dokumentieren. Der Untersuchungsbereich kann die gesamte Einrichtung umfassen oder auf einzelne Standorte, Gebäude oder organisatorische Einheiten begrenzt werden. Da der Aufwand für die nachfolgenden Schritte steigt, je weiter der Untersuchungsbereich gewählt wird, kann es etwa bei begrenzten Ressourcen für die IT-Risikoanalyse durchaus sinnvoll sein, sich bei dieser Abgrenzung auf einen Ausschnitt des Krankenhauses zu beschränken, beispielsweise auf solche Organisationseinheiten, für die eine IT-Risikoanalyse besonders dringlich erscheint.

Die aus der Prozesserhebung resultierende **Prozessübersicht** muss alle im Untersuchungsbereich angesiedelten Prozesse zur unmittelbaren pflegerischen und medizinischen Patientenversorgung (Kernprozesse) sowie die für das reibungslose Funktionieren dieser Prozesse erforderlichen Unterstützungsprozesse, beispielsweise die Dienstleistungen von Logistik, Küche oder Haustechnik, vollständig umfassen.

Erforderliche Kenntnisse

Eine Prozessübersicht des Untersuchungsbereichs ist eine wichtige Grundlage für die Ermittlung kritischer Prozesse und deren IT-Abhängigkeiten. Sofern eine solche Übersicht noch nicht existiert, ist sie daher für die IT-Risikoanalyse neu anzufertigen. Hierfür sind Interviews mit Mitarbeitern der verschiedenen Organisationseinheiten des Untersuchungsbereichs zu führen und die Ergebnisse in geeigneter Form zu dokumentieren. Es erleichtert diese Arbeit, wenn die Personen, die die Prozesserhebung durchführen, Kenntnisse und Erfahrungen in der Prozessmodellierung haben.

Rolle der Krankenhausleitung

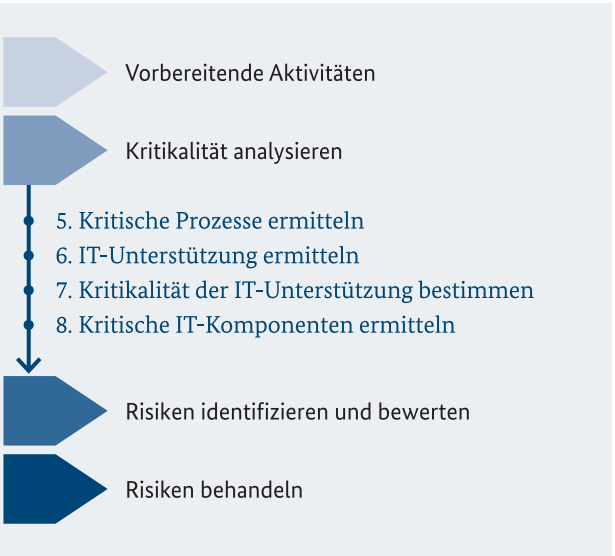
Aufgrund ihrer zentralen Verantwortung für das ordnungsgemäße Funktionieren der Krankenhausprozesse müssen alle grundlegenden Entscheidungen, die für die IT-Risikoanalyse und in ihrem Rahmen getroffen werden, von der Krankenhausleitung mitgetragen werden. Hierzu gehören bei den Vorarbeiten insbesondere die Entscheidungen zur Abgrenzung des Untersuchungsbereichs sowie zu den Definitionen der übergeordneten Schutzziele des Krankenhauses und den auf diese bezogenen IT-Schutzzielen. Eine wesentliche Voraussetzung hierfür ist eine regelmäßige Unterrichtung der Leitung. Zu diesem Zweck sind bei der Initialisierung der IT-Risikoanalyse geeignete Verfahrensweisen festzulegen.

Bezug zum übergeordneten Risikomanagement

Falls im Krankenhaus bereits ein übergeordnetes Risikomanagement (z. B. nach [BBK-LF]) etabliert ist, können in diesem Rahmen erarbeitete Ergebnisse den Aufwand für die IT-Risikoanalyse erheblich verringern. Es sollte zudem darauf geachtet werden, Widersprüche zwischen einer übergeordneten Risikoanalyse und der IT-Risikoanalyse – zum Beispiel sich widersprechende Schutzzieldefinitionen – zu vermeiden.

Ausführlich sind die Vorarbeiten für die IT-Risikoanalyse in Kapitel 2 des Leitfadens „Risikoanalyse Krankenhaus-IT" beschrieben.

2.2 Kritikalität analysieren



Aufgabe der **Kritikalitätsanalyse** ist es, die Abhängigkeiten wesentlicher Prozesse eines Krankenhauses von der eingesetzten Informationstechnik zu erkennen. Ziel ist, diejenigen Teile der IT-Infrastruktur zu identifizieren, deren Ausfallsicherheit und Störungsfreiheit für die unterstützten Prozesse besonders dringlich ist und deren Ausfallrisiken folglich zu begrenzen sind. In diesem Aufgabenblock sind daher zunächst diejenigen Prozesse zu bestimmen, deren Ausfall für die Schutzziele der Einrichtung von kritischer Bedeutung ist. Für diese kritischen Prozesse sind sodann deren IT-Unterstützung und deren Kritikalität zu ermitteln.

Für die Bestimmung der **Kritikalität der Prozesse** bieten sich Interviews mit Mitarbeitern der beteiligten Organisationseinheiten an. Hierfür sind geeignete und zu den übergeordneten Schutzzielen des Krankenhauses passende Bewertungskriterien zu definieren. Diese ergeben sich beispielsweise im Hinblick auf das Schutzziel „Schutz der Patienten" aus den Auswirkungen eines Ausfalls oder einer Störung des Prozesses auf die Patientenversorgung und somit auf das Leben und die Gesundheit der betroffenen Patienten. Wichtig ist, dass die kritischen Prozesse sorgfältig bestimmt werden und Prozesse nicht vorschnell als unkritisch eingestuft und von der weiteren Untersuchung ausgeschlossen werden.

Für die sich anschließende Bestimmung der **Kritikalität der Informationstechnik** ist zunächst zu ermitteln, welche IT-Anwendungen in den kritischen Prozessen verwendet werden und für welche Aufgaben der IT-Einsatz jeweils erforderlich ist. In Abstimmung mit den Prozessbeteiligten ist ferner – beispielsweise mithilfe von Kriterien wie der maximal tolerierbaren Ausfallzeit – zu bewerten, wie schwerwiegend sich Störungen der IT auf die Erledigung dieser Aufgaben auswirken würden. Für die hierbei als kritisch identifizierten IT-Anwendungen ist dann mit sachkundigen Mitarbeitern der IT-Abteilung zu untersuchen, welche technischen Komponenten für den Betrieb der IT-Anwendungen unbedingt erforderlich, also „kritisch" sind. Hierzu zählen üblicherweise IT-Objekte wie Server, Clients, Kommunikationsnetze oder Speichersysteme.

Erforderliche Kenntnisse

Für die Kritikalitätsanalyse ist zu ermitteln, wie kritisch ein Prozess im Hinblick auf die Einhaltung der Schutzziele des Krankenhauses ist, welche IT-Anwendungen in den kritischen Prozessen verwendet werden und welche technischen Komponenten für den Betrieb dieser Anwendungen notwendig sind. Das Wissen zu den ersten beiden Punkten sollte bei den Anwendern, das Wissen zu den kritischen technischen Komponenten bei den IT-Mitarbeitern vorhanden sein, sodass die gewünschten Informationen leicht in Interviews erfragt werden können.

Rolle der Krankenhausleitung

Die Krankenhausleitung muss alle Entscheidungen mittragen, die für das Ergebnis der Kritikalitätsanalyse wichtige Weichenstellungen bedeuten. Hierzu zählt vor allem der bewusste Ausschluss einzelner Prozesse von der Untersuchung. Über die zugrunde gelegten Bewertungskriterien sollte die Krankenhausleitung unterrichtet werden.

Bezug zum übergeordneten Risikomanagement

Wenn im Rahmen einer übergeordneten Risikoanalyse, des Notfallmanagements oder anderer Planungen bereits eine Zusammenstellung kritischer Prozesse und Ressourcen verfasst wurde, können die dort erzielten Ergebnisse nach einer Prüfung ihrer Aktualität und gegebenenfalls vorgenommenen Anpassungen für die IT-Risikoanalyse übernommen werden. Dies gilt in erster Linie für den ersten Teilschritt dieses Aufgabenblocks, die Identifikation der kritischen Prozesse.

In Kapitel 3 des Leitfadens „Risikoanalyse Krankenhaus-IT" werden die Schritte dieses Aufgabenblocks und Hilfsmittel zur Durchführung detailliert beschrieben.

2.3 Risiken identifizieren und bewerten

Im dritten Aufgabenblock sind für die als kritisch identifizierten IT-Komponenten **Risikoszenarien** zu identifizieren und mithilfe von Einschätzungen zu deren Eintrittswahrscheinlichkeiten und Auswirkungen zu bewerten. Ein solches Risikoszenario ergibt sich aus dem Zusammentreffen von Bedrohungen für eine betrachtete IT-Komponente und Schwachstellen, die in ihr oder ihrem Betriebsumfeld vorliegen können. Die Einschätzung der **Eintrittswahrscheinlichkeit** eines Risikoszenarios kann durch die Betrachtung von Faktoren, die dessen Eintreten begünstigen, erleichtert werden. Beispielsweise sind erfolgreiche Angriffe auf IT-Komponenten, die leicht zugänglich sind, wahrscheinlicher als solche, auf die nur ein kleiner Personenkreis Zugriff hat, und Angriffe, die ein tiefes Expertenwissen erfordern, unwahrscheinlicher als solche, für die Kenntnisse eines Computerlaien genügen. Für die Bewertung der **Auswirkungen** ist darauf zu schauen, welche Folgen eine Störung oder Unterbrechung für die Verfügbarkeit der kritischen Prozesse des Krankenhauses hat.

Zur Darstellung des aus der Eintrittswahrscheinlichkeit und der Auswirkung resultierenden **Risikowerts** kann ein fünfstufiges Schema mit den folgenden Kategorien dienen: „Sehr niedrig", „Niedrig", „Mittel", „Hoch" und „Sehr hoch". Eine Risikomatrix (siehe Abbildung 3) eignet sich zur Darstellung

Auswirkungen	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

Abbildung 3: Beispiel einer Risikomatrix

der Ergebnisse. Sie zeigt in übersichtlicher Form die für die Wahrscheinlichkeiten und Auswirkungen von Risikoszenarien vorgenommenen Bewertungen und die daraus resultierenden Risikowerte.

Wie hoch ein Risiko eingestuft wird, hängt entscheidend von den zugrunde gelegten Bewertungskriterien ab. Da der Risikowert eine wichtige Kenngröße für die Risikobehandlung ist, müssen diese sorgfältig definiert sein, um Fehleinstufungen von Risiken zu vermeiden.

Erforderliche Kenntnisse

Bei der Zusammenstellung des Arbeitsteams für diese Aufgabe ist zu beachten, dass die Identifikation von Risikoszenarien, die Einschätzung von Wahrscheinlichkeiten und die Bewertung von Auswirkungen keine trivialen Aufgaben sind. Vielmehr ist umfangreiches und detailliertes Wissen nötig: IT-Kenntnisse erleichtern es beispielsweise, Bedrohungen und Schwachstellen zu identifizieren, mit Anwendungswissen können die möglichen Auswirkungen eines Risikoszenarios präziser bewertet werden. Das Team sollte entsprechend zusammengesetzt sein. Gegebenenfalls bietet es sich auch an, auf externe Erfahrungen (anderer Krankenhäuser, spezialisierter Beratungsunternehmen) zurückzugreifen.

Rolle der Krankenhausleitung

Da die ermittelten Risikowerte eine Entscheidungsgrundlage für die im Nachgang der IT-Risikoanalyse zu treffenden Maßnahmen zur Risikobehandlung sind, muss die Krankenhausleitung über die Ergebnisse und die ihnen zugrunde liegenden Bewertungskriterien unterrichtet werden.

Bezug zum übergeordneten Risikomanagement

Sofern in einem Krankenhaus ein übergeordnetes Risikomanagement etabliert ist und bereits Risikoanalysen zum Beispiel zur Gebäude- oder Versorgungssicherheit durchgeführt wurden, können die erzielten Ergebnisse auch für die IT-Risikoanalyse berücksichtigt werden. Gleiches gilt für die angewendeten Bewertungskriterien: Die Kriterien, die zum Beispiel zur Bewertung der Auswirkungen eines Risikoszenarios verwendet werden, sollten bei einer übergeordneten Risikoanalyse und der IT-Risikoanalyse zueinanderpassen.

In Kapitel 4 des Leitfadens „Risikoanalyse Krankenhaus-IT“ werden die Schritte dieses Aufgabenblocks und Hilfsmittel zur Durchführung detailliert beschrieben.

2.4 Risiken behandeln

Die Höhe der im letzten Schritt ermittelten Risikowerte ist ein Indikator für den Handlungsbedarf zur Absicherung der kritischen Krankenhausprozesse und ihrer IT-Unterstützung und gibt einen Hinweis darauf, ob ein Risiko **vermieden**, **reduziert**, **transferiert** oder **übernommen** werden sollte.

Sofern der Anwendungszweck dies zulässt, können mögliche Schäden durch Verzicht auf die risikobehaftete Situation **vermieden** werden, beispielsweise durch Außerbetriebnahme einer riskanten IT-Anwendung. Die **Reduktion von Risiken** empfiehlt sich, wenn der Anwendungszweck es nicht erlaubt, die Risiken zu vermeiden, aber die Wahrscheinlichkeit oder die Auswirkungen von IT-Ausfällen mit angemessenem Aufwand durch Sicherheitsmaßnahmen auf ein vertretbares Maß

abgesenkt werden können. Wenn ein Risiko nicht vermieden werden kann, eine Einrichtung aber gleichzeitig nicht in der Lage ist, mit eigenen Mitteln für hinreichende Sicherheit zu sorgen, kann dieses auf andere Institutionen **transferiert** werden, beispielsweise durch den Abschluss einer Versicherung oder Outsourcing. In beiden Fällen entbindet dies ein Krankenhaus jedoch nicht von der grundsätzlichen Verantwortung für die Verfügbarkeit seiner Prozesse. Ein Risikotransfer muss sich mit den Schutzzielen eines Krankenhauses vereinbaren lassen. Allenfalls bei einem sehr geringen Risikowert können Risiken **übernommen** werden, kann also auf Maßnahmen zur Absicherung der betrachteten IT-Komponente verzichtet werden.

Erforderliche Kenntnisse

Für die beschriebenen Aufgaben sind sowohl technisches Wissen als auch Prozesskenntnisse hilfreich. Das Wissen um die möglichen technischen Sicherheitsmaßnahmen erleichtert beispielsweise die Entscheidung, ob sich Risiken mit vertretbarem Aufwand signifikant reduzieren lassen, und hilft bei der Auswahl und Konkretisierung geeigneter Maßnahmen. Prozesswissen ist eine Voraussetzung dafür, dass die Entscheidungen zur Risikobehandlung und die ausgewählten Maßnahmen zur Absicherung der IT und der kritischen Krankenhausprozesse zu den Arbeitsabläufen des Krankenhauses passen.

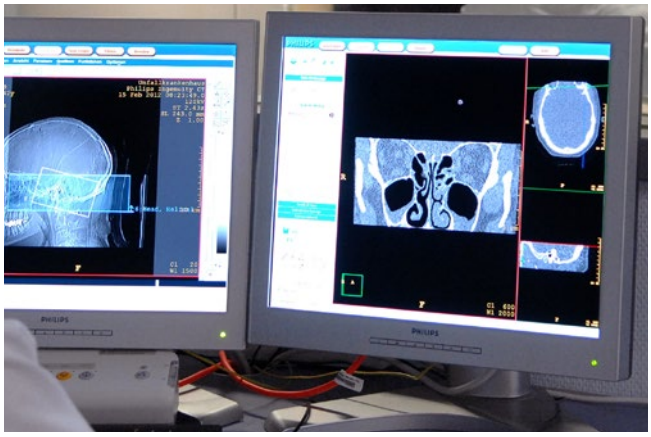
Rolle der Krankenhausleitung

Alle Entscheidungen zur Risikobehandlung müssen von der Krankenhausleitung verantwortet werden. Sie muss die Entscheidungen zur Übernahme und die Maßnahmen zur Vermeidung, Verlagerung und Reduzierung von Risiken unterstützen und gegebenenfalls hierfür erforderliche Ressourcen bewilligen.

Bezug zum übergeordneten Risikomanagement

Alle Entscheidungen zur Behandlung von Risiken sowie die aus diesen Entscheidungen resultierenden Maßnahmen sind Bestandteil des Gesamtsicherheitskonzepts eines Krankenhauses und daher mit einem gegebenenfalls vorhandenen übergeordneten Risikomanagement abzustimmen.

In Kapitel 5 des Leitfadens „Risikoanalyse Krankenhaus-IT“ werden die Schritte dieses Aufgabenblocks detailliert beschrieben.



2.5 Nutzen und Grenzen der IT-Risikoanalyse

Die im Rahmen der IT-Risikoanalyse erfolgte intensive Untersuchung der kritischen IT-Abhängigkeiten eines Krankenhauses erleichtert angemessene Entscheidungen zur Risikobehandlung. Sie unterstützt damit die zielgerichtete Auswahl von Maßnahmen, mit denen die Verfügbarkeit der kritischen Prozesse eines Krankenhauses gesichert werden kann.

Zu beachten ist, dass die IT-Risikoanalyse und die aufgrund ihrer Ergebnisse getroffenen Entscheidungen immer auf einer Momentaufnahme basieren. Umstrukturierungen und andere Veränderungen in einem Krankenhaus, aber auch äußere Faktoren, etwa eine geänderte Bedrohungslage, können die Ergebnisse einer durchgeführten IT-Risikoanalyse veralten lassen. Die Aktualität der IT-Risikoanalyse sollte daher in regelmäßigen Abständen, anlassbezogen auch außerplanmäßig, geprüft werden.

Eine IT-Risikoanalyse hat durch ihr spezifisches Anwendungsgebiet bedingte Grenzen und muss durch weitere Aktivitäten ergänzt werden. So ist Informationstechnik zwar eine wichtige, aber nicht die einzige kritische Ressource eines Krankenhauses. Für eine umfassende Sicherheit muss die IT-Risikoanalyse daher durch die Untersuchung der Kritikalität und der Ausfallrisiken weiterer Ressourcen ergänzt werden.

Sowohl für die IT-Risikoanalyse als auch für die weiteren Risikoanalysen gilt, dass ihre Ergebnisse in einen systematischen Prozess zur Behandlung der Risiken für die Krankenhausprozesse einzubinden sind und zu adäquaten Maßnahmen führen müssen. Für den Schutz der IT-Infrastruktur werden hierzu im folgenden Kapitel einige Handlungsfelder aufgezeigt.

3 IT-Sicherheit: Handlungsbedarf erkennen

3 IT-Sicherheit: Handlungsbedarf erkennen

Aufgrund seiner wichtigen Aufgaben für die Gesundheitsversorgung der Bevölkerung steht ein Krankenhaus, auch durch gesetzliche Regelungen, in der Pflicht, die Verfügbarkeit seiner Dienstleistungen zu gewährleisten. Angesichts der zunehmenden Abhängigkeit der Patientenversorgung von einer störungsfrei funktionierenden IT-Infrastruktur muss folglich auch der IT-Sicherheit ein hoher Stellenwert eingeräumt werden.

Die folgenden Fragen und zugehörigen Erläuterungen benennen Handlungsfelder, die für die Gewährleistung angemessener IT-Sicherheit besonders wichtig sind. Eine vollständige Abdeckung aller relevanten Themengebiete ist an dieser Stelle selbstverständlich nicht möglich. Die Auswahl soll Ihnen aber als Anreiz dienen, den Umsetzungsstand Ihrer Einrichtung zu prüfen, und aufzeigen, welchen Beitrag die IT-Risikoanalyse zur Absicherung der IT-Infrastruktur eines Krankenhauses leisten kann.

Sind die Prozesse Ihrer Einrichtung und deren IT-Abhängigkeiten bekannt?

Eine regelmäßig aktualisierte Prozessübersicht (z. B. als „Prozesslandkarte“) erleichtert es nicht nur, Effektivität und Effizienz der Abläufe eines Krankenhauses zu verbessern, sondern auch die kritischen Prozesse und IT-Abhängigkeiten zu erkennen. Sie ist damit eine wichtige Grundlage für die IT-Risikoanalyse. Hierfür sollte die Übersicht angemessen detailliert die Krankenhausprozesse, deren Zusammenwirken und deren IT-Unterstützung beschreiben.

Verfügen die IT-Zuständigen Ihrer Einrichtung über einen umfassenden Überblick über die IT-Infrastruktur und deren Komponenten?

Ein aktuelles und vollständiges Inventar der IT-Infrastruktur hilft bei der Ermittlung derjenigen IT-Komponenten, die für das korrekte Funktionieren der kritischen IT-Anwendungen unverzichtbar sind. Es erleichtert darüber hinaus die Entwicklung von Sicherheitskonzepten zum Schutz dieser Anwendungen. Das Inventar sollte sämtliche eingesetzten IT-Systeme (Server, Clients usw.) und alle für deren Betrieb wichtigen Angaben enthalten, beispielsweise Einsatzzweck, Softwareausstattung sowie die Art der Netzanbindung.

Sind die für Ihre Einrichtung unverzichtbaren (kritischen) Bestandteile der IT-Infrastruktur bekannt?

Die Kenntnis der unverzichtbaren IT-Anwendungen und IT-Komponenten ist eine Grundvoraussetzung für den Schutz vor IT-Ausfällen, welche die Handlungsfähigkeit Ihrer Einrichtung gefährden, und unterstützt die Auswahl angemessener Sicherheitsmaßnahmen. Die IT-Risikoanalyse ist ein Instrument, um die bestehenden Kenntnisse durch ein strukturiertes Vorgehen systematisch und möglichst vollständig zu erweitern.

Gibt es in Ihrer Einrichtung eine ausgewiesene Zuständigkeit für IT-Sicherheit?

Für die organisatorische Verankerung der IT-Sicherheit in Ihrer Einrichtung ist es hilfreich, wenn in Person eines IT-Sicherheitsbeauftragten eine zentrale Zuständigkeit für die Koordination der zugehörigen Aufgaben festgelegt wird. Ein IT-Sicherheitsbeauftragter ist der Krankenhausleitung berichtspflichtig und sollte eng mit allen Stellen zusammenarbeiten, die mit Sicherheitsfragen der Einrichtung befasst sind. Ihm obliegt es vor allem, die Entwicklung von Sicherheitskonzepten zu steuern und die Umsetzung der darin vorgesehenen Maßnahmen zu kontrollieren.

Werden in Ihrer Einrichtung ausreichende finanzielle und personelle Ressourcen für den IT-Betrieb und dessen Absicherung bereitgestellt?

Informationstechnik trägt auf vielfältige Weise zur Leistungsfähigkeit des Krankenhauses bei. Gerade dadurch ist sie aber auch zu einer kritischen Ressource für die Prozesse eines Krankenhauses geworden, deren Funktionsfähigkeit nur durch ausreichende Ressourcen für den IT-Betrieb und dessen Absicherung zuverlässig gewährleistet werden kann. Die IT-Risikoanalyse kann dazu beitragen, diejenigen Bestandteile der IT-Infrastruktur zu identifizieren, auf denen in dieser Hinsicht ein besonderes Augenmerk liegen sollte.

Sind die IT-Netze Ihrer Einrichtung hinreichend abgesichert?

Selbst der geplant durchgeführte Anschluss von Krankenhausnetzen an öffentliche Netze wie das Internet kann mit hohen Risiken verbunden sein und erfordert eine sorgfältige Absicherung z. B. durch ein zentrales Sicherheitsgateway, an dem der ein- und ausgehende Datenverkehr geprüft und bei Bedarf abgeblockt werden kann. Es ist aber auch sicherzustellen, dass zentrale Schutzmaßnahmen nicht durch unkontrollierte Netzzugänge, z. B. via WLAN oder mobile Datenverbindungen, ausgehebelt werden können. Auch die ausreichende Absicherung öffentlich zugänglicher Netzanschlüsse, z. B. in Patientenzimmern, ist in einer Einrichtung mit Publikumsverkehr von wichtiger Bedeutung. Die IT-Risikoanalyse kann helfen, solche Segmente des Krankenhausnetzes zu identifizieren, die in besonderer Weise abzusichern sind, und Schwachstellen in den vorhandenen Schutzvorkehrungen zu erkennen.

Unterliegen die IT-Systeme Ihrer IT-Infrastruktur einem systematischen Update- und Patchmanagement?

Die IT-Zuständigen müssen nahezu täglich damit rechnen, dass neue Schwachstellen in der eingesetzten Betriebssystem- und Anwendungssoftware bekannt werden. Um zu verhindern, dass eine Schwachstelle für Angriffe auf das Krankenhausnetz ausgenutzt wird, müssen die für den IT-Betrieb zuständigen Mitarbeiter sich regelmäßig über solche Sicherheitslücken informieren und von den Herstellern bereitgestellte Patches und Updates zeitnah auf die betroffenen IT-Systeme aufspielen. Dies gilt speziell für die als kritisch identifizierten IT-Komponenten. Ein Konzept für diese Aufgabe muss auch geeignete Regelungen für die Behandlung medizinischer Spezialanwendungen vorsehen.

Sind die IT-Systeme und IT-Anwendungen Ihrer Einrichtung hinreichend gegen unberechtigte Zugriffe geschützt?

In Krankenhausnetzen werden hochgradig sensible Daten verarbeitet und kritische IT-Anwendungen betrieben. Dies erfordert starke Mechanismen zum Zugangs- und Zugriffsschutz. Vor allem bei den als kritisch identifizierten IT-Anwendungen und IT-Komponenten müssen unautorisierte Zugriffe verhindert werden. Dabei ist darauf zu achten, dass durch zu restriktive Regelungen zum Zugriffsschutz die Verfügbarkeit von Daten und Anwendungen, die für die Patientenversorgung unverzichtbar sind, nicht gefährdet wird.

Sind die Mitarbeiter Ihrer Einrichtung für den sicheren Umgang mit kritischer Informationstechnik geschult?

Zur Vermeidung von IT-Sicherheitsvorfällen ist es erforderlich, dass die Benutzer hinreichend für Risiken bei der Anwendung von IT sensibilisiert und im sicheren Umgang mit dieser Technik geschult sind. Auch Administratoren und andere mit dem IT-Betrieb betraute Mitarbeiter müssen ausreichende Fortbildungsmöglichkeiten erhalten. Die IT-Risikoanalyse kann dazu beitragen, die Sensibilität für IT-Sicherheit in einem Krankenhaus zu erhöhen.

Liegen Notfallkonzepte für die kritischen IT-Anwendungen Ihrer Einrichtung vor?

Die IT-Risikoanalyse zeigt auf, welche IT-Anwendungen für die kritischen Prozesse eines Krankenhauses besonders wichtig sind. Trotz aller Sicherheitsmaßnahmen können IT-Ausfälle niemals völlig ausgeschlossen werden. Daher sind für alle kritischen IT-Anwendungen Notfallkonzepte zu entwickeln, in denen Ersatzmaßnahmen zur Überbrückung eines IT-Ausfalls und Maßnahmen für den Wiederanlauf der IT-Anwendungen beschrieben sind. Diese IT-Notfallkonzepte sind in ein Gesamtnotfallkonzept des Krankenhauses zu integrieren, in dem das Vorgehen bei Ausfällen weiterer kritischer Ressourcen beschrieben ist.

Beteiligt sich Ihre Einrichtung an Initiativen oder Kooperationen zur IT-Sicherheit?

Die vielfältigen Bedrohungen für die IT-Infrastruktur machen es nahezu unerlässlich, Erfahrungen im Umgang mit Risiken und zu Themen der IT-Sicherheit einrichtungs- und ggf. sogar branchenübergreifend auszutauschen. Auf diese Weise können alle Teilnehmer des Austausches von dem kollektiven Wissen um Problemfelder und Lösungsansätze profitieren. Neben brancheninternen Kreisen bieten sich hierzu verschiedene staatliche Initiativen an, beispielsweise die Allianz für Cyber-Sicherheit (www.allianz-fuer-cybersicherheit.de). Diese bietet nicht nur die Möglichkeit zum Erfahrungsaustausch, sondern auch dokumentierte Empfehlungen zur Cyber-Sicherheit sowie Informationen zu aktuellen Gefährdungen im Rahmen der Risikokommunikation an.

4 Weitere Informationen

4 Weitere Informationen

Literaturverzeichnis

[LF-RiKrIT]
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *Schutz Kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT. Leitfaden, 2013.*
http://www.kritis.bund.de
Der Leitfaden bietet eine ausführliche Darstellung der in dieser Broschüre dargestellten Vorgehensweise zur Risikoanalyse der IT-Infrastruktur eines Krankenhauses. Die einzelnen Schritte werden detailliert und mit Beispielen beschrieben. Im Anhang und in ergänzenden Publikationen werden zusätzliche Hilfsmittel zur Durchführung bereitgestellt.

[LF-BMI]
Bundesministerium des Innern (Hrsg.): *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement. Ein Leitfaden für Unternehmen und Behörden, 2008.*
http://www.kritis.bund.de
Dieser Leitfaden stellt ein Managementkonzept vor, das Betreiber Kritischer Infrastrukturen (Unternehmen und Behörden) bei der strukturierten Ermittlung von Risiken, der darauf basierenden Umsetzung vorbeugender Maßnahmen sowie dem effektiven und effizienten Umgang mit Krisen unterstützt.

[LF-BBK]
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (Hrsg.): *Schutz Kritischer Infrastruktur: Risikomanagement im Krankenhaus, 2009.*
http://www.kritis.bund.de
Dieser Leitfaden zur Identifikation und Reduzierung von Ausfallrisiken in Kritischen Infrastrukturen des Gesundheitswesens richtet sich an die Träger größerer Einrichtungen des Gesundheitswesens, insbesondere Krankenhäuser, und an Gesellschaften, die mehrere Krankenhäuser, Pflegeheime und verwandte Einrichtungen betreiben. Er konkretisiert den Leitfaden für Unternehmen und Behörden [LF-BMI] auf das besondere Anwendungsgebiet „Große Einrichtungen des Gesundheitswesens".

[KRITIS-Strategie]
Bundesministerium des Innern (Hrsg.): *Nationale Strategie zum Schutz Kritischer Infrastrukturen, 2009.*
http://www.bmi.bund.de/SharedDocs/Downloads/DE/Broschueren/2009/kritis.pdf
Dieses Dokument beschreibt die Zielvorstellungen und den politisch-strategischen Ansatz des Bundes zum Schutz Kritischer Infrastrukturen.

[IT-Grundschutz]
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *BSI-Standard 100-1: Managementsysteme für Informationssicherheit, Version 1.5, 2008.*
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, Version 2.0, 2008.*
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *BSI-Standard 100-3: Risikoanalyse auf Basis von IT-Grundschutz, Version 2.5, 2008.*
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *BSI-Standard 100-4: Notfallmanagement, Version 1.0, 2008.*
Bundesamt für Sicherheit in der Informationstechnik (Hrsg.): *IT-Grundschutz-Kataloge, fortlaufend aktualisiert.*
https://www.bsi.bund.de/grundschutz
Die BSI-Standards beschreiben Anforderungen an ein Managementsystem für Informationssicherheit (BSI-Standard 100-1), die Umsetzung dieser Anforderungen in Gestalt der IT-Grundschutz-Vorgehensweise (BSI-Standard 100-2), eine dazu passende Risikoanalyse-Methode (BSI-Standard 100-3) sowie Aufbau und Betrieb eines Notfallmanagements (BSI-Standard 100-4). Die IT-Grundschutz-Kataloge enthalten thematisch strukturierte Bausteine mit Verweisen auf typische Gefährdungen und Standardsicherheitsmaßnahmen, mit denen diesen Gefährdungen begegnet werden kann.

Endnoten

1. [KRITIS-Strategie], Seite 3
2. Tagesspiegel vom 18.09.2006, http://www.tagesspiegel.de/weltspiegel/ueberschwemmungen-chaos-in-mittelhessen/753824.html
3. Hamburger Abendblatt vom 02.02.2008, http://www.abendblatt.de/hamburg/article516596/Stromausfall-im-Krankenhaus-Boberg-Patienten-in-Gefahr.html
4. http://www.gulli.com/news/5922-san-diego-63-monate-haft-fuer-boeswilligen-hack-aus-rache-2008-06-14
5. T-Online, http://computer.t-online.de/computervirus-legt-krankenhaus-lahm/id_52376022/
6. Heise Online, http://heise.de/-217489
7. Heise Online, http://heise.de/-196929
8. Heise Online, http://heise.de/-1122484
9. PC Welt, http://www.pcwelt.de/news/Oranje-infiziert-Verschluesselungswurm-Dorifel-geht-um-6464564.html
10. MIT Technology Review, http://www.technologyreview.com/news/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/

Glossar

Begriff	Beschreibung
Bedrohung	Umstand oder Ereignis, durch den oder das ein Schaden an einer kritischen IT-Komponente und eine Beeinträchtigung der Verfügbarkeit entstehen können.
Eintrittswahrscheinlichkeit	Wert, der die Wahrscheinlichkeit des Eintretens eines Risikoszenarios beschreibt.
Gefährdung	Bedrohung, die konkret über eine Schwachstelle auf ein Zielobjekt einwirken kann.
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-Komponente	Technische Komponente (Hardware, Software, Kommunikationsverbindung), die für den Betrieb einer IT-Anwendung erforderlich ist.
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 [KRITIS Strategie].
Prozess	Summe der Tätigkeiten und Bearbeitungsschritte in einem Krankenhaus zur Erbringung einer Dienstleistung.
Risiko	Produkt aus der Eintrittswahrscheinlichkeit und der Auswirkung eines Schadens.
Risikoanalyse	Systematisches Verfahren zur Identifikation und Bewertung von Risiken.
Risikomanagement	Prozess bzw. Verfahren zum planvollen Umgang mit Risiken.
Risikomatrix	Hilfsmittel zur grafischen Darstellung von Risikowerten.
Risikowert	Maß zur Bewertung eines Risikos aufgrund von Einschätzungen zur Eintrittswahrscheinlichkeit und den Auswirkungen eines Schadensereignisses.
Risikoszenario	Sinnvolle Kombination einer Bedrohung mit einer hierzu passenden Schwachstelle (synonym zu „Gefährdung“).
Schutzziel, übergeordnet	Beschreibung eines herbeizuführenden Sollzustandes bezüglich zu schützender Bereiche (Prozesse) eines Krankenhauses.
Schutzziel, Informationstechnik	Konkretisierung der übergeordneten Schutzziele für den Bereich der Informationstechnik mithilfe der Grundwerte Verfügbarkeit, Integrität und Vertraulichkeit.
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.

Impressum

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189
53175 Bonn
bsi@bsi.bund.de
Internet: www.bsi.bund.de
Telefon: +49 (0) 22899 9582 - 0
Telefax: +49 (0) 22899 9582 - 5400

Stand
März 2013

Druck
Druckpartner Moser Druck + Verlag GmbH
53359 Rheinbach

Texte und Redaktion
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bildnachweis
Dorothea Scheurlen DGPh, ukb: Titel, S.4, S.8, S.14, S.16

Diese Broschüre ist Teil der Öffentlichkeitsarbeit des BSI; sie wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt.

www.bsi.bund.de