HOCHSCHULE MITTWEIDA
UNIVERSITY OF APPLIED SCIENCES

MASTERARBEIT

Herr B.Sc.
Lukas Riedt

Risikoanalyse der Cybersicherheit kleiner und mittlerer Unternehmen (KMU) mit vergleichender Konzeptionierung und Evaluierung am Beispiel einer Zahnarztpraxis

Mittweida, 2024

Fakultät Angewandte Computer- und
Biowissenschaften

MASTERARBEIT

Risikoanalyse der Cybersicherheit kleiner und mittlerer Unternehmen (KMU) mit vergleichender Konzeptionierung und Evaluierung am Beispiel einer Zahnarztpraxis

Autor:
Herr B.Sc.

Lukas Riedt

Studiengang:
Cybercrime/Cybersecurity

Seminargruppe:
CY22wC-M

Erstprüfer:
Prof. Dr. rer. pol. Ronny Bodach

Zweitprüfer:
Stefan Schildbach, M.Sc.

Einreichung:
Mittweida, 11.10.2024

Verteidigung/Bewertung:
Mittweida, 2024

Faculty Angewandte Computer- und Biowissenschaften

MASTER THESIS

Risk analysis of the cyber security of small and medium-sized enterprises (SMEs) with comparative conceptualization and evaluation using the example of a dental surgery

author:
Mr. B.Sc.

Lukas Riedt

course of studies:
Cybercrime/Cybersecurity

seminar group:
CY22wC-M

first examiner:
Prof. Dr. rer. pol. Ronny Bodach

second examiner:
Stefan Schildbach, M.Sc.

submission:
Mittweida, 11.10.2024

defence/evaluation:
Mittweida, 2024

Bibliografische Beschreibung:

Riedt, Lukas:
Risikoanalyse der Cybersicherheit kleiner und mittlerer Unternehmen (KMU) mit vergleichender Konzeptionierung und Evaluierung am Beispiel einer Zahnarztpraxis. - 2024. - 10 S. Verzeichnisse, 126 S. Inhalt, 435 S. Anhänge

Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Masterarbeit, 2024

Referat:

In der von der Digitalisierung mehr und mehr durchdrungenen Welt hat der Umgang mit elektronischen Daten und der Schutz dieser Daten immer größere Bedeutung für Unternehmen. Dies trifft auch auf kleine und mittlere Unternehmen (KMU) zu. Die vorliegende Masterarbeit stellt die Risikoanalysestandards des IT-Grundschutzes, OCTAVE-S, den B3S „Medizinische Versorgung“, die ISO/IEC-Norm 27005 und die Threat-Modeling-Konzepte STRIDE und DREAD vor und vergleicht sie. Dies geschieht im Hinblick auf KMU. Zur Evaluation werden die Standards und Konzepte auf eine Zahnarztpraxis angewendet.

Hinweis:

In der vorliegenden Arbeit wird in der Regel darauf verzichtet, bei Personenbezeichnungen sowohl die männliche als auch die weibliche Form zu nennen. Die männliche Form gilt in allen Fällen, in denen dies nicht explizit ausgeschlossen wird, für beide Geschlechter.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Formelverzeichnis

Abkürzungsverzeichnis

AktG	Aktiengesetz
B3S	Branchenspezifischer Sicherheitsstandard
BCM	Business-Continuity-Management
BCMS	Business-Continuity-Managementsystem
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	BSI-Kritisverordnung
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
CVSS	Common Vulnerability Scoring System
DIN	Deutsches Institut für Normung
dLS	durchschnittliche Länge der Sätze
DNS	Domain Name System
DoS	Denial-of-Service
DREAD	Damage, Reproducibility, Exploitability, Affected users, Discoverability
DSGVO	Datenschutz-Grundverordnung
dSW	durchschnittliche Silbenzahl der Worte
E-Rezept	Elektronisches Rezept
EN	Europäische Norm
ePA	Elektronische Patientenakte
EU	Europäische Union
FRE	Flesch-Reading-Ease
GmbH	Gesellschaft mit beschränkter Haftung
HGB	Handelsgesetzbuch
IEC	International Electrotechnical Commission
ISB	Informationssicherheitsbeauftragter
ISDN	Integrated Services Digital Network
ISMS	Informationssicherheitsmanagementsystem
ISO	Internationale Organisation für Normung
IT	Informationstechnik
KIM	Kommunikation im Medizinwesen
KKU	kleine und Kleinstunternehmen

KMU	Kleine und mittlere Unternehmen
KonTraG	Gesetz zur Kontrolle und Transparenz im Unternehmensbereich
KRITIS	Kritische Infrastrukturen
KZBV	Kassenzahnärztliche Bundesvereinigung
NAS	Network Attached Storage
NIS-2-Richtlinie	zweite Richtlinie zur Netzwerk- und Informationssicherheit
NIS2UmsuCG	NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz
NIST	National Institute of Standards and Technology der USA
OCTAVE®	Operationally, Critial Threat, Asset and Vulnerability Evaluation
PDCA	Plan, Do, Check, Act
SGB	Sozialgesetzbuch
SIS	Sicherer Internet Service
SMB	Server-Message-Block-Protokoll
SME	Small and medium-sized enterprise
StaRUG	Gesetz über den Stabilisierungs- und Restrukturierungsrahmen für Unternehmen
STRIDE	Spoofing identity, tampering, Repudiation, Information Disclosure, Denial-of-Service, Elevation of Privilege
TI	Telematikinfrastruktur
VoIP	Voice-over-Internet-Protocol
VPN	Virtual private network
WLAN	Wireless Local Area Network

1 Einleitung

Die Bedeutung von Informationstechnik und der elektronischen Verarbeitung von Informationen haben in den letzten Jahrzehnten stark zugenommen. Diese Entwicklung ist nicht nur im privaten Bereich zu beobachten, sondern vor allem auch bei Unternehmen und öffentlichen Einrichtungen. Den Vorteilen dieses Fortschritts stehen aber auch Risiken gegenüber. Aufgrund der zunehmenden Vernetzung und Abhängigkeit von Informationstechnik stellen Cyber-Angriffe eine immer größer werdende Bedrohung für Unternehmen dar. So können beispielsweise Ausfälle der IT-Systeme ein gesamtes Unternehmen lahmlegen oder der Verlust von sensiblen Daten erhebliche Konsequenzen haben. Nach Angaben des vom Branchenverband Bitkom e.V. veröffentlichten Wirtschaftsschutzberichts 2023 entstehen mit 148,2 Milliarden Euro 72 Prozent der Schäden bei Unternehmen durch Cyber-Angriffe. 52 Prozent der befragten Unternehmen gaben an, dass sie sich durch Cyber-Angriffe in ihrer Existenz bedroht fühlen. Die am häufigsten auftretenden Arten von Cyber-Angriffen sind laut der im Jahr 2023 erfolgten Digitalisierungsumfrage der Deutschen Industrie- und Handelskammer die Spionage mit 31 Prozent und Ransomware mit 26 Prozent. [1] [2, S. 9]

Diese Gefahren erhöhen den Bedarf an Vorkehrungen zur Absicherung der eingesetzten Informationstechnik und deren Kommunikation untereinander. Damit eine Organisation umfassende und zielgerichtete Maßnahmen zur Absicherung sensibler Daten und der Einhaltung von Vorgaben treffen kann, wurden eine Reihe von Standards entwickelt. Dazu gehören unter anderem der IT-Grundschutz des BSI, die ISO/IEC-Normen der Reihe 27000 und die Standards der OCTAVE®-Reihe, welche sich mit Risikoanalyse im Bereich der Informationssicherheit beschäftigen. Die Risikoanalyse behandelt den Prozess zum Identifizieren, Einschätzen, Bewerten und Behandeln von Risiken [3, S. 6f.]. Eingebunden ist sie häufig in ein Managementsystem, das dem Vorgehen einen strukturierten Rahmen gibt, der für die langfristige Planung und Steuerung der Sicherheitsaktivitäten zuständig ist [4].

Eine besondere Herausforderung stellt die Cyber-Sicherheit für kleine und mittlere Unternehmen (KMU) dar. Aufgrund ihrer begrenzten Ressourcen und dem Fehlen von IT-Personal sind Sicherheitsmaßnahmen in diesen oftmals nicht ausreichend umgesetzt. Mit 99,3 Prozent machen KMU die deutliche Mehrheit aller Unternehmen in Deutschland aus [5]. Dies ist auch ein Grund, weshalb KMU zu den Organisationstypen gehören, die überproportional häufig Opfer von Cyber-Angriffen werden [6]. Im Praxisreport „Mittelstand@IT-Sicherheit“ des Vereins „Deutschland sicher im Netz e.V.“ aus dem Jahr 2022 wurden Unternehmen in Hinblick auf ihre IT-Sicherheit befragt, die überwiegend den KMU zuzuordnen sind. Von diesen gaben lediglich 20 Prozent an, dass sie Schutzmaßnahmen mit Standards wie dem IT-Grundschutz oder der ISO 27001 identifizieren und bewerten. 13 Prozent der Befragten beauftragen externe Dienstleister. Mit 53 Prozent entwickelt der Großteil eigene

Maßnahmen. Die verbleibenden 14 Prozent ergreifen keine Maßnahmen, um Risiken zu begegnen. [7, S. 24]

Auch im Gesundheitswesen schreitet die Digitalisierung immer weiter voran. Mit der Telematikinfrastruktur (TI) werden viele Gesundheitsanwendungen in den digitalen Raum verschoben. Hier können die elektronische Patientenakte (ePA) oder elektronische Rezept (E-Rezept) genannt werden. Gerade im Gesundheitswesen können jedoch ein fehlender Schutz von sensiblen Daten oder Ausfälle der Versorgung weitreichende Folgen haben, weshalb die Sicherheit in diesem Bereich eine zentrale Rolle spielt. [8]

Verdeutlicht wird dies auch durch Angriffe auf Krankenhäuser, über welche immer wieder in den Medien berichtet wird. So informiert der Westdeutsche Rundfunk über einen Cyber-Angriff auf Krankenhäuser im Kreis Soest. In Folge dieses Angriffs mussten Operationen verschoben und neue Patienten konnten nicht aufgenommen werden. Oftmals werden medizinische Einrichtungen mit Ransomware angegriffen. Bei diesen haben die Täter das Ziel, Lösegeld zu erpressen. Folgen dieser Angriffe können Ausfälle der IT-Systeme, ein fehlender Zugriff auf Patientendaten und Medizingeräte sein. Dies kann zu Einschränkungen der medizinischen Versorgung bis hin zu lebensbedrohlichen Folgen führen. Um die IT-Sicherheit von Krankenhäusern der Kritischen Infrastruktur zu stärken, wurde der branchenspezifische Sicherheitsstandard (B3S) „Medizinische Versorgung“ entwickelt [9, S. 6]. [10] [11]

Nicht nur in der stationären Versorgung von Patienten, sondern auch in Arzt- und Zahnarztpraxen nehmen IT-Sicherheitsfragen eine immer größer werdende Rolle ein. Aus diesem Grund gibt es seit dem Jahr 2020 eine IT-Sicherheitsrichtline für Arzt- und Zahnarztpraxen. Mit dieser Richtlinie hat sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) in der Studie „SiRiPrax“ beschäftigt. Zu den Erkenntnissen der Studie gehört, dass die Richtlinie lediglich 58 Prozent der Befragten bekannt ist und nur ein Drittel der Praxen angibt, die Richtlinie vollständig umzusetzen. Gründe, die dafür angegeben werden, ist ein fehlendes Problembewusstsein sowie fehlendes Budget, Personal und fehlende Zeit. Auch die bisherige Betroffenheit von Cyber-Angriffen bei Praxen wurde abgefragt. Mit etwa zehn Prozent, die bereits mindestens einen Vorfall erlebt haben, ist die Betroffenheit relativ gering. [12] [8]

Eine weitere Studie des BSI aus diesem Themengebiet mit dem Titel „Cybersicherheit in Arztpraxen“ evaluiert das Sicherheitsniveau von 16 Arzt- und Zahnarztpraxen und bestimmt Schwachstellen, die in Praxen häufig vorhanden sind. Die Untersuchung, zeigt, dass keine der Praxen ein ISMS aufweist. Auch der Schutz vor Schadsoftware und das Einspielen von Updates werden in vielen Praxen vernachlässigt. Allgemein konnten in der Studie eine Vielzahl von Schwachstellen in den untersuchten Praxen festgestellt werden. [13]

Ziel dieser Arbeit ist es, verschiedene Konzepte zur Risikoanalyse der Cybersicherheit zu analysieren und miteinander zu vergleichen. Dabei soll die Perspektive von KMU eingenommen und die Eignung und Praktikabilität der Standards für diese bewertet werden. Zur praktischen Untersuchung sollen die Standards an einer Zahnarztpraxis angewendet werden.

In den folgenden Kapitel werden zunächst Grundlagen rund um die Begriffe der Risikoanalyse und Informationssicherheit thematisiert. Anschließend wird erklärt, was „kleine und mittlere Unternehmen“ genau sind. Danach werden rechtliche Grundlagen erläutert, die zur Einführung von IT-Sicherheitsmaßnahmen verpflichten. Darauf folgt die Vorstellung von vier Standards, die sich mit der Risikoanalyse beschäftigen. Dabei handelt es sich um den IT-Grundschutz des BSI, den branchenspezifischen Sicherheitsstandards „Medizinische Versorgung“, OCTAVE®-S und die ISO/IEC-Norm 27005. Ergänzt werden diese von den Threat-Modeling-Konzepten STRIDE und DREAD.

Das dritte Kapitel befasst sich mit dem Vergleich der Standards und Konzepte. Hier wird zunächst die KMU-Tauglichkeit der Standards anhand einer von Mark Le Corre entwickelten Methode überprüft. Im Anschluss erfolgt ein Vergleich der einzelnen Phasen der Risikoanalysestandards.

Im vierten Kapitel werden die Standards am Beispiel einer Zahnarztpraxis evaluiert. Dazu wird der IT-Grundschutz mit seiner Risikoanalyse und der OCTAVE-S-Standard am Praxisbeispiel bearbeitet. Darüber hinaus werden spezielle Aspekte des B3S „Medizinische Versorgung“ und der ISO/IEC-Norm 27005 in Bezug auf die Zahnarztpraxis betrachtet sowie STRIDE und DREAD angewendet.

Abschließend werden die Ergebnisse diskutiert und zusammengefasst.

2 Grundlagen

In diesem Kapitel werden grundlegende Begriffe erklärt, rechtliche Verpflichtungen zum Ergreifen von IT-Sicherheitsmaßnahmen dargelegt und die bereits erwähnten Risikoanalysestandards vorgestellt.

2.1 Begriffserklärungen

Zunächst wird der Begriff der Informationssicherheit erklärt und anschließend mit der IT-Sicherheit und der Cybersicherheit verglichen. Danach wird der Begriff „Risiko“ definiert und die unterschiedliche Bedeutung der Risikoanalyse im Deutschen und im Englischen aufgezeigt. Abschließend werden die deutsche und die europäische Definition kleiner und mittlerer Unternehmen beleuchtet.

2.1.1 Informationssicherheit, IT-Sicherheit und Cybersicherheit

Die Informationssicherheit beschäftigt sich mit dem Schutz von Informationen. Dabei ist es unerheblich, ob die Information auf einem IT-System gespeichert ist oder nicht. Die Verfügbarkeit, Integrität und Vertraulichkeit sind elementare Schutzziele, die hier sichergestellt werden sollen. Die Verfügbarkeit ist gegeben, wenn die Berechtigten auf die Information oder das System in definierter Form und Zeit zugreifen können. Mit der Wahrung Integrität soll verhindert werden, dass die Information manipuliert wird. Dieses Schutzziel beschreibt also die Richtigkeit und Vollständigkeit der Information [14]. Die Vertraulichkeit ist gewahrt, wenn nur Berechtigte auf die Information zugreifen. Für Andere darf die Information nicht zugänglich sein. Darüber hinaus können weitere Schutzziele wie Authentizität und Nichtabstreitbarkeit relevant sein. [15, S. 159ff.]

Zum strukturierten Vorgehen in Fragen der Informationssicherheit wird in der Regel ein Informationssicherheitsmanagementsystem (ISMS) aufgebaut. Dieses regelt, wie Prozesse und Bemühungen in Bezug auf die Informationssicherheit geplant und gesteuert werden. Ein solches Managementsystem umfasst die Planung, den Betrieb, die Überwachung sowie Prozesse zur Aufrechterhaltung und Verbesserung der Informationssicherheit. Angelehnt ist der Managementprozess an den PDCA-Zyklus nach Deming. Dieser steht für „Plan“, „Do“, „Check“ und „Act“ und beschreibt einen allgemeinen Prozess, mit dem eine kontinuierliche Verbesserung erlangt werden soll. Nach der letzten Phase, dem „Act“, wird erneut mit der ersten Phase begonnen, wodurch ein Kreislauf entsteht. Weitere Details zu Informationssicherheitsmanagementsystemen werden in Kapitel 2.3.1 anhand des IT-Grundschutzes des BSI vorgestellt. [14] [16]

Unter dem Begriff „Asset“ werden die zu schützenden Objekte zusammengefasst. Übersetzen kann man diesen mit „Wert“. Im Deutschen werden auch häufig die Begriffe Risikoobjekt oder Schutzobjekt verwendet. Assets sind Objekte, die für die Organisation einen Wert haben. Neben den oben erwähnten Informationen können das auch IT-Systeme, Anwendungen oder Geschäftsprozesse sein. Genauso wie für Informationen, ist es auch für andere Assets das Ziel, die Schutzziele zu erfüllen. [17] [14]

Während sich die Informationssicherheit mit dem Schutz von Informationen beschäftigt, unabhängig davon, wo und wie sie gespeichert sind, beschränkt sich die IT-Sicherheit auf den Schutz von elektronisch gespeicherten Informationen und der Informationstechnik, auf der diese gespeichert sind. Somit kann die IT-Sicherheit als Teilgebiet der Informationssicherheit angesehen werden. [18]

Die Cybersicherheit bezieht sich wiederum auf den Cyber-Raum und Gefahren, die aus diesem hervorgehen. Der Cyber-Raum beinhaltet das Internet und andere Netze sowie die daran angeschlossenen IT-Systeme und deren Kommunikation, Anwendungen und Informationen. [4]

2.1.2 Begriffe Risiko, Risikoanalyse und Risikomanagement

Die DIN EN ISO/IEC 27000 definiert Risiko als „Auswirkung von Ungewissheit auf Ziele“ [19, S. 16]. Dies beinhaltet sowohl negative als auch positive Abweichungen von einem erwarteten Ergebnis. Im Bereich der Informationssicherheit hat sich ein engerer Risikobegriff etabliert, der sich auf die negativen Folgen konzentriert. Bei „Zielen“ handelt es sich im Kontext der Informationssicherheit um die im vorherigen Kapitel erwähnten Schutzziele. Bewertet wird ein Risiko hier nach seiner Eintrittswahrscheinlichkeit und der Höhe des zu erwartenden Schadens. [15, S. 11ff.]

Ausschlaggebend für ein Risiko ist das Vorliegen einer Bedrohung. Das ist eine schadhafte Ursache für ein unerwünschtes Ereignis. Eine Bedrohung kann eine Schwachstelle eines Risikoobjektes ausnutzen, um einen Schaden herbeizuführen. Aus Bedrohungen und Schwachstellen ergibt sich die Eintrittswahrscheinlichkeit eines Risikos. Mit Maßnahmen sollen die Eintrittswahrscheinlichkeit und die Schadenshöhe reduziert und somit dem Risiko begegnet werden. [15, S. 13ff.]

Das BSI nennt das konkrete Einwirken auf eine Schwachstelle eines Risikoobjektes durch eine Bedrohung Gefährdung. Ein Beispiel für eine Bedrohung könnte ein Schadprogramm sein. Wenn dies auf ein IT-System mit fehlendem Virenschutz trifft, ist eine Schwachstelle gegeben und es liegt eine Gefährdung vor. [4]

Bei einer Risikoquelle handelt es um die Ursache des Risikos. Diese kann von menschlicher, umweltbedingter oder technischer Natur sein. [20, S. 10]

Im Rahmen des Risikomanagements werden Handlungen einer Organisation in Bezug auf Risiken gesteuert. Nach der ISO/IEC-Norm 27000 umfasst dies die Identifizierung, Analyse, Bewertung und Behandlung von Risiken sowie Handlungen zur Kontextfestlegung, Überwachung, Überprüfung und Kommunikation von Risiken. [19, S. 18]

Abhängig vom betrachteten Standard unterscheidet sich die Bedeutung des Begriffes der Risikoanalyse. Nachfolgend sind dafür beispielhaft die unterschiedlichen Verwendungen des Begriffes in den Standards des BSI und in der ISO/IEC-Norm 27005 dargestellt.

Die Risikoanalyse nach IT-Grundschutz des BSI umfasst das Identifizieren, Einschätzen, Bewerten und Behandeln von Risiken. Der Begriff der Risikoanalyse wird hier für den vierstufigen Prozess verwendet, da er sich im Deutschen dafür etabliert hat. Im Gegensatz dazu umfasst die Risikoanalyse der ISO/IEC-Norm 27005 und englischsprachiger Literatur nur einen Prozessschritt. Dieser entspricht der Einschätzung von Risiken und zum Teil der Risikobewertung des BSI-Standards. In Tabelle 1 sind die Prozessschritte des BSI-Standards und der ISO/IEC-Norm im Vergleich dargestellt. [3, S. 51f.]

Tabelle 1: Vergleich der Begriffe „Risikoanalyse“ aus IT-Grundschutz des BSI und der ISO/IEC 27005 (Tabelle nach [3, S. 51f.] und [20])

<table>
<tr><th>Risikoanalyse nach IT-Grundschutz</th><th>ISO/IEC 27005 „Risikomanagement“</th></tr>
<tr><td>Gefährdungsübersicht</td><td>Identifizieren von Risiken</td></tr>
<tr><td>Einschätzen von Risiken</td><td rowspan="2">Analyse von Risiken</td></tr>
<tr><td rowspan="2">Bewerten von Risiken</td></tr>
<tr><td rowspan="2">Bewerten von Risiken</td></tr>
<tr><td rowspan="2">Behandeln von Risiken</td></tr>
<tr><td>Behandeln von Risiken</td></tr>
</table>

In dieser Arbeit wird im Allgemeinen der Risikoanalysebegriff des BSI verwendet. Wenn sich eine Aussage konkret auf einen Standard bezieht, wird der Sprachgebrauch dieses Standard genutzt.

2.1.3 Definition KMU

Die Abkürzung KMU steht für kleine und mittlere Unternehmen und charakterisiert Unternehmen nach ihrer Größe. Zu den KMU gehören Kleinstunternehmen, kleine Unternehmen und mittlere Unternehmen. In Deutschland sind Größen von Kapitalgesellschaften im Handelsgesetzbuch (HGB) in § 267 HGB definiert. Dort sind sie in kleine, mittelgroße und große Kapitalgesellschaften unterteilt. Der Begriff Kleinstkapitalgesellschaft wird in § 267a HGB

erläutert. Ausschlaggebend für die Einteilung in die Größenklassen sind folgende drei Merkmale:

- Die Bilanzsumme
- „Die Umsatzerlöse in den zwölf Monaten vor dem Abschlußstichtag“
- Die Anzahl der Arbeitnehmer im Jahresdurchschnitt

Zur Einteilung in eine Größenklasse dürfen zwei der drei Kriterien nicht überschritten werden. Bei Kleinstkapitalgesellschaften sind das

- eine Bilanzsumme von 450 000 Euro,
- Umsatzerlöse von 900 000 Euro „in den zwölf Monaten vor dem Abschlußstichtag“ und
- zehn Arbeitnehmer im Jahresdurchschnitt. [21]

Bei kleinen Kapitalgesellschaften betragen die Grenzen

- 7,5 Millionen Euro für die Bilanzsumme,
- 15 Millionen Euro für die Umsatzerlöse „in den zwölf Monaten vor dem Abschlußstichtag“ und
- fünfzig für die Anzahl der Arbeitnehmer im Jahresdurchschnitt. [22]

Mittelgroße Kapitalgesellschaften zeichnen sich durch

- eine Bilanzsummengrenze von bis zu 25 Millionen Euro,
- eine Umsatzerlösgrenze von bis zu 50 Millionen Euro „in den zwölf Monaten vor dem Abschlußstichtag“ und
- eine Arbeitnehmerzahlgrenze von zweihundertfünfzig

aus. [22]

Große Kapitalgesellschaften überschreiten zwei der drei Grenzwerte für mittelgroße Kapitalgesellschaften. Eine Kapitalgesellschaft, die nach § 264d HGB eine Kapitalmarktorientierte Kapitalgesellschaft ist, wird immer als große Kapitalgesellschaft angesehen und nicht als KMU. [22]

Neben der nationalen Definition des Begriffs ist auch die europäische Definition relevant. Diese wird von der Europäischen Kommission in der Empfehlung „2003/361/EG“ vom 6. Mai 2003 vorgenommen. Danach werden für KMU (engl. SMEs für „small and medium-sized enterprises“) die Merkmale Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme herangezogen. Die Anzahl der Mitarbeiter ist auf Vollzeitbeschäftigte in einem Jahr bezogen. Ist eine Person nicht das ganze Jahr in Vollzeit beschäftigt, wird der jeweilige Anteil auf die Gesamtmitarbeiterzahl angerechnet. Ein Kleinstunternehmen hat danach

- weniger als zehn Mitarbeiter und
- einen Jahresumsatz oder eine Jahresbilanzsumme von bis zu zwei Millionen Euro.

Ein kleines Unternehmen hat

- weniger als 50 Mitarbeiter und
- einen Jahresumsatz oder eine Jahresbilanzsumme von bis zu zehn Millionen Euro.

Ein mittleres Unternehmen hat wiederum

- weniger als 250 Mitarbeiter und
- einen Jahresumsatz von maximal 50 Millionen Euro oder
- eine Jahresbilanzsumme von bis zu 43 Millionen Euro.

Ein Unternehmen ist nach dieser Empfehlung „jede Einheit, unabhängig von ihrer Rechtsform, die eine wirtschaftliche Tätigkeit ausübt.“ [23]

2.2 Rechtliche Grundlagen

Im Folgenden werden einige ausgewählte rechtliche Grundlagen genannt, die Organisationen zur Einführung von Maßnahmen und einem Management von Risiken im Bereich der Cybersicherheit verpflichten. Zunächst werden allgemeine Regelungen genannt, aus denen Anforderungen an die Cybersicherheit abgeleitet werden können. Daraufhin werden Gesetze aufgeführt, die sich explizit mit der IT- und Cybersicherheit beschäftigen. Dabei wird jeweils die Relevanz für KMU beachtet. Abschließend werden spezielle Vorschriften zur Cybersicherheit im Gesundheitsbereich in den Blick genommen.

2.2.1 Allgemeine Anforderungen zum Risikomanagement

Mit dem 1998 in Kraft getretenem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) wurde für eine Vielzahl von Unternehmen die Pflicht eingeführt, ein allgemeines Risikomanagement zu betreiben. Da heutzutage nahezu jedes Unternehmen Informationstechnik nutzt und mit dem Internet verbunden ist, sind diese Gesetze auch für Risiken im Bereich der Cybersicherheit relevant. [24]

§ 91 Abs. 2 Aktiengesetz (AktG) fordert Maßnahmen, mit denen Gefährdungen für das Unternehmen früh erkannt werden können. In § 91 Abs. 3 AktG, der mit einem späteren Gesetz eingeführt wurde, wird explizit die Einrichtung eines Risikomanagementsystems gefordert. [25] [24]

Auch im Handelsgesetzbuch (HGB) finden sich Regelungen zum Umgang mit Unternehmensrisiken. So sollen in einem Lagebericht nach § 289 HGB Chancen und Risiken für die Entwicklung des Unternehmen behandelt. [26]

Mit dem 2021 in Kraft getretenem Stabilisierungs- und Restrukturierungsgesetz (StaRUG) werden zum Beispiel Gesellschaften mit beschränkter Haftung (GmbH) und somit auch KMU zu einem Risikomanagement verpflichtet. [27]

2.2.2 BSI-Gesetz und BSI-KritisV

Das „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik“ (BSI-Gesetz) ist 2009 in Kraft getreten. Es regelt die Rolle und Aufgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI). [28]

Das Gesetz definiert die Kritische Infrastruktur als Einrichtungen oder Anlagen, die „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind“ und aus den Sektoren „Energie, Informationstechnik und Kommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen sowie Siedlungsabfallentsorgung“ stammen. Diese Definition kann auch auf KMU zutreffen. [29]

In § 8a des Gesetzes werden für Betreiber Kritischer Infrastrukturen Anforderungen an die Sicherheit ihrer Informationstechnik gestellt. Diese sollen nach dem Stand der Technik Vorkehrungen treffen, damit die Schutzziele der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit bei für die Kritische Infrastruktur relevanten IT-Systeme und Komponenten gewahrt werden können. Im zweiten Absatz des Gesetzes wird die Möglichkeit der Einführung von branchenspezifischen Sicherheitsstandards für Betreiber Kritischer Infrastrukturen beschrieben. Einer dieser Standards wird mit dem branchenspezifischen Sicherheitsstandard „Medizinische Versorgung“ in Kapitel 2.3.2 vorgestellt. [30]

Zur exakten Bestimmung, ob eine Organisation zu den Kritischen Infrastrukturen gehört, sind in der BSI-Kritisverordnung (BSI-KritisV) Kriterien für die einzelnen Sektoren angegeben. Im Sektor Gesundheit sind beispielsweise die stationäre Patientenversorgung, die Versorgung mit „lebenserhaltenden Medizinprodukten“ und „verschreibungspflichtigen Arzneimitteln“ kritische Dienstleistungen. Für Krankenhäuser beträgt der Schwellwert 30.000 vollstationäre Fälle pro Jahr. Für die Versorgung mit Medizinprodukten werden Schwellwerte für den Jahresumsatz oder die Anzahl der hergestellten oder abgegebenen Packungen pro Jahr aufgestellt. [31]

2.2.3 NIS-2-Richtlinie

Die im Jahr 2023 in Kraft getretene „The Network and Information Security (NIS) Directive“ (NIS-2-Richtlinie) der EU erweitert die bisher gültige NIS-Richtlinie aus dem Jahr 2016. Sie verfolgt das Ziel, die Cybersicherheit in der EU zu stärken, indem Anforderungen an besonders bedeutende Einrichtungen gestellt werden. Darüber hinaus wird die Zusammenarbeit der EU-Mitgliedsstaaten im Bereich der Cybersicherheit thematisiert. [32]

Der Geltungsbereich der neuen Richtlinie wurde im Vergleich zu ihrem Vorgänger deutlich ausgeweitet, wodurch auch eine Vielzahl von KMU betroffen sind. Die Richtlinie unterscheidet zwischen wesentlichen und wichtigen Einrichtungen. [33]

Zu den wesentlichen Einrichtungen gehören solche, die einer Liste von elf besonders kritischen Sektoren wie Energie, Verkehr und Gesundheitswesen zugeordnet werden können

und nach der in Kapitel 2.1.3 genannten europäischen KMU-Definition mindestens ein mittleres Unternehmen sind. Unabhängig von der Größe der Einrichtung können zusätzlich weitere Organisationen wie DNS-Diensteanbieter, kritische Einrichtungen oder Einrichtungen der öffentlichen Verwaltung als wesentlich eingestuft werden. Eine zweite Sektorenliste beschreibt weitere Typen von Einrichtungen, die als wesentlich oder wichtig eingestuft werden können. Darüber hinaus werden weitere Faktoren beschrieben, die für eine wesentliche oder wichtige Einrichtung ausschlaggebend sind. Die Einteilung bleibt in Teilen dem jeweiligen EU-Mitgliedstaat überlassen. [33]

Diese Einrichtungen müssen „Risikomanagementmaßnahmen im Bereich der Cybersicherheit“ umsetzen, um Risiken für Netz- und Informationssysteme zu minimieren. Konkret genannt werden darunter Maßnahmen im Bereich von Schulungen, der Kryptografie, der Multi-Faktor-Authentifizierung und im Backup-Management. Auch die Entwicklung von Konzepten für die Risikoanalyse und Bewältigung von Vorfällen und die Überprüfung dieser Konzepte werden gefordert. Abhängig von Größe und Kategorie der Einrichtung unterscheiden sich die Anforderungen und auch Strafen bei Verstößen [34]. [33]

Die Richtlinie geht ebenfalls auf Pflichten zur Registrierung von Einrichtungen an einer zentralen Stelle und auf Meldepflichten ein. [33]

In Deutschland wird die Richtlinie mit dem NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) umgesetzt. Dies muss bis Oktober 2024 erfolgen. Zum Zeitpunkt dieser Arbeit ist die Umsetzung der Richtlinie in das deutsche Recht nicht abgeschlossen. [34]

2.2.4 Datenschutzgrundverordnung (DSGVO)

Im Jahr 2018 ist die Datenschutz-Grundverordnung (DSGVO) in Kraft getreten. Sie regelt die Verarbeitung personenbezogener Daten in der EU. In Deutschland wird sie durch das neue Bundesdatenschutzgesetz (BDSG) umgesetzt. In der DSGVO werden die Bedingungen für das rechtmäßige Erheben, Verarbeiten und Weitergeben personenbezogener Daten sowie Rechte von Betroffenen dargelegt. Die DSGVO ist für jede öffentliche und private Organisation relevant, die personenbezogene Daten verarbeitet. [35]

Damit der Datenschutz gewährleistet werden kann, stellt die DSGVO Sicherheitsanforderungen an die Verarbeitung der Daten. Artikel 32 der DSGVO fordert den Datenverarbeitenden dazu auf, Risiken für die Rechte des Betroffenen einzuschätzen. Daran angepasst müssen Maßnahmen getroffen werden, die das Risiko auf ein angemessenes Niveau senken. Dabei sollen die Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit der genutzten Systeme und Dienste gewahrt werden. Die Maßnahmen enthalten beispielsweise die Pseudonymisierung oder die Verschlüsselung der Daten. Die Überprüfung der Wirksamkeit der Maßnahmen wird ebenfalls gefordert. [36]

Für den Fall, dass ein hohen Risikos erwartet wird, muss „für die Rechte und Freiheiten natürlicher Personen“ eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchgeführt werden. Nach dem siebten Absatz dieses Artikels beinhaltet diese die Beschreibung der Verarbeitungsvorgänge, eine Bewertung der Risiken und Maßnahmen, die die Risiken mildern. [37]

Die personenbezogenen Gesundheitsdaten umfassen alle Daten zum physischen und psychischen Gesundheitszustand einer Person. Dazu gehören Informationen zu Krankheiten, Behinderungen, Krankheitsrisiken, erfolgte Behandlungen, Untersuchungsergebnissen und Kennzeichen, die aus gesundheitlichen Gründen vergeben wurden und anhand derer eine Person identifiziert werden kann, über den vergangenen, aktuellen und zukünftigen Gesundheitszustand einer Person. [38]

Diese Gesundheitsdaten gehören nach Art. 9 Abs. 1 DSGVO zu den besonders schützenswerten personenbezogenen Daten [39]. Das BDSG präzisiert in § 22, wann diese Daten in Deutschland verarbeitet werden dürfen und nennt Schutzmaßnahmen, die getroffen werden müssen. Dazu gehören unter anderem die Sensibilisierung der beteiligten Personen, die Verschlüsselung der Daten und die Beschränkung des Zugangs zu den Daten. [40]

2.2.5 SGB V: Cybersicherheit im Gesundheitswesen

Im fünften Sozialgesetzbuch (SGB) sind einige Gesetze zu finden, die sich speziell mit der Cybersicherheit im Gesundheitswesen befassen. Dazu gehört einerseits § 391 SGB V „IT-Sicherheit in Krankenhäusern“. Dieser verpflichtet Krankenhäuser, die nicht bereits als KRITIS gelten, Maßnahmen zum Schutz von Informationstechnik und Patienteninformationen vorzunehmen. [41]

Andererseits ist hier § 390 SGB V „IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung“ zu nennen. Nach diesem Gesetz müssen die Kassenärztlichen Bundesvereinigungen für Ärzte und Zahnärzte eine Richtlinie vorgeben, die Maßnahmen zur IT-Sicherheit behandelt. Hervorgehoben werden hierbei Anforderungen im Zusammenhang mit der Telematikinfrastruktur und die Mitarbeitersensibilisierung. [42]

2.3 Risikoanalysekonzepte

Um all diese rechtlichen Anforderungen zu erfüllen, braucht eine Organisation einen strukturierten Ansatz, mit dem sie Anforderungen, Umstände und Aktivitäten erheben, planen und steuern kann. Für diese Aufgabe wurden eine Reihe von Standards entwickelt. Vier von diesen werden in den folgenden Kapitel vorgestellt. Dabei handelt es sich um den IT-Grundschutz des BSI, den branchenspezifischen Sicherheitsstandard „Medizinische Versorgung“, OCTAVE-S und die ISO/IEC-Norm 27005. Darüber hinaus werden Grundlagen zu den Threat-Modeling-Konzepten STRIDE und DREAD dargestellt.

2.3.1 IT-Grundschutz des BSI

Der IT-Grundschutz ist eine vom Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte Sammlung von Standards zur strukturierten Umsetzung von Informationssicherheit auf einem angemessenem Niveau in Unternehmen und Behörden. Grundsätzlich gilt dies für Institutionen aller Arten und Größen. [43, S. 10]

Das BSI ist eine Bundesbehörde, die sich mit der Informations- und Cybersicherheit in Deutschland befasst [44]. Die Aufgaben der Behörde sind unter anderem im BSI-Gesetz und im IT-Sicherheitsgesetz verankert [45]. Darunter fallen zum Beispiel der Schutz von Regierungsnetzen und zentraler Netzübergänge vor Cyberangriffen, das Fungieren als zentrale Meldestellte innerhalb der Bundesverwaltung und die Aufsicht über Betreiber Kritischer Infrastrukturen (KRITIS) [45]. Genauso ist es dafür zuständig, Sicherheitsrisiken einzuschätzen und die Cybersicherheitslage sowohl national als auch international zu beobachten [44]. Das BSI ist nicht nur zuständig für öffentliche Stellen und Kritische Infrastrukturen, sondern auch Ansprechpartner und Bereitsteller von Empfehlungen, Best Practices und Standards für Wirtschaft und Bürger [46].

Als ein solcher Standard, der auch an private Unternehmen gerichtet ist, beschreibt der IT-Grundschutz einen ganzheitlichen Ansatz zur Informationssicherheit. Das heißt, dass sich dieser nicht nur auf technische Aspekte beschränkt, sondern auch die Themen Infrastruktur, Organisation und Personal behandelt. [43, S. 6]

Er ist mit Normen der ISO-Reihen 27000 und 31000 kompatibel oder berücksichtigt diese und ermöglicht eine Zertifizierung nach ISO/IEC 27001 auf Basis des IT-Grundschutzes. [43, S. 12] [43, S. 39]

Der IT-Grundschutz besteht aus den vier Standards

- BSI-Standard 200-1: Managementsysteme für Informationssicherheit (ISMS),
- BSI-Standard 200-2: IT-Grundschutz-Methodik,
- BSI-Standard 200-3: Risikoanalyse auf der Basis von IT-Grundschutz,
- BSI-Standard 200-4: Business Continuity Management,

die den methodischen Rahmen zum Aufbau eines ISMS beinhalten und dem IT-Grundschutz-Kompendium, das konkrete Sicherheitsanforderungen und Maßnahmen darstellt. In den folgenden Kapiteln werden diese Dokumente näher beleuchtet. [47]

2.3.1.1 IT-Grundschutz-Kompendium

Das IT-Grundschutz-Kompendium ist neben den BSI-Standards eine zentrale Veröffentlichung des IT-Grundschutzes, die in der Regel jährlich aktualisiert wird. Während die BSI-Standards die Methodik des IT-Grundschutzes beschreiben, gibt das IT-Grundschutz-

Kompendium mit der Sammlung von Grundschutz-Bausteinen und elementaren Gefährdungen inhaltliche Hilfestellungen bei der Umsetzung des IT-Grundschutzes. In dieser Arbeit wird das Kompendium aus dem Jahr 2023 verwendet. [4] [48]

Das Kompendium beinhaltet eine Auflistung von insgesamt 47 elementaren Gefährdungen. Diese kommen bei der Risikoanalyse im BSI-Standard 200-3 zum Einsatz, sind produktneutral und möglichst technikneutral. Indirekte Gefährdungen, die zum Beispiel durch das Fehlen von Sicherheitsmaßnahmen entstehen, gehören nicht zu den elementaren Gefährdungen. Beispiele für elementare Gefährdungen sind allgemeine Gefährdungen wie Feuer oder Personalausfall genauso wie technische Gefährdungen wie Schadprogramme. Eine elementare Gefährdung betrifft einen oder mehrere der Grundwerte Vertraulichkeit, Integrität und Verfügbarkeit. [4] [3, S. 13]

Das Kernstück des Kompendiums bilden die IT-Grundschutz-Bausteine. Mit Hilfe dieser wird in der IT-Grundschutz-Methodik (BSI-Standard 200-2) die Modellierungsphase durchgeführt. In dieser werden passende Bausteine für den Informationsverbund ausgewählt. Von diesen gibt es Prozess- und System-Bausteine, welche jeweils weiter untergliedert sind. Prozess-Bausteine werden meist auf den gesamten oder einen großen Teil des Informationsverbunds angewendet. Diese sind in die folgenden Schichten unterteilt:

- ISMS (Sicherheitsmanagement)
- ORP (Organisation und Personal)
- CON (Konzepte und Vorgehensweisen)
- OPS (Betrieb)
- DER (Detektion und Reaktion)

Mit System-Bausteinen werden meist einzelne oder Gruppen von Zielobjekten modelliert. Die System-Bausteine werden in die Schichten

- APP (Anwendungen),
- SYS (IT-Systeme),
- IND (Industrielle IT),
- NET (Netze und Kommunikation) und
- INF (Infrastruktur)

unterteilt. [4]

Jeder dieser Bausteine betrachtet ein bestimmtes Thema und ist nach der gleichen Struktur aufgebaut. Diese beginnt mit einer Beschreibung des Zielobjekts, einer Zielsetzung sowie Hinweisen zur Modellierung und der Abgrenzung zu anderen Bausteinen. Im Anschluss wird ein Überblick über spezifische Gefährdungen gegeben, die beim Zielobjekt in Betracht kommen. [4]

Darauf folgen die zu erfüllenden Anforderungen für den Baustein. Diese werden in Basis-Anforderungen, Standard-Anforderungen und „Anforderungen bei erhöhtem Schutzbedarf“

aufgeteilt. Basis-Anforderungen sollten zunächst erfüllt werden. Anschließend sollten Standard-Anforderungen umgesetzt werden, die den aktuellen Stand der Technik bei normalen Schutzbedarf abbilden. Bei den Anforderungen für erhöhten Schutzbedarf handelt es sich lediglich um Vorschläge. Bei einem erhöhtem Schutzbedarf kommt nach IT-Grundschutz-Methodik die Risikoanalyse zum Einsatz, bei der zusätzliche Maßnahmen ermittelt werden. [4]

Ein Beispiel für einen Baustein ist der „SYS.2.1 Allgemeiner Client“. Dieser beschreibt betriebssystemunabhängig einen Client. Darauf aufbauend gibt es zum Beispiel den Baustein „SYS.2.2.3 Clients unter Windows“ speziell für Windows-Systeme. Bei der Modellierung müssen beide Bausteine ausgewählt werden. Das Konzept, dass zunächst ein allgemeiner Baustein eine Grundlage bildet und darauf aufbauend spezifische Bausteine existieren, findet sich an vielen Stellen des Grundschutz-Kompendiums wieder. [4]

2.3.1.2 BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS)

Der Standard 200-1 definiert zunächst grundlegende Anforderungen und Bestandteile eines Informationssicherheitsmanagementsystems (ISMS) und beschreibt allgemein wie ein solches in einer Institution aufgebaut werden kann. [43, S. 12]

Nach Definition dieses Standards umfasst ein Managementsystem „alle Regelungen, die für die Steuerung und Lenkung einer Institution sorgen und letztlich zur Zielerreichung führen sollen” [43, S. 15]. Ein Informationssicherheitsmanagementsystem wiederum, ist der Teil des Managementsystems, der die Informationssicherheit im Fokus hat. Es bestimmt somit die Instrumente und Methoden der Leitungsebene zur Lenkung der Aufgaben und Aktivitäten in Bezug auf die Informationssicherheit. Ein ISMS umfasst die Komponenten Managementprinzipien, Ressourcen, Mitarbeiter und Sicherheitsprozess. [43, S. 15]

Der Sicherheitsprozess setzt sich aus der Leitlinie zur Informationssicherheit, dem Sicherheitskonzept und der Sicherheitsorganisation zusammen. In der Leitlinie zur Informationssicherheit erklärt die Leitungsebene die Sicherheitsziele und die Sicherheitsstrategie zu deren Umsetzung. Die Sicherheitsstrategie wird wiederum einerseits mit Hilfe einer Sicherheitsorganisation, in welcher die Mitarbeiter sowie deren Rollen und Aufgaben im Sicherheitsprozess geplant werden, und andererseits mit Hilfe des Sicherheitskonzepts realisiert. [43, S. 15f.] [43, S. 30]

In diesem Standard werden die Gesamtverantwortung und Aufgaben der Leitungsebene im Informationssicherheitsmanagement herausgehoben, wie beispielsweise die Zuteilung und Bereitstellung von Ressourcen. Es wird verdeutlicht, dass die Mitarbeiter in den Sicherheitsprozess integriert werden müssen. [43]

Der Sicherheitsprozess und seine Komponenten sind an einen „Lebenszyklus“ angelehnt, dem PDCA-Zyklus nach Deming. Dieser besteht aus den vier Phasen „Plan“, „Do“, „Check“

und „Act“. Nach Abschluss der letzten Phase beginnt der Zyklus von vorne. Der Lebenszyklus der Informationssicherheit nach IT-Grundschutz des BSI hat die Phasen

- „Planung,
- Umsetzung der Planung bzw. Durchführung des Vorhabens,
- Erfolgskontrolle bzw. Überwachung der Zielerreichung
- und Beseitigung von erkannten Mängeln und Schwächen bzw. Optimierung sowie Verbesserung.“ [43, S. 18]

Auch aufgrund sich ständig veränderter Rahmenbedingungen ist Informationssicherheit kein einmalig zu erreichender Zustand, sondern ein Prozess, der regelmäßig überprüft und optimiert werden muss. Dies geschieht in den Schritten „Erfolgskontrolle bzw. Überwachung der Zielerreichung“ und der „Beseitigung von Mängeln bzw. Optimierung sowie Verbesserung“. [43, S. 17]

2.3.1.3 BSI-Standard 200-2 IT-Grundschutz-Methodik

Der BSI-Standard 200-2 konkretisiert die im Standard 200-1 beschriebenen Schritte und gibt eine Anleitung zum Aufbau eines Informationssicherheitsmanagementsystems. Dabei beschreibt und erklärt der Standard die Phasen des Informationssicherheitsprozesses in einzelnen Kapitel. Er stellt verschiedene Vorgehensweisen mit Unterschieden in Aufwand und Fokus der betrachteten Geschäftsprozesse und Zielobjekte zur Auswahl. Dies ermöglicht eine an die Institution angepasste Vorgehensweise, die auch für KMU praktikabel ist. [18]

Abbildung 1 zeigt die einzelnen Phasen des Sicherheitsprozesses, welche im Folgenden näher beschrieben werden.

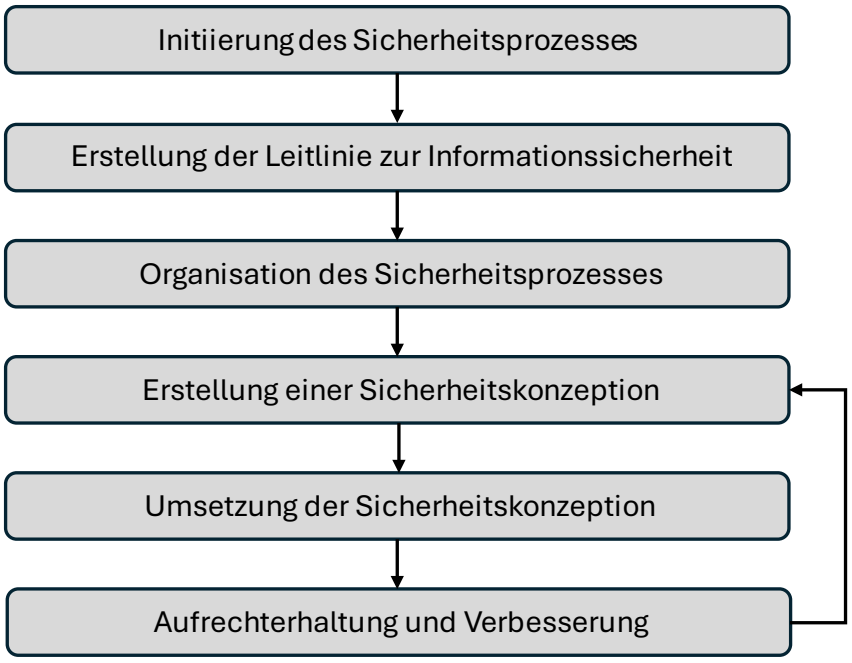

Abbildung 1: Phasen des Sicherheitsprozesses (Abbildung nach [18])

Initiierung des Sicherheitsprozesses

In der ersten Phase übernimmt die Leitungsebene zunächst die Verantwortung für den Sicherheitsprozess und initiiert diesen. Sie ist auch für die Steuerung des Prozesses und für die Zuteilung von Ressourcen verantwortlich. In dieser Phase wird der Sicherheitsprozess konzipiert und geplant. Dazu gehört, dass man sich die Rahmenbedingungen vergegenwärtigt und Informationssicherheitsziele formuliert. Genauso beinhaltet das eine erste Erfassung von Prozessen, Anwendungen und IT-Systemen. Darüber hinaus muss eine der drei Vorgehensweise „Standard-Absicherung“, „Basis-Absicherung“ und „Kern-Absicherung“ ausgewählt und der Geltungsbereich bestimmt werden. Letzteres sind die Bereiche der Institution, die geschützt werden sollen. Der Geltungsbereich für die Erstellung einer Sicherheitskonzeption wird auch Informationsverbund genannt. [18]

Erstellung der Leitlinie zur Informationssicherheit

Die Ergebnisse der vorangegangenen Schritte werden in einer Leitlinie gebündelt und mit dieser institutionsweit bekanntgegeben. Diese bezieht sich neben den oben genannten Punkten auf die Bedeutung der Informationssicherheit für die Institution, wichtige Inhalte der Sicherheitsstrategie und der Organisationstruktur, welche nachfolgend beschrieben wird. [18]

Organisation des Sicherheitsprozesses

Die nächste Phase beschäftigt sich mit der Organisation und den Aufgaben von Mitarbeitern im Sicherheitsprozess. Zu nennen ist hier der Informationssicherheitsbeauftragte (ISB), der

den Sicherheitsprozess koordinieren soll. Je nach Art und Größe der Institution können weitere Mitarbeiter mit Aufgaben der Informationssicherheit betraut werden. Bei der Organisation des Sicherheitsprozesses muss auch auf die Einbindung der Verantwortlichen für die Informationssicherheit in die Institutionsstrukturen und -abläufe geachtet werden. Der ISB sollte zum Beispiel als Stabsstelle eingerichtet sein, die direkt der Managementebene berichtet. [18, S. 36]

Erstellung einer Sicherheitskonzeption

Zur Erstellung der Sicherheitskonzeption beschreibt der Standard die drei Vorgehensweisen „Standard-Absicherung“, „Basis-Absicherung“ und „Kern-Absicherung“. Diese werden im Folgenden näher dargestellt. Die Vorgehensweisen unterscheiden sich in Geltungsbereich und Schutzniveau und sind in Abbildung 2 zu sehen. Während sich die Kern-Absicherung nur um einen bestimmten, besonders gefährdeten Bereich der Institution kümmert, bietet die Basis-Absicherung eine breite und grundlegende Absicherung aller relevanten Geschäftsprozesse. Die Standard-Absicherung soll wiederum für einen breiten und tiefgehenden Schutz sorgen. Die Wahl über die Vorgehensweise wurde bereits in der Initiierungsphase getroffen. [18, S. 28ff.]

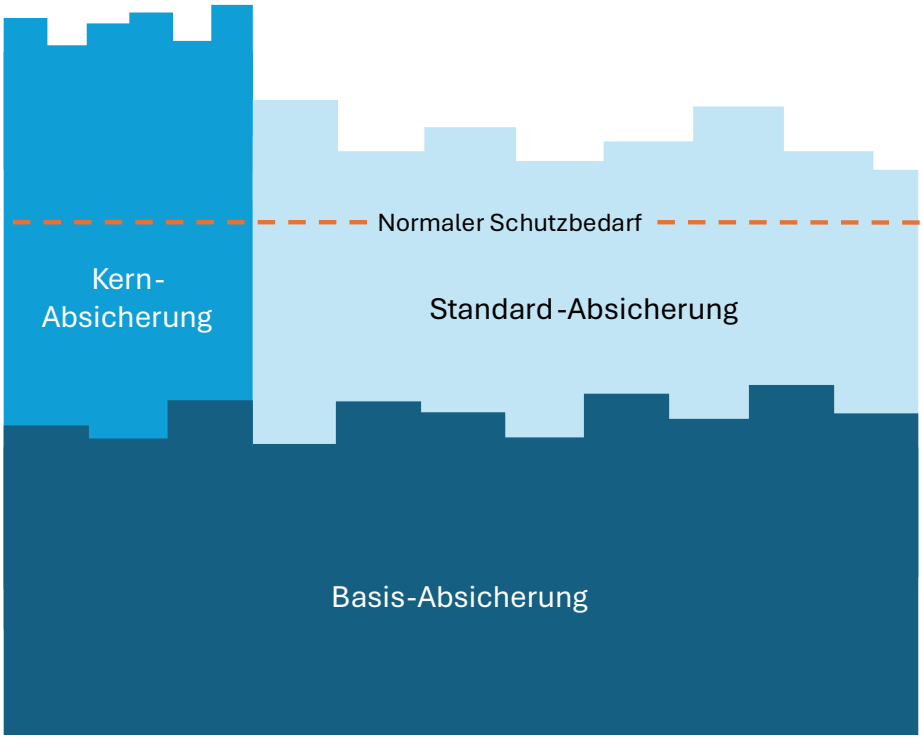

Abbildung 2: Vorgehensweisen der Sicherheitskonzeption und ihr Absicherungsgrad (Abbildung nach [49])

Standard-Absicherung

Mit der Standardvariante soll die Absicherung der Institution sowohl in Umfang als auch in der Tiefe auf einem angemessenem Niveau erfolgen. Es sollte das Ziel sein, diese

Vorgehensweise für die gesamte Institution zu etablieren. In Abbildung 3 sind die einzelnen Arbeitsschritte der Standard-Absicherung dargestellt. [18, S. 30]

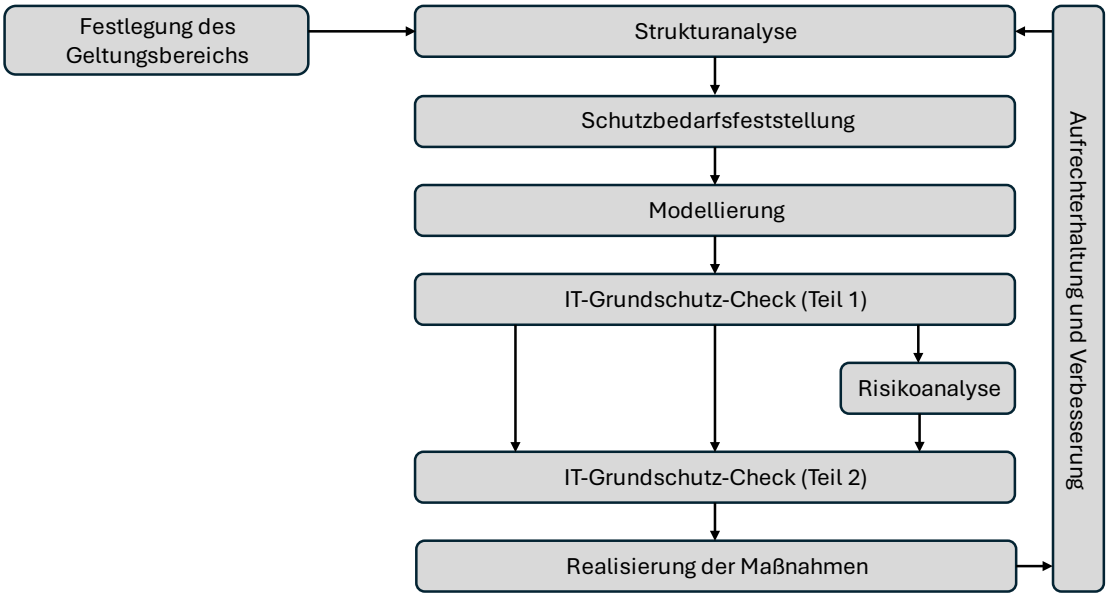

Abbildung 3: Erstellung der Sicherheitskonzeption bei der Standard-Absicherung (Abbildung nach [18, S. 76])

Für den in den vorhergehenden Schritten festgelegten Geltungsbereich wird zunächst eine Strukturanalyse durchgeführt. Hier werden unter anderem Geschäftsprozesse, Anwendungen, IT-Systeme und Räume sowie deren Zusammenhänge erfasst. Erhobene Objekte werden in einem Netzplan grafisch dargestellt. [18, S. 78f.]

In der Schutzbedarfsfeststellung wird den erfassten Objekten, Geschäftsprozessen und Anwendungen anhand zu erwartender Schäden eine Schutzbedarfskategorie zugeordnet. Der Standard schlägt dabei die drei Kategorien „normal“, „hoch“ und „sehr hoch“ vor. Der Schutzbedarf wird jeweils für die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit bestimmt. [18, S. 104]

Nach Abschluss der Schutzbedarfsfeststellung wird der Informationsverbund in der Modellierung mit Bausteinen des IT-Grundschutz-Kompendiums nachgebildet. Für jedes Objekt, jeden Geschäftsprozess und jede Anwendung werden ein oder mehrere Bausteine ausgewählt. Aus diesen ergeben sich Sicherheitsanforderungen, für deren Erfüllung Sicherheitsmaßnahmen getroffen werden müssen. [18, S. 134ff.]

Nach der Modellierung des Informationsverbunds wird mit dem IT-Grundschutz-Check das aktuelle Sicherheitsniveau eingeschätzt. Dazu wird im „Soll-Ist-Vergleich“ überprüft, welche der zuvor ermittelten Sicherheitsanforderungen erfüllt, und welche noch nicht erfüllt sind. Daraus ergibt sich ein Handlungsbedarf an umzusetzenden Maßnahmen. Dies geschieht vor und nach der Risikoanalyse. [18, S. 77f.] [18, S. 145]

Unter bestimmten Umständen ist mit einer zusätzlichen Risikoanalyse die Ermittlung weiterer Maßnahmen zum Schutz der Objekte, Geschäftsprozesse und Anwendungen erforderlich. Diese Umstände und das Vorgehen bei der Risikoanalyse werden in Kapitel 2.3.1.4 erklärt. [18, S. 78]

Basis-Absicherung

Die Basis-Absicherung bietet einen vereinfachten Einstieg in das Informationssicherheitsmanagement mit dem IT-Grundschutz. Diese Variante kann mit geringerem Aufwand bei Zeitdruck oder Ressourcenmangel durchgeführt werden, was zum Beispiel für KMU hilfreich ist. Mit ihr kann man schnell den größten Risiken begegnen und im weiteren Verlauf ein höheres Sicherheitsniveau mit Hilfe der anderen Vorgehensweisen aufbauen. Im Vergleich zur Standard-Absicherung (s. Abbildung 3) ist die Anzahl der Arbeitsschritte in der Basis-Absicherung reduziert (s. Abbildung 4). Zu den entfallenden Schritten gehört unter anderem die Risikoanalyse. [18, S. 28f.]

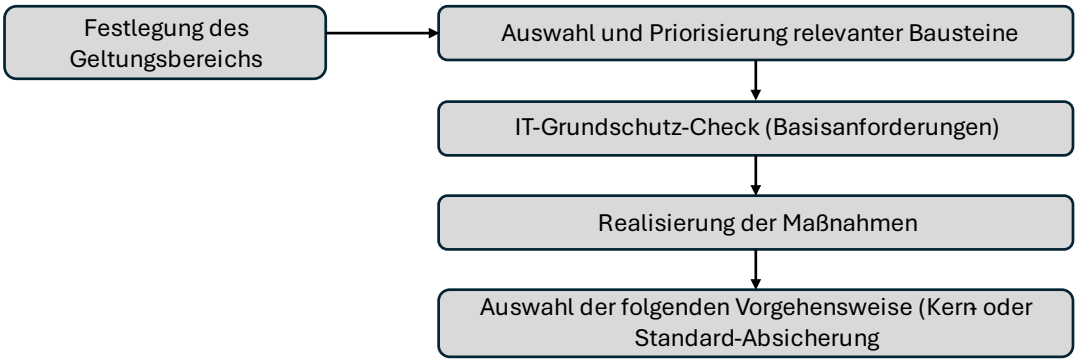

Abbildung 4: Vorgehen bei der Basis-Absicherung (Abbildung nach [18, S. 61])

Nach der Auswahl des Geltungsbereichs werden Bausteine des IT-Grundschutz-Kompendiums ausgewählt und priorisiert und damit der Informationsverbund nachgebildet. Anschließend wird im IT-Grundschutz-Check überprüft, welche Basis-Anforderungen bereits erfüllt sind. Daraufhin müssen für fehlende Basis-Anforderungen Sicherheitsmaßnahmen umgesetzt werden. Die Basis-Absicherung sieht keinen zyklischen Prozess vor. Daher besteht der letzte Schritt aus dem Übergang in die Standard- oder Kern-Absicherung. [18, S. 61f.]

Kern-Absicherung

Die Schritte der Kern-Absicherung stimmen weitestgehend mit denen der Standard-Absicherung überein. Die Vorgehensweise unterscheidet primär durch einen kleinen und gezielt abgegrenzten Geltungsbereich. Damit sollen die wichtigsten Geschäftsprozesse und Informationen der Institution abgesichert werden. [18, S. 28f.]

Zunächst wird der Geltungsbereich festgelegt und die wichtigsten Geschäftsbereiche identifiziert. Die darauf folgenden Schritte

- der „Strukturanalyse“,
- der „Schutzbedarfsfeststellung“,
- der „Modellierung“,
- des „IT-Grundschutz-Checks“,
- der „Risikoanalyse und weiterführende Sicherheitsmaßnahmen“
- und der „Umsetzung und weitere Schritte“ (Verbesserung, Erweiterung, Zertifizierung)

sind bereits aus der Standard-Absicherung bekannt. [18, S. 68]

Ausgehend von der Kern-Absicherung kann die Ausweitung des Sicherheitsprozesses auf weitere Institutionsbereiche mit der Basis- oder Standardabsicherung oder mit einer Erweiterung des Geltungsbereiches für die Kern-Absicherung erfolgen. [18, S. 74]

Umsetzung der Sicherheitskonzeption

In der Umsetzungsphase der Sicherheitskonzeption werden die Ergebnisse der vorangegangenen Phase gesichtet und Kosten und Aufwand dieser Maßnahmen geschätzt. Anschließend werden die Reihenfolge der Umsetzung der Maßnahmen und die für die Umsetzung zuständigen Mitarbeiten festgelegt und ein Realisierungsplan erstellt. [18, S. 158ff.]

Aufrechterhaltung und Verbesserung

Die letzte Phase, die den zyklischen Charakter des Sicherheitsprozesses verdeutlicht, hat das Ziel, das Informationssicherheitsniveau aufrechtzuerhalten und stetig zu verbessen. Hierzu wird der gesamte Sicherheitsprozess regelmäßig überprüft. Auch eine Erweiterung der Vorgehensweise von Basis- oder Kern-Absicherung auf die Standard-Absicherung bietet sich an dieser Stelle an. Die in dieser Phase erarbeiteten Ergebnisse bilden die Basis für eine neue Iteration im Informationssicherheitsprozess. [18, S. 164ff.]

2.3.1.4 BSI-Standard 200-3 Risikoanalyse auf der Basis von IT-Grundschutz

Eine Risikoanalyse nach BSI-Standard 200-3 ist der Prozess der Beurteilung und Behandlung von Risiken. Die Beurteilung umfasst das Identifizieren, Einschätzen und Bewerten von Risiken. Basierend auf elementaren Gefährdungen des IT-Grundschutz-Kompendiums sollen ergänzende Maßnahmen zur Minimierung der Risiken für bestimmte Objekte des Informationsverbunds erarbeitet werden. [3, S. 6f.]

Der Standard erfordert, dass im Sicherheitsprozess des IT-Grundschutzes (BSI-Standard 200-2) die Phase des ersten IT-Grundschutz-Checks und vorhergehende Phasen

abgeschlossen sind und eine Liste von für die Risikoanalyse vorgemerkten Objekten, Geschäftsprozessen und Anwendungen vorhanden ist. Eingebunden in den Sicherheitsprozess des IT-Grundschutzes ist die Risikoanalyse nach dem ersten IT-Grundschutz-Check (s. Abbildung 5). Im Anschluss an die Risikoanalyse wird erneut ein IT-Grundschutz-Check durchgeführt. [3, S. 7ff.]

Die Risikoanalyse kommt im Rahmen des IT-Grundschutzes zum Einsatz, wenn

- der Schutzbedarf eines Zielobjekts als hoch oder sehr hoch in mindestens einem der Schutzziele eingeschätzt wurde,
- es für ein Zielobjekt keinen passenden Baustein im IT-Grundschutz-Kompendium gibt oder
- das Zielobjekt im Informationsverbund in einem nicht vom IT-Grundschutz vorgesehenen Szenario eingesetzt wird. [3, S. 6]

Für Zielobjekte, die in einem vorgesehenen Einsatzszenario mit Bausteinen des IT-Grundschutz-Kompendiums abgebildet werden können und nur einen normalen Schutzbedarf haben, wurde bereits vom BSI eine Risikoanalyse vollzogen. Daher ist für diese keine Risikoanalyse notwendig. Das tritt in der Regel auf den größten Teil des Informationsverbundes zu. [3, S. 5f.]

Der Risikoanalyseprozess dieses Standards besteht aus den vier Schritten (s. Abbildung 5)

- Erstellung einer Gefährdungsübersicht,
- Risikoeinstufung,
- Risikobehandlung und
- Konsolidierung des Sicherheitskonzepts.

Die einzelnen Schritte der Risikoanalyse werden in diesem Kapitel erklärt. [3, S. 7]

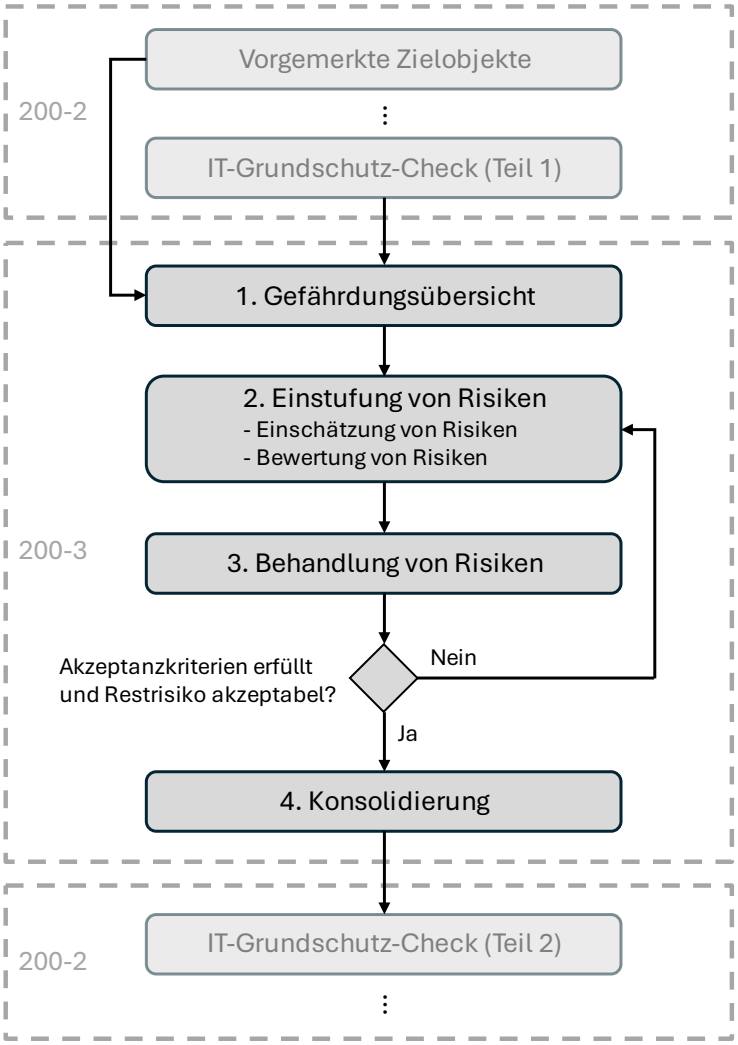

Abbildung 5: Arbeitsschritte der Risikoanalyse und Integration in den Sicherheitsprozess (Abbildung nach [3, S. 7])

Bevor jedoch der Prozess der Risikoanalyse gestartet werden kann, muss die Institution Grundsätze zum Umgang mit Risiken bestimmen. Diese sollten von der Leitungsebene in einer Richtlinie dargelegt werden. Diese macht beispielsweise Angaben über Verantwortlichkeiten und Risikoakzeptanzkriterien. Letztere sind von der Risikoneigung, auch Risikoappetit genannt, abhängig. Eine Institution sollte sich der eigenen Risikoneigung bewusst sein und diese dokumentieren. Die IT-Grundschutz-Methodik ermöglicht auch die Wahl eines anderen Standards zur Risikoanalyse als den BSI-Standard 200-3. Die Wahl des Standards sollte ebenfalls in der Richtlinie festgehalten werden. [3, S. 10]

Erstellung der Gefährdungsübersicht

In der ersten Phase der Risikoanalyse wird anhand der elementaren Gefährdungen des IT-Grundschutz-Kompendiums eine Gefährdungsübersicht erstellt. Dabei wird für jedes Zielobjekt jede elementare Gefährdung herangezogen und überprüft, ob diese für das Objekt relevant ist. Falls es für das Objekt einen passenden Baustein gibt, der bereits elementare

Gefährdungen angibt, muss überprüft werden, ob zusätzliche elementare Gefährdungen relevant sind. Die elementaren Gefährdungen werden danach bewertet, ob sie für das Zielobjekt „direkt relevant“, „indirekt relevant“ oder „nicht relevant“ sind. Nur „direkt relevante“ Gefährdungen fließen in die Risikoanalyse ein. [3, S. 16ff.]

Neben elementaren Gefährdungen müssen für die Objekte zusätzliche Gefährdungen ermittelt werden, welche aus dem speziellen Anwendungsfall des Zielobjekts abgeleitet werden können. Hierbei werden nicht primär neue elementare Gefährdungen gesucht, sondern eher bestimmte Aspekte einer elementaren Gefährdung konkretisiert, um besser spezifische Maßnahmen entwickeln zu können. Dabei sollten Gefährdungen für ein Zielobjekt gesucht werden, die einen Grundwert (Vertraulichkeit, Integrität und Verfügbarkeit) betreffen, dessen Schutzbedarf als hoch oder sehr hoch eingestuft wird. [3, S. 23]

Das Resultat dieses Schrittes ist eine Zuordnung von elementaren Gefährdungen sowie zusätzlichen Gefährdungen zu jedem Zielobjekt, das in der Risikoanalyse betrachtet wird. Hier wurden also die Risiken identifiziert. [3, S. 16ff.]

Risikoeinstufung

Die nachfolgende Phase, die Risikoeinstufung, teilt sich in die beiden Arbeitsschritte der Risikoeinschätzung und der Risikobewertung auf.

In der Risikoeinschätzung wird für jede im vorherigen Schritt ermittelte Gefährdung jedes Zielobjekts die Eintrittshäufigkeit der Gefährdung und die Schadenshöhe, die von der Gefährdung ausgeht, eingeschätzt. Der Standard schlägt eine qualitative Einschätzung der Risiken mit jeweils vier Kategorien vor. Diese können vom Anwender angepasst werden. Für die Eintrittshäufigkeit werden die Kategorien „selten“, „mittel“, „häufig“ und „sehr häufig“ vorgeschlagen. Die Einteilung in diese soll auf Basis von Statistiken und der Erfahrung von Fachpersonal erfolgen. Die potenzielle Schadenshöhe kann in die Kategorien „vernachlässigbar“, „begrenzt“, „beträchtlich“ und „existenzbedrohend“ eingeteilt werden. Die Einschätzung der Schadenskategorie muss von der Institution selbst vorgenommen werden. Dabei sollten nicht nur direkte Schäden, sondern auch Folgeschäden, Behebungskosten und Schäden beachtet werden, die über das Finanzielle hinausgehen. [3, S. 26]

In der Risikobewertung wird eine Risikomatrix anhand der Kategorien „Eintrittshäufigkeit“ und „Schadenshöhe“ aufgespannt (s. Abbildung 6). In den Feldern der Matrix ist die Risikokategorie angegeben. Vorgeschlagen werden die Kategorien „gering“, „mittel“, „hoch“ und „sehr hoch“. Auf welchem Feld der Matrix welche Risikokategorie liegt, muss vom Anwender bestimmt werden. Mit der Risikomatrix kann nun für eine bestimmte Gefährdung eines Zielobjekts, nach Einschätzung von Eintrittshäufigkeit und Schadenshöhe, das Risiko bestimmt werden. Schon umgesetzte oder geplante Maßnahmen zur Erfüllung der Basis- und Standard-Anforderungen werden bei der Risikobestimmung beachtet. [3, S. 27f.]

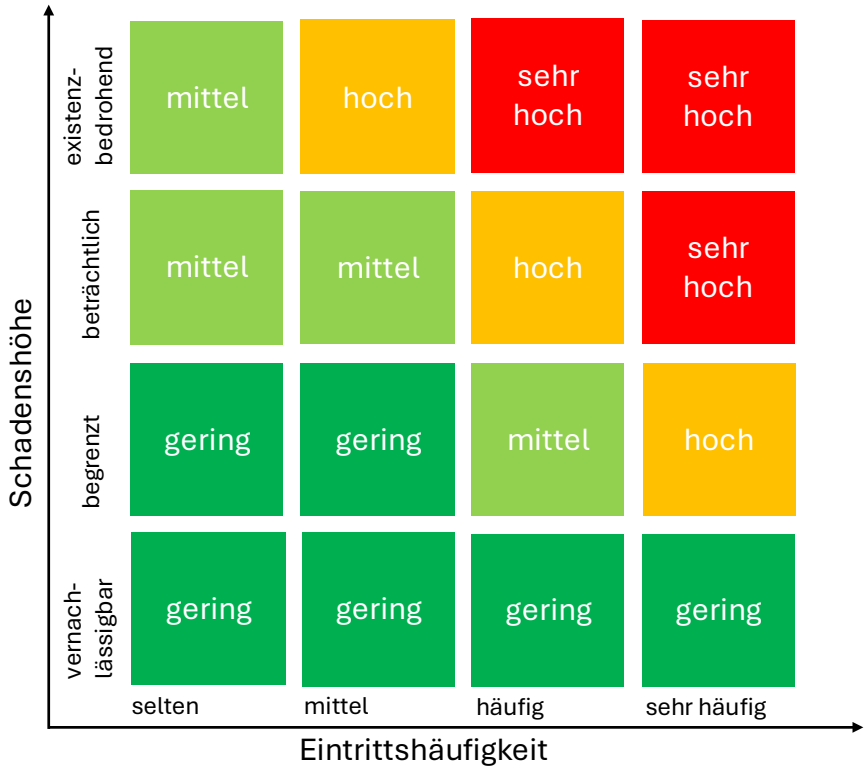

Abbildung 6: Beispiel einer Risikomatrix (Abbildung nach [50])

Risikobehandlung

Im Anschluss folgt die Phase der „Behandlung von Risiken“. Dabei stellt sich zunächst die Frage, Risiken welcher Kategorie akzeptiert werden und welche Risiken behandelt werden müssen. Dies hängt von den Risikoakzeptanzkriterien ab. Grundsätzlich gibt es die vier Optionen „vermeiden“, „reduzieren“, „transferieren“ und „akzeptieren“ im Umgang mit Risiken. [3, S. 33]

Bei der Risikovermeidung werden zum Beispiel Geschäftsprozesse oder der Informationsverbund umstrukturiert, um die Ursache des Risikos auszuschließen. Durch die Einführung ergänzender Maßnahmen kann das Risiko reduziert werden. Der Risikotransfer sorgt dafür, dass die Institution das Risiko zum Beispiel mit einer Versicherung oder durch Outsourcing mit einer anderen Institution teilt. Die letzte Option ist die Akzeptanz des Risikos. [3, S. 33f.]

Die Risikoeinstufung und die Behandlungsphase von Risiken müssen so lange wiederholt werden, bis das Restrisiko den Akzeptanzkriterien entspricht. Verantwortlich für das Restrisiko ist die Leitungsebene und daher muss sie diesem letztendlich zustimmen. [3, S. 34]

Konsolidierung des Sicherheitskonzepts

Nach der Ermittlung neuer Maßnahmen, muss das Sicherheitskonzept konsolidiert werden. Hier werden bisher bestehende Sicherheitsmaßnahmen und neue Maßnahmen überprüft und gegebenenfalls angepasst. Dies geschieht unter anderem in Hinblick auf Kostenfragen,

der Eignung der Maßnahmen, um den Gefährdungen zu begegnen, der Akzeptanz bei den Mitarbeitern und dem Zusammenwirken der Maßnahmen. In der Risikoanalyse erarbeitete neue Gefährdungen und Anforderungen sollten in die Dokumentation des IT-Grundschutz-Prozesses integriert werden. [3, S. 39]

Nach Abschluss der Risikoanalyse wird der IT-Grundschutz-Prozess, der in Kapitel 2.3.1.3 beschrieben ist, fortgesetzt.

2.3.1.5 BSI-Standard 200-4 Business Continuity Management

Der BSI-Standard 200-4 “Business Continuity Management” (BCM) ist seit 2023 gültig und ersetzt den BSI-Standard 100-4 “Notfallmanagement”. Er beschreibt eine Methodik zum Aufbau eines Managementsystems, das das Ziel verfolgt, den Geschäftsbetrieb auch in Notfällen und Schadensfällen aufrechtzuerhalten bzw. schnell wieder fortzusetzen. [51, S. 11ff.]

Dieses Business-Continuity-Managementsystem (BCMS) zielt auf den Schutz „zeitkritischer Geschäftsprozesse“ ab, welche vor Ausfällen geschützt werden sollen, die einen erheblichen Einfluss auf den Geschäftsbetrieb haben. Der Prozess des Systems basiert auf dem PDCA-Zyklus und umfasst die Initiierung, Implementierung, Steuerung sowie Aufrechterhaltung und Verbesserung des Business-Continuity-Managements. [51, S. 15] [51, S. 19]

Der Standard ist nach einem Stufenmodell aufgebaut, das dem Anwender den Einstieg in das BCM vereinfachen soll. Damit richtet er sich auch an kleine und mittlere Institutionen. Die drei Stufen „Reaktiv-BCMS“, „Aufbau-BCMS“ und „Standard-BCMS“ unterscheiden sich in Methodik und Umfang der betrachteten Geschäftsprozesse. Das Reaktiv-BCMS ist im Umfang der Geschäftsprozesse reduziert und fokussiert sich auf Maßnahmen zur Notfallbewältigung. Das Aufbau-BCMS umfasst die gesamte Methodik des BCM einschließlich Vorsorgemaßnahmen. In Bezug auf den Umfang der Geschäftsprozesse ist es jedoch weiterhin eingeschränkt. Indem das BCMS um weitere Geschäftsprozesse ergänzt wird, entwickelt es sich letztendlich zum Standard-BCMS. Dieses umfasst alle Geschäftsprozesse und die gesamte Methodik und stellt die anzustrebende Variante dar. [51, S. 41]

Der Standard beinhaltet auch Ausführungen zu einer „BCM-Risikoanalyse“. Diese beschreibt jedoch keine eigene Risikoanalyse-Methodik, sondern stellt für das BCM relevante Besonderheiten bei der Risikoanalyse heraus. Zur Risikoanalyse kann hier zum Beispiel der BSI-Standard 200-3 verwendet werden. [51, S. 199]

Die Risikoanalyse dient hier dazu, Risiken zu identifizieren und zu behandeln, die die zeitkritischen Geschäftsprozesse bedrohen. Daher steht das Schutzziel der Verfügbarkeit im Fokus bei der Erstellung der Gefährdungsübersicht nach BSI-Standard 200-3. Der Einfluss der anderen Schutzziele auf die Verfügbarkeit darf jedoch nicht außer Acht gelassen werden. Die Schritte der Risikoeinschätzung und Risikobewertung unterscheiden sich hier

nicht. Anhand von Eintrittshäufigkeit und Schadenshöhe wird eine Risikomatrix gebildet und Risikokategorien gebildet. Bei der Behandlung von Risiken wird von der Option des Risikotransfers abgeraten, da hier getroffene Maßnahmen keinen Einfluss auf die Aufrechterhaltung des Geschäftsbetriebs haben. [51, S. 199ff.]

2.3.1.6 IT-Grundschutz-Profile und KMU im IT-Grundschutz

Ein IT-Grundschutz-Profil ist ein Musterszenario für ein „bestimmtes Anwendungsfeld“, mit dem ein Unternehmen oder eine Behörde den Informationssicherheitsprozess des IT-Grundschutzes mit geringerem Aufwand aufbauen kann. Dieses ist an die Rahmenbedingungen der Branche angepasst und beinhaltet die vom Ersteller des Profils geleisteten Grundlagen in den Schritten des Sicherheitsprozesses. Die IT-Grundschutz-Profile werden auf der Webseite des BSI veröffentlicht. Dazu gehören zum Beispiel Profile für Hochschulen, Kommunalverwaltungen oder Reedereien. [52, S. 5] [53]

Durch die Verwendung eines Grundschutz-Profils können Zeit und Ressourcen bei der Anwendung des IT-Grundschutzes auf die eigene Institution eingespart werden. Weitere Vorteile sind die Vergleichbarkeit der Sicherheitskonzepte innerhalb der Branche und der fachbezogene Sprachgebrauch des Profils, da diese mit Vertretern des Anwendungsbereiches entwickelt werden. [52, S. 6]

Bei der Erstellung eines Grundschutz-Profils wird nach einer Zusammenfassung für das Management der Geltungsbereich des Profils festgelegt. Hier wird die Zielgruppe des Profils beschrieben sowie die gewählte IT-Grundschutz-Vorgehensweise dargelegt. Daran anschließend werden auf den Anwendungsbereich bezogen die IT-Grundschutz-Schritte der Strukturanalyse, Schutzbedarfsfeststellung und der Modellierung verallgemeinert durchgeführt. Hieraus ergibt sich eine Referenzarchitektur mit den passenden IT-Grundschutz-Bausteinen. Die Sicherheitsanforderungen der Bausteine werden auf Relevanz überprüft und für das Anwendungsfeld konkretisiert. Auch neue Anforderungen und spezifische Maßnahmen für einen Baustein können hier ermittelt werden. Sofern ein Zielobjekt nicht mit den Grundschutz-Bausteinen modelliert werden kann, wird eine Risikoanalyse durchgeführt und ein neuer Baustein für die Anwender des Grundschutz-Profils ergänzt. Genauso muss eine Risikoanalyse bei erhöhtem Schutzbedarf durchgeführt werden. [52]

Nach Angaben des BSI ist der IT-Grundschutz sowohl für kleine als auch für große Institutionen geeignet. Neben den IT-Grundschutz-Profilen bietet auch die Modernisierung des IT-Grundschutzes von den BSI-Standards 100-1 bis 100-4 auf die Standards 200-1 bis 200-4 einen für KMU verbesserten Sicherheitsprozess. Mit der Einführung der drei Vorgehensweisen Basis-, Kern- und Standard-Absicherung wird besonders für KMU ein besserer Einstieg in den IT-Grundschutz ermöglicht. So kann an die Institution und deren Ressourcen angepasst, zunächst nur die Basis-Absicherung vollzogen oder die kritischen Geschäftsbereiche mit der Kern-Absicherung gesichert werden. Mit abnehmender Größe der Institution

gestaltet sich der Einsatz des IT-Grundschutzes als eher unpraktikabel. So schreibt das BSI, dass die vollständige Etablierung des IT-Grundschutzes für kleine und Kleinstunternehmen (KKU) meist nicht geeignet ist [47]. [18]

2.3.2 Branchenspezifischer Sicherheitsstandard „Medizinische Versorgung“

Ein branchenspezifischer Sicherheitsstandard, kurz „B3S“, soll Betreiber Kritischer Infrastrukturen dabei unterstützen, ihre Pflichten nach § 8a BSIG einzuhalten. Diese Standards werden von Branchenvertretern nach § 8a Abs. 2 BSIG vorgeschlagen und vom BSI überprüft. Die Pflichten nach § 8a BSIG betreffen den Schutz der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der für die Funktionsfähigkeit Kritischer Infrastrukturen relevanten IT-Systeme, Komponenten und Prozesse, indem der „Stand der Technik“ eingehalten wird. Dafür werden in den Standards auf die jeweilige Branche bezogene Sicherheitsanforderungen definiert. Zur Kritischen Infrastruktur zählen Organisationen bestimmter Bereiche, bei denen die Verletzung der Schutzziele erhebliche Folgen für die Gesellschaft und deren Versorgungssicherheit haben [54]. [30] [55]

Der branchenspezifische Sicherheitsstandard „Medizinische Versorgung“

Der von der Deutschen Krankenhausgesellschaft veröffentlichte branchenspezifische Sicherheitsstandard „Medizinische Versorgung“ (auch „B3S Gesundheit“ genannt) ist speziell an Krankenhäuser gerichtet und bezieht sich auf die Sicherstellung der Informationssicherheit bei der stationären Versorgung von Patienten. Der Standard adressiert neben Krankenhäusern, die als Kritische Infrastruktur gelten, auch Krankenhäuser, die Sicherheitsvorkehrungen nach § 391 SGB V „IT-Sicherheit in Krankenhäusern“ umsetzen müssen. Ein Krankenhaus zählt ab 30.000 vollstationären Fällen pro Jahr zur Kritischen Infrastruktur. [9, S. 8f.]

Da der Standard von und für eine bestimmte Branche entwickelt wurde, ist er in dieser Hinsicht mit den IT-Grundschutz-Profilen vergleichbar. Im Gegensatz zu diesen basiert er jedoch nicht auf der Methodik des IT-Grundschutz, sondern auf den

- ISO-Normen der Reihe 27000 (s. Kap 2.3.4),
- der ISO-Norm 22301 „Betriebliches Kontinuitätsmanagement-System (BKMS)“

sowie den gesundheitsversorgungsspezifischen Normen

- ISO 27799 „Medizinische Informatik – Informationssicherheitsmanagement im Gesundheitswesen bei Verwendung der ISO/IEC 27002“ und
- DIN EN 80001-1:2011-11; VDE 0756-1:2011-11 „Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten – Teil 1: Aufgaben, Verantwortlichkeiten und Aktivitäten“. [9, S. 89]

Aus diesen Standards wird eine Vorgehensweise zum Aufbau eines ISMS und entsprechende Anforderungen abgeleitet. Neben den vier in § 8a BSIG genannten Schutzzielen, definiert und beachtet der Standard die zwei branchenspezifischen Schutzziele „Patientensicherheit“ und „Behandlungseffektivität“. Die „Patientensicherheit“ dient dem Schutz der physischen und psychischen Gesundheit. Bei der Behandlungseffektivität wird das effektive Zusammenwirken von „Prozessen und Informationen zur medizinischen Behandlung“ in den Blick genommen. [9, S. 9f.]

Das Vorgehen bei der Umsetzung des Standards wird nachfolgend beschrieben.

Zunächst muss der Geltungsbereich für das ISMS festgelegt werden. Im Fokus stehen dabei die Bereiche, die für die Erbringung der stationären medizinischen Versorgung notwendig sind. Um den Anwender zu unterstützen, werden branchentypische Systeme aus den Bereichen Informationstechnik, Kommunikationstechnik, Medizintechnik und Versorgungstechnik sowie Anwendungen und Prozesse der stationären Versorgung von der Aufnahme bis zur Entlassung des Patienten beschrieben. Darüber hinaus sollte eine Informationssicherheitsleitlinie entwickelt werden. [9, S. 12ff.]

Der Standard beschreibt allgemeine Anforderungen und Maßnahmen zum Aufbau des ISMS, die von jedem Anwender zu beachten sind. Zu deren Umsetzung müssen Richtlinien und Konzepte erstellt werden. Dazu gehören Anforderungen an die Managementstruktur und die Organisation wie die Planung von Verantwortlichkeiten im Sicherheitsprozess, die Einrichtung einer Kontaktstelle für das BSI, der Umgang mit externen Dienstleistern und das betriebliche Kontinuitätsmanagement. Darüber hinaus werden Anforderungen zur Umsetzung technischer Prozesse wie ein Berechtigungskonzept, Konzepte zur Vorfallserkennung oder ein Kryptografiekonzept gestellt. Andererseits werden die konkreten Objekte des Krankenhauses in einem Risikomanagement betrachtet. Diese wird nachfolgend erläutert. [9, S. 52ff.]

Zuvor werden noch Informationen zur krankenhausspezifischen Gefährdungslage dargelegt. Hier werden allgemeine und IT-spezifische Bedrohungen sowie Schwachstellen aufgelistet. Daraus ergeben sich insgesamt 19 branchenspezifische Gefährdungen. Darüber hinaus wird die Gefährdungslage für krankenhausspezifischen Anwendungen und Technik beschrieben und relevante Schutzziele genannt. Zum Abschluss des Kapitels werden relevante Systeme, Komponenten und Anwendungen aus den Bereichen Informationstechnik, Kommunikationstechnik, Medizintechnik und Versorgungstechnik aufgelistet. [9, S. 30ff.]

Risikomanagement des B3S „Medizinische Versorgung“

Zentrales Element des Standards ist das Risikomanagement. Dazu wird einleitend ein Standardmodell beschrieben. Dieses besteht zunächst aus der Ermittlung der Objekte, die geschützt werden sollen. Anschließend wird die Kritikalität dieser Objekte und Risikoakzeptanzkriterien festgelegt. Daraufhin werden Bedrohungen und Schwachstellen identifiziert

und die Risiken bewertet und behandelt. Im letzten Schritt wird das Risiko kommuniziert und überwacht. [9, S. 43]

Im Rahmen des Risikomanagements stellt der Standard zu erfüllende Anforderungen im Risikomanagementprozess auf. Die Leitungsebene ist für die Steuerung des Prozesses und die Vergabe von Verantwortlichkeiten zuständig. Das Risikomanagement beginnt mit der Ermittlung der Risikoobjekte und der Verantwortlichen für diese. Die in den Kapiteln zum Geltungsbereich und zur branchenspezifischen Gefährdungslage bereitgestellten Informationen zu Systemen und Anwendungen können dabei als Hilfestellung dienen. [9, S. 43f.]

Neben den allgemeinen Schutzzielen werden auch die branchenspezifischen Schutzziele „Behandlungseffektivität“ und „Patientensicherheit“ für die Bewertung der Kritikalität der Risikoobjekte herangezogen. Für diese beiden Schutzziele wird eine qualitative Bewertung mit drei Kategorien vorgeschlagen. [9, S. 45f.]

Die Kritikalität von Systemen der vier Bereiche Informationstechnik, Kommunikationstechnik, Medizintechnik und Versorgungstechnik wird danach bewertet, wie lange ein Ausfall ohne relevante Beeinträchtigung der medizinischen Versorgung hingenommen werden kann. Hierfür gibt es drei Klassen. Ein System der „Klasse 1“ darf nur für kurze Zeit ausfallen, während Systeme der Klassen zwei und drei mittel- bzw. langfristig kompensiert werden können. Diese Klassen sollen später in Risikobewertung zur Priorisierung genutzt werden. [9, S. 50f.]

Im Rahmen der Risikoidentifikation wird der Ansatz des BSI referenziert. Dabei wird mithilfe der elementaren Gefährdungen des IT-Grundschutz-Kompendiums für jedes erhobene Objekt jede elementare Gefährdung betrachtet und geprüft, ob diese für das Objekt relevant ist. Zur Kategorisierung der identifizierten Bedrohungen sollen Bedrohungsprofile abgeleitet werden. Vorgeschlagen werden die Profile „Personen mit Netzzugang“, „Personen mit physischem Zugang“, „technische Bedrohungen“ und „weitere Bedrohungen“. [9, S. 47]

Im Anschluss werden die Risikoobjekte hinsichtlich Eintrittswahrscheinlichkeit und Schadenspotenzial der Risiken unter Berücksichtigung bestehender Maßnahmen bewertet. Diese Einschätzung erfolgt qualitativ und mündet in eine Risikomatrix, deren Felder die verschiedenen Risikoklassen abbilden. Die Priorisierung sollte hier anhand der drei Kritikalitätsklassen vorgenommen werden. [9, S. 47f.]

Zur Behandlung der Risiken werden die Optionen der Risikominderung, -vermeidung und -akzeptanz aufgestellt. Hier werden neue Maßnahmen konzipiert oder Geschäftsstrukturen verändert, um den Auswirkungen der Risiken zu begegnen. Von der Leitungsebene müssen Kriterien für die Akzeptanz von Restrisiken aufgestellt und getroffene Maßnahmen bestätigt werden. [9, S. 49f.]

In Bezug auf die Risikokommunikation und Risikoüberwachung im Krankenhaus sollte die Leitungsebene regelmäßig über die Risikosituation informiert werden und Maßnahmen zur Überwachung bestimmen. [9, S. 50]

Anschließend an den Risikomanagementprozess müssen die Maßnahmen, die sich aus den oben genannten Richtlinien und Konzepten sowie dem Risikomanagement ergeben, umgesetzt werden. Darüber hinaus wird die Bedeutung von Schulungsmaßnahmen herausgehoben. [9, S. 86]

Das ISMS muss regelmäßig evaluiert, weiterentwickelt und überprüft werden. [9, S. 52f.] Ein Nachweis der Umsetzung von Maßnahmen nach BSIG muss alle zwei Jahre erfolgen. [30]

2.3.3 OCTAVE®

Im Folgenden wird zunächst auf den Ansatz von OCTAVE eingegangen und anschließend der OCTAVE-S-Standard im speziellen betrachtet.

2.3.3.1 Konzept der OCTAVE®-Standards

OCTAVE ist ein im Software Engineering Institute der US-amerikanischen Carnegie Mellon University entwickelter Ansatz zum Umgang mit Informationssicherheitsrisiken. OCTAVE steht dabei für „Operationally Critical Threat, Asset, and Vulnerability Evaluation" und beschäftigt sich demnach mit der Bewertung von Assets, Schwachstellen und Bedrohungen, die kritische Auswirkungen auf eine Organisation haben können. Ein Asset ist etwas, das für die Organisation einen Wert hat [56, S. 13]. [57, S. 1]

Die Grundsätze von OCTAVE sind in den „OCTAVE Criteria" beschrieben. Diese umfassen zum Beispiel Anforderungen zu einem interdisziplinären Analyseteam. Die Risikoanalyse sollte selbstgesteuert sein, sodass die Analyseergebnisse von Mitarbeiter innerhalb der Organisation erarbeitet werden. Typische Sicherheitsziele, die Beachtung finden, sind Vertraulichkeit, Integrität und Verfügbarkeit. [58]

OCTAVE stellt nicht technologische, sondern organisatorische Risiken in den Mittelpunkt. Zusammen mit dem Fokus auf die strategische Planung und Sicherheitspraktiken spiegeln sich diese Aspekte in den drei Phasen von OCTAVE wider (s. Abbildung 7). [57, S. 3]

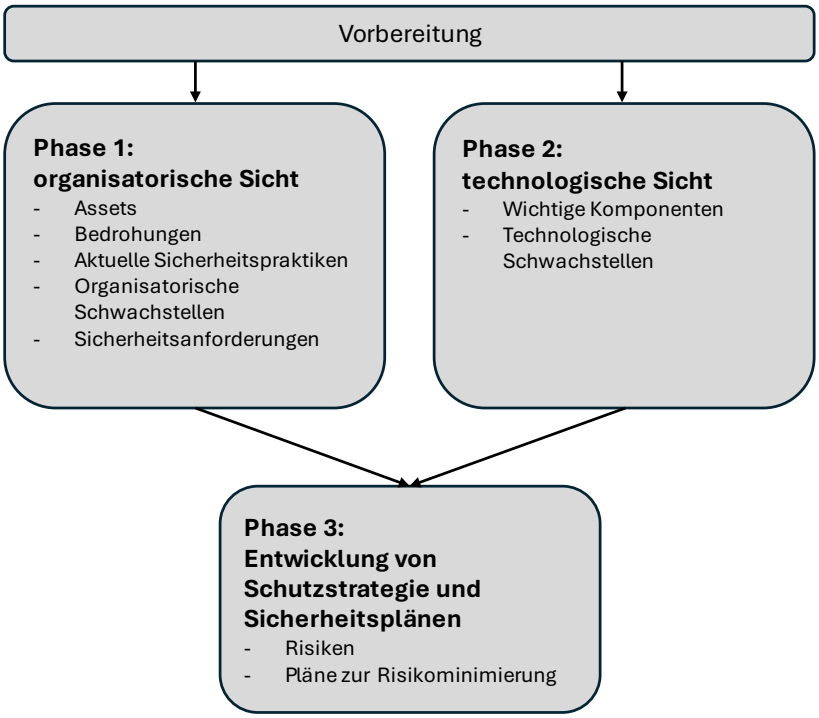

Abbildung 7: Die drei Phasen von OCTAVE (Abbildung nach [57, S. 5])

In der ersten Phase werden die Assets der Organisation und aktuelle Sicherheitsmaßnahmen identifiziert. Anschließend werden für die wichtigsten Assets Sicherheitsanforderungen beschrieben und Bedrohungsprofile für die Assets entwickelt. In der zweiten Phase wird die Infrastruktur der Organisation in den Fokus gerückt und Schwachstellen in dieser identifiziert. In Phase drei werden Risiken für die wichtigen Assets identifiziert und Maßnahmen entwickelt. Letztendlich folgt daraus eine Schutzstrategie und Pläne zum Umgang mit den Risiken. [57, S. 5]

Bei OCTAVE handelt es sich um keinen durchgängigen Managementprozess, der den kompletten PDCA-Zyklus abdeckt. Es werden lediglich Risiken identifiziert und analysiert sowie Schutzstrategien und Maßnahmen geplant. Für die Implementierung, Überwachung und Kontrolle wird ein zusätzlicher Managementrahmen benötigt. [57, S. 8f.]

Implementiert sind diese Kriterien in den Methoden OCTAVE und OCTAVE-S. Deren aktuelle Versionen wurden 2001 und 2005 veröffentlicht [59]. Während OCTAVE an hierarchische Unternehmen mit über 300 Mitarbeitern gerichtet ist, adressiert OCTAVE-S Organisationen mit einer flachen Hierarchie, die bis circa 100 Mitarbeiter haben. Die Phasen stimmen in beiden Ansätzen überein. Unterschiede gibt es in den einzelnen Arbeitsschritten innerhalb der Phasen. [57]

Weitere Veröffentlichungen der OCTAVE-Reihe sind OCTAVE Allegro und OCTAVE Forte. OCTAVE Allegro wurde 2007 veröffentlicht und stellt Informationswerte in das Zentrum der Risikoanalyse [59]. Das 2020 veröffentlichte OCTAVE FORTE betrachtet alle Arten von

Risiken in der Analyse und bezieht die Leitungsebene des Unternehmens mit einem Risikomanagement-Zyklus mehr ein [60].

Im folgenden Kapitel wird das für kleinere Unternehmen konzipierte OCTAVE-S näher beleuchtet.

2.3.3.2 OCTAVE®-S

Wie bereits erwähnt ist OCTAVE-S an kleine Unternehmen bis 100 Mitarbeiter mit begrenzten Ressourcen und einer einfachen IT-Infrastruktur gerichtet. Die Analyse wird hier von einem kleinen Team durchgeführt, das in seiner Zusammensetzung umfassende Kenntnisse von allen Bereichen des Unternehmens hat. Im Vergleich zur OCTAVE-Standardmethode ist OCTAVE-S sehr strukturiert, was die Anwendung für unerfahrene Nutzer vereinfachen soll. [61, S. 3ff.]

Die Dokumentation zu OCTAVE-S umfasst insgesamt zehn Bände, die den Standard erklären. Der erste Band enthält eine Einführung zu OCTAVE und OCTAVE-S. Anschließend werden im zweiten Band Vorbereitungshandlungen beschrieben. Der dritte Band beinhaltet Ausführungen zur OCTAVE-S-Methode, die die genauen Arbeitsschritte bei der Umsetzung der drei OCTAVE-Phasen darlegen. Die darauf folgenden Bände vier bis neun umfassen Arbeitsblätter, mit Hilfe derer die einzelnen Phasen bearbeitet werden. Zum Abschluss wird im zehnten Band die Durchführung der OCTAVE-S-Methode beispielhaft an einer medizinischen Einrichtung aufgezeigt. [62]

Vorbereitungshandlungen

Zur Vorbereitung auf die Evaluation mit OCTAVE-S müssen zunächst einige Voraussetzungen geschaffen werden. Dazu gehören die Unterstützung der Geschäftsleitung und die Zusammenstellung eines Analyseteams. Hier wird auch der Geltungsbereich definiert, die Durchführung geplant sowie Anpassungen des Vorgehens an die eigene Organisation vorgenommen. [63]

Methode des OCTAVE-S

Die in den „OCTAVE Criteria“ definierten Phasen sind in OCTAVE-S in einzelne Prozesse unterteilt, welche wiederum in insgesamt 30 Arbeitsschritte aufgeteilt sind. Tabelle 2 gibt eine Übersicht über die Phasen, Prozesse und deren Inhalte der OCTAVE-S-Methode. [56]

Tabelle 2: Phasen, Prozesse und Aktivitäten von OCTAVE-S (nach [56])

Phase	Prozess	Aktivität
Phase 1: Entwicklung von Asset-basierten Bedrohungsprofilen	Prozess 1: Identifizieren der Informationen der Organisation	P1.1: Kriterien zur Bewertung von Auswirkungen entwickeln
		P1.2: Assets der Organisation ermitteln
		P1.3: Bewertung der Sicherheitspraktiken der Organisation
	Prozess 2: Erstellen von Bedrohungsprofilen	P2.1: Auswahl kritischer Assets
		P2.2: Schutzziele der Assets identifizieren
		P2.3: Bedrohungen für kritische Assets ermitteln
Phase 2: Schwachstellen in der Infrastruktur identifizieren	Prozess 3: Analyse der IT-Infrastruktur in Bezug auf kritische Assets	P3.1: Zugriffswege auf Assets ermitteln
		P3.2: Analyse von technologiebasierten Prozessen in Bezug auf die Assets
Phase 3: Entwicklung von Schutzstrategie und Sicherheitsplänen	Prozess 4: Identifizieren und Analysieren von Risiken	P4.1: Bewertung potentieller Auswirkungen der Bedrohungen
		P4.2: Entwicklung von Kriterien zur Bewertung der Eintrittswahrscheinlichkeit von Bedrohungen (optional)
		P4.3: Eintrittswahrscheinlichkeit der Bedrohungen bewerten (optional)
	Prozess 5: Entwicklung von Schutzstrategie und Plänen zum Umgang mit den Risiken	P5.1: Beschreiben der aktuellen Schutzstrategie
		P5.2: Auswahl von Ansätzen im Umgang mit Risiken
		P5.3: Pläne zum Umgang mit Risiken entwickeln
		P5.4: Auswirkungen auf die Schutzstrategie erheben
		P5.5: weitere Schritte identifizieren

Phase 1: Entwicklung von Asset-basierten Bedrohungsprofilen

Im ersten Prozess der ersten Phase werden zunächst Kriterien zur Bewertung von Auswirkungen entwickelt. Dabei werden für Bereiche wie das Ansehen der Organisation, finanzielle Auswirkungen und rechtliche Folgen Grenzen definiert, um Auswirkungen in die Kategorien Hoch, Mittel und Gering einteilen zu können. Anschließend werden die Assets der Organisation ermittelt. Ein Asset kann eine Information, ein IT-System, Anwendungen oder auch ein Mensch mit seinen Fähigkeiten und seinem Wissen sein. Im letzten Schritt dieses Prozesses werden die bereits bestehenden Sicherheitspraktiken ermittelt und bewertet. Dabei werden strategische und operative Sicherheitsbereiche beachtet. Zu den strategischen Bereichen gehören

- die Schaffung von Bewusstsein für Sicherheit und Schulungen,
- die Sicherheitsstrategie,
- das Sicherheitsmanagement,
- Sicherheitsrichtlinien und Sicherheitsvorschriften,
- das kollaborative Sicherheitsmanagement und
- das Notfallmanagement.

Die operativen Bereiche umfassen

- die physische Zugangskontrolle,
- die Überwachung und Prüfung der physischen Sicherheit,
- die Verwaltung von Netzwerk und Systemen,
- die Überwachung und Prüfung der IT-Sicherheit,
- die Authentifizierung und die Autorisierung,
- das Schwachstellenmanagement,
- die Verschlüsselung,
- die Sicherheitsarchitektur und das Sicherheitsdesign und
- das Management von Vorfällen. [56, S. 9ff.]

Im darauffolgenden Prozess (Tabelle 2, Prozess 2) werden die wichtigsten drei bis fünf Assets ausgewählt. Für diese werden daraufhin relevante Schutzziele identifiziert. Abschließend werden Bedrohungen für jedes Asset ermittelt (Tabelle 2, Prozess 3). Eine Bedrohung hat die Merkmale

- des Assets selbst,
- des Zugriffs (über das Netzwerk oder physisch),
- des Akteurs (Hier stellt sich die Frage, wer oder was die Schutzziele bedroht. Das können zum Beispiel Innentäter oder Außentäter sein genauso wie Hardware-Defekte oder Malware.),
- dessen Motiv (vorsätzlicher oder zufälliger Angriff)
- und die Auswirkung auf die Schutzziele des Assets (Offenlegung, Veränderung, Zerstörung oder Verlust des Assets oder die Unterbrechung des Zugangs).

Mit diesen Merkmalen werden Bedrohungsbäume für die Kategorien

- menschlicher Akteur mit Netzzugang,
- menschlicher Akteur mit physischem Zugang,
- Systemprobleme und
- andere Probleme

erstellt. Dabei sind die Zugriffsart und das Motiv nur für die ersten beiden Bedrohungskategorien relevant. Abbildung 8 zeigt ein Beispiel für einen solchen Bedrohungsbaum. Die Äste der Bäume werden markiert, wenn die Merkmalsausprägung für das Asset eine Bedrohung darstellt. Äste werden im Folgenden "aktiv" genannt, wenn der Pfad bis zum Ende des Baums markiert wird. Diese vier Bedrohungsbäume werden auch Bedrohungsprofile genannt. Das heißt, die Bedrohungen für das Asset werden anhand ihrer Quelle (Netzzugang, physischer Zugang, Systemprobleme oder anderes Problem) in Profile gruppiert. Innerhalb eines Bedrohungsprofils befinden sich mehrere Bedrohungen für das Asset. Zum Beispiel die vorsätzliche Zerstörung des Assets von einem Innentäter mit physischem Zugang gehört zum Profil „menschlicher Akteur mit physischem Zugang“. Auch die ungewollte Offenlegung des Assets durch einen Außentäter mit physischem Zugang gehört zu diesem Bedrohungsprofil. Eine ungewollte Offenlegung des Assets von einem Außentäter über das Netzwerk gehört wiederum zum Bedrohungsprofil „menschlicher Akteur mit Netzzugang“. [56, S. 19ff.]

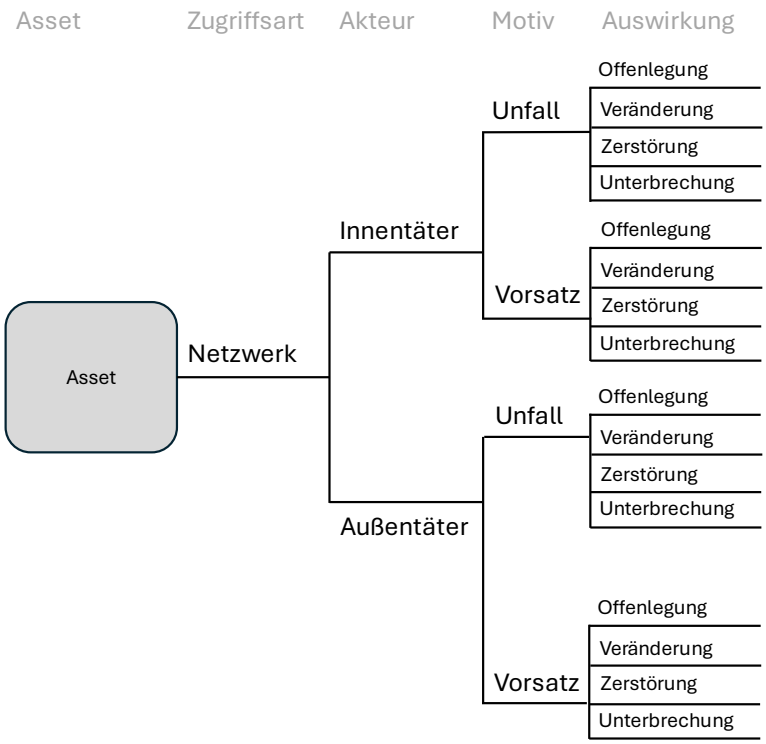

Abbildung 8: Bedrohungsbaum für menschliche Akteure mit Netzzugang (nach [64, S. 12])

Phase 2: Schwachstellen in der Infrastruktur identifizieren

Die zweite Phase besteht aus einem Prozess (Tabelle 2, Prozess 3), in dem die IT-Infrastruktur in Bezug auf die ausgewählten Assets analysiert wird. Dabei werden zunächst die Zugriffswege auf die Assets innerhalb der Infrastruktur der Organisation betrachtet. Dies geschieht, indem das IT-System analysiert wird, das am engsten mit dem Asset verbunden ist. Dies kann zum Beispiel das System sein, auf dem sich das Asset befindet. Diese Systeme werden in Komponentenklassen eingeordnet. Im nächsten Schritt werden die Klassen von Komponenten betrachtet, die für die kritischen Assets identifiziert wurden. Zu diesen Klassen werden die verantwortlichen Personen notiert und die aktuellen Sicherheitsvorkehrungen beim Betrieb der Komponenten bewertet. Abschließend werden in der „Gap-Analyse“ Arbeitsschritte der ersten Phase um die neuen Erkenntnisse ergänzt. [56, S. 31ff.]

Phase 3: Entwicklung von Schutzstrategie und Sicherheitsplänen

Im Rahmen der dritten Phase werden zunächst Risiken identifiziert und analysiert (Tabelle 2, Prozess 4). Dabei werden die zu Beginn entwickelten Kriterien zur Bewertung von Auswirkungen auf die identifizierten Bedrohungen angewendet und diese in die Auswirkungskategorien Gering, Mittel und Hoch eingeordnet. Die beiden darauffolgenden Schritte sind optional. Hier werden Maße für die Eintrittshäufigkeit von Bedrohungen definiert und die Bedrohungen anhand dieser Kriterien ebenfalls in die Kategorien Gering, Mittel und Hoch eingeteilt. Optional sind diese, da einigen Nutzern des Standards die Erfahrung und Daten fehlen könnten, um die Eintrittshäufigkeit einzuschätzen. [56, S. 47ff.]

Der letzte Prozess (Tabelle 2, Prozess 5) besteht aus der Entwicklung der Schutzstrategie und der Pläne zum Umgang mit den Risiken. Im ersten Schritt wird die gegenwärtige Schutzstrategie beschrieben, indem diese für die strategischen und operativen Sicherheitsbereiche abgefragt wird. Eine Schutzstrategie bestimmt allgemein wie die Organisation ihr Sicherheitslevel verbessern und aufrechterhalten will. Anschließend werden Ansätze zum Umgang mit den Risiken ausgewählt. Risiken können akzeptiert, entschärft oder zurückgestellt werden. Eine Entschärfung wird vorgenommen, indem Maßnahmen etabliert werden. Ein zurückgestelltes Risiko wird weiter beobachtet und später erneut bewertet. Hier wird eine Auswahl von circa drei Sicherheitsbereichen vorgenommen, die verbessert werden müssen. Auf diese Bereiche konzentrieren sich die Tätigkeiten zur Behandlung der Risiken. Für die zu entschärfenden Risiken werden nun Pläne entwickelt, mit denen das Risiko für die kritischen Assets reduziert werden soll. Für jeden der ausgewählten Sicherheitsbereiche wird jeweils ein Plan erstellt. Die Maßnahmen werden danach unterschieden, ob sie zu einer Änderung der Schutzstrategie führen oder die aktuelle Schutzstrategie ergänzen. Im darauffolgenden Schritt werden die Auswirkungen des vorherigen Schritts auf die Schutzstrategie erhoben. Zum Abschluss wird das weitere Vorgehen nach der OCTAVE-S-Evaluation geplant. Das umfasst die Umsetzung der Ergebnisse der Evaluation, die Ausweitung der Evaluation um weitere Assets oder Sicherheitsbereiche sowie eine Planung für die nächste Umsetzung von OCTAVE-S. [56, S. 61ff.]

2.3.4 Normen der ISO/IEC-Reihe 27000

Eine Norm legt Anforderungen für Produkte, Dienstleistungen oder Verfahren fest, definiert Begriffe oder gibt Prüfverfahren vor. Mit der Normung soll für ein bestimmtes Thema ein Dokument herausgegeben werden, das basierend auf dem Konsens von Experten „für die allgemeine und wiederkehrende Anwendung Regeln, Leitlinien oder Merkmale für Tätigkeiten oder deren Ergebnisse festlegt“ [65, S. 25]. Eine Norm muss von einer Normungsorganisation angenommen werden. Diese Organisationen bestehen auf internationaler, regionaler und nationaler Ebene. [65]

Die Norm „DIN EN ISO/IEC 27000:2020: Informationstechnik – Sicherheitsverfahren – Informationssicherheitsmanagementsysteme – Überblick und Terminologie“ ist beispielsweise die deutsche Version der ursprünglich vom Technischen Komitee „ISO/IEC JTC 1“ „Information technology“ als „ISO/IEC 27000:2018“ entwickelten Norm. Diese wurde vom Technischen Komitee „CEN/CLC/JTC 13“ „Cybersicherheit und Datenschutz“ und dem nationalen Arbeitskreis „Anforderungen, Dienste und Richtlinien für IT Sicherheitssysteme“ übernommen. Dabei steht „IEC“ für die Internationale Elektrotechnische Kommission, „ISO“ für die Internationale Organisation für Normung und „EN“ für Europäische Norm. „DIN“ ist das Deutsche Institut für Normung. [19, S. 2]

In diesem Kapitel wird zunächst die Normen-Reihe ISO 27000 kurz vorgestellt und anschließend die Norm ISO 27005 “Leitfaden zur Handhabung von Informationssicherheitsrisiken” näher betrachtet.

2.3.4.1 Überblick über die ISO/IEC-Reihe 27000

Die Normen der ISO-Reihe 27000 beschäftigen sich mit dem Aufbau und Betrieb eines ISMS. Dazu werden Anforderungen festgelegt, zu deren Umsetzung allgemeine und branchenspezifische Leitfäden veröffentlicht werden. Die Reihe umfasst eine Vielzahl von Normen, von denen einige im Nachfolgenden erklärt werden. [19]

Die ISO/IEC-Norm 27000 gibt einen Überblick über die Normenfamilie, erläutert wichtige Begriffe und erklärt die Bedeutung und Komponenten eines ISMS. [19]

Die Norm ISO/IEC 27001 beinhaltet allgemeine Anforderungen an Aufbau, Betrieb, Überwachung sowie Aufrechterhaltung und Verbesserung eines ISMS für eine Organisation. Ebenso wird die Umsetzung von Sicherheitsmaßnahmen gefordert und Anforderungen an die Beurteilung und Behandlung von Risiken werden beschrieben. Diese Anforderungen umfassen beispielsweise die Festlegung des Anwendungsbereichs, Aufgaben der Leitungsebene und regelmäßige Verbesserung des ISMS. Auch die Identifizierung, Analyse, Bewertung und Behandlung von Risiken wird hier gefordert. [19, S. 30] [66]

ISO 27002 listet allgemeine Sicherheitsmaßnahmen auf und gibt Informationen zur Umsetzung dieser in einem ISMS. Diese Maßnahmen umfassen die organisatorische, personenbezogene, physische und technische Ebene. [67]

In der ISO/IEC-Norm 27003 wird der Anwender bei der Umsetzung der Anforderungen der ISO/IEC 27001 unterstützt. Sie bietet dazu eine Anleitung zur Implementierung eines ISMS. [19, S. 31]

Die Norm ISO/IEC 27004 nimmt wiederum die Bereiche der Überwachung und Wirksamkeitsüberprüfung des ISMS in den Blick und hilft bei der Umsetzung der entsprechenden Anforderungen der ISO/IEC 27001. [19, S. 32]

Das Risikomanagement in der Informationssicherheit ist das Thema der Norm ISO/IEC 27005. Diese bietet ebenfalls einen Leitfaden zur Umsetzung der Anforderungen der ISO/IEC 27001. [19, S. 32]

Mit Anforderungen, Leitfäden und Richtlinien für Prüfungen und Zertifizierungen beschäftigen sich die Normen ISO/IEC 27006 bis 27008. [19, S. 30ff.]

Darüber hinaus gibt es eine Reihe von branchenspezifischen Normen. Dabei kann beispielhaft die ISO-Norm 27799 genannt werden. Diese gibt aufbauend auf der ISO/IEC 27002 Hilfestellungen zum „Sicherheitsmanagement im Gesundheitswesen“, indem Umsetzungshinweise und Ergänzungen in Hinblick auf diese Branche bereitgestellt werden. [19, S. 37]

2.3.4.2 ISO/IEC 27005

Mit der Norm „DIN EN ISO/IEC 27005 Informationssicherheit, Cybersicherheit und Datenschutz – Leitfaden zur Handhabung von Informationssicherheitsrisiken“ wird dem Anwender eine Hilfestellung zur Umsetzung von Anforderungen der ISO/IEC-Norm 27001 bereitgestellt. Dabei wird auf Anforderungen, die sich mit der Identifikation, Analyse, Bewertung und Behandlung von Informationssicherheitsrisiken beschäftigen sowie daran anknüpfende Anforderungen zum Management eingegangen. Darüber hinaus werden wichtige Begriffe im Bereich des Risikomanagements erläutert. Grundsätzlich ist die Norm für Institutionen jeder Größe anwendbar. [20]

Für diese Arbeit wird der 2024 veröffentlichte Entwurf der Norm betrachtet. Dieser passt die Norm neben einigen Änderungen an die aktuellen Versionen der mit der ISO/IEC 27005 in Relation stehenden Normen an. [20, S. 5]

Als Grundlage für das Informationssicherheitsrisikomanagement dieser Norm dient der allgemeine Risikomanagementprozess der ISO-Norm 31000. Der Managementprozess für Informationssicherheitsrisiken der ISO/IEC 27005 ist in Abbildung 9 zu sehen. [20, S. 15f.]

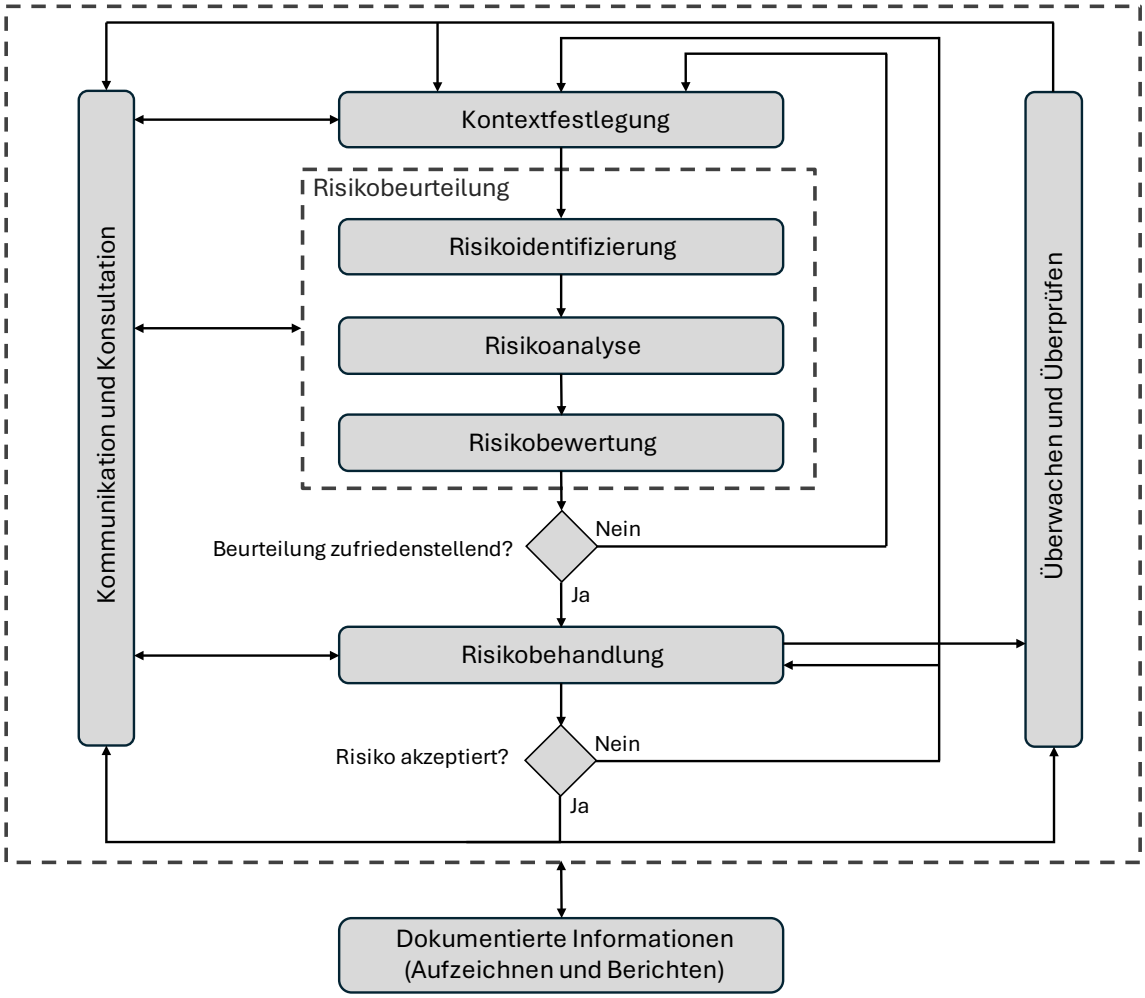

Abbildung 9: Risikomanagementprozess der ISO/IEC 27005 (Abbildung nach [20, S. 16])

Im ersten Schritt muss der Kontext festgelegt werden. Dies umfasst die Organisation und Aufgaben der Unternehmensleitung sowie Verantwortlichkeiten. Neben der ISO-Norm 27001 müssen weitere Normen und Regularien identifiziert werden, die Anforderungen vorgeben. Hier muss auch ein Verfahren für das Risikomanagement gewählt, Risikoakzeptanzkriterien bestimmt und Kriterien für die Risikobeurteilung festgelegt werden. Zu letzteren sind die Folgen, die Eintrittswahrscheinlichkeit und das Risikoniveau zu nennen. [20, S. 18ff.]

Auf die Kontextfestlegung folgt die Risikobeurteilung. Diese umfasst die Identifizierung, Analyse und Bewertung von Risiken. [20, S. 25]

Bei der Risikoidentifizierung müssen Risiken, die die Schutzziele der Vertraulichkeit, Integrität und Verfügbarkeit gefährden, erkannt werden. Diese müssen beschrieben und einem Risikoeigentümer zugeordnet werden. Der Risikoeigentümer ist für das Risiko verantwortlich. Zur Identifizierung von Risiken werden der ereignisbasierte und der wertbasierte Ansatz beschrieben. Während ersterer in den Blick nimmt, wie Risiken auf Grundlage von Ereignissen und deren Folgen beurteilt werden können, werden bei letzterem Risiken auf Basis von Vermögenswerten, Bedrohungen und Schwachstellen beurteilt. [20, S. 26ff.]

Im Anschluss folgt der Schritt der Risikoanalyse. In dieser wird für jedes in der Risikoidentifikation ermittelte Risiko die Folgen und die Eintrittswahrscheinlichkeit bewertet. Aus diesen beiden ergibt sich das Risikoniveau. Die Bewertung kann qualitativ mit Kategorien wie Hoch, Mittel und Gering erfolgen oder quantitativ, indem die Folgen und die Eintrittswahrscheinlichkeit numerisch angegeben werden. Eine dritte Möglichkeit ist das semiquantitative Vorgehen mit Kategorien, denen numerische Werte zugewiesen werden. [20, S. 29ff.]

Die darauffolgende Risikobewertung schließt die Risikobeurteilung ab. In diesem Schritt werden die Risikoakzeptanzkriterien und die Beurteilungskriterien herangezogen, um den weiteren Umgang mit den identifizierten Risiken zu planen. Dazu wird das ermittelte Risikoniveau mit den Kriterien abgeglichen. An dieser Stelle wird auch eine Priorisierung für Risiken vorgenommen, die nicht akzeptiert werden können. Diese müssen der Risikobehandlung unterzogen werden. [20, S. 32f.]

Im Anschluss wird überprüft, ob die Ergebnisse der Risikobewertung akzeptabel sind. Abhängig davon werden die Kontextfestlegung und die Risikobeurteilung wiederholt oder die Risikobehandlung als nächster Prozessschritt durchgeführt. [20, S. 16f.]

Im Rahmen der Risikobehandlung werden Maßnahmen entwickelt, um den Risiken entgegenzuwirken. Als Behandlungsoptionen werden hierbei die Risikovermeidung, die Risikoänderung, die Risikoteilung und die Risikobeibehaltung genannt. Ein Risiko wird vermieden, indem die mit dem Risiko in Verbindung stehende Aufgabe nicht ausgeführt wird. Bei der Risikoänderung werden die Eintrittswahrscheinlichkeit und die Folgen verändert. Teilen kann man ein Risiko mit einer weiteren Partei, zum Beispiel mit einer Versicherung. Bei der Beibehaltung werden Risiken unter einer Abwägung der Vor- und Nachteile zunächst akzeptiert. [20, S. 34f.]

Um mögliche Lücken in den geplanten Maßnahmen zu finden, sollen diese mit dem Maßnahmenkatalog des Anhangs A der ISO/IEC 27001 abgeglichen werden [20, S. 38]. In Behandlungsplänen wird die Umsetzung der Maßnahmen abhängig von der Risikopriorisierung geplant [20, S. 39ff.].

Abschließend muss entschieden werden, ob die Restrisiken akzeptiert werden können. Falls das nicht der Fall ist, beginnt der Risikobehandlungsprozess von vorne. [20, S. 41f.]

Im Rahmen des Risikomanagements müssen einige weitere Managementprozesse beachtet werden. Dazu gehört der Austausch mit relevanten internen und externen Parteien, die in alle Schritte des Risikomanagements eingebunden werden sollen. Auch Aufgaben der Führungsebene und die Bedeutung der Dokumentation der einzelnen Arbeitsschritte werden beleuchtet. Die gesamten Prozesse sollen ständig auf Wirksamkeit und Effizienz überprüft und Veränderungen der Rahmenbedingungen erkannt werden, sodass das Risikomanagement fortlaufend weiterentwickelt wird. [20, S. 43ff.]

2.3.5 STRIDE/DREAD

Bei STRIDE und DREAD handelt es sich um zwei Konzepte aus dem Bereich des Threat Modeling, was mit dem Begriff „Bedrohungsmodellierung“ übersetzt werden kann. Das sind Methoden, mit denen Bedrohungen und Sicherheitsprobleme identifiziert und bewertet werden können. Sie werden häufig bei der Entwicklung von Anwendungen genutzt, können aber auch Netzwerkeebene angewendet werden. Mit diesen Modellen sollen Komponenten einer Anwendung oder eines IT-Systems in Hinblick auf Sicherheitsfragen strukturiert dargestellt und analysiert werden. Auf Basis der identifizierten und bewerteten Bedrohungen müssen im Anschluss Gegenmaßnahmen entwickelt werden. [68] [69]

Bei der Risikoanalyse und dem Threat Modeling gibt es viele Gemeinsamkeiten. So werden beide zum Identifizieren und Bewerten von Risiken beziehungsweise Bedrohungen und Schwachstellen genutzt. Eine Risikoanalyse der vorgestellten Standards hat meist einen größeren Umfang und wird regelmäßig wiederholt, während sich das Threat Modeling detaillierter auf einen bestimmten Bereich konzentriert. [70]

STRIDE wurde 1999 zur Entdeckung von Schwachstellen bei der Entwicklung von Anwendungen bei Microsoft entwickelt. Mit diesem Modell können Bedrohungen anhand von sechs Kategorien identifiziert werden. Die einzelnen Buchstaben von „STRIDE“ stehen für diese Kategorien:

- Spoofing Identitiy: Bei diesen Bedrohungen täuscht der Angreifer vor, etwas oder jemand anderes zu sein als er wirklich ist. So kann er beispielsweise vortäuschen ein anderer Benutzer zu sein, um unbefugt Zugriff zu erhalten.
- Tampering: Dies beschreibt die unbefugte Manipulation von Daten oder Programmcode.
- Repudiation: Bei diesen Bedrohungen kann der Nutzer eine von ihm durchgeführte Handlung abstreiten, ohne dass ihm nachgewiesen werden kann, dass er die Handlung durchgeführt hat.
- Information Disclosure: Bei der Offenlegung von Informationen werden diese für unberechtigte Personen zugänglich gemacht oder an diese weitergegeben.
- Denial-of-Service (DoS): Denial-of-Service-Angriffe haben das Ziel, den Zugang zu einer Anwendung oder einem System für Berechtigte zu unterbinden, indem diese beispielsweise überlastet werden.
- Elevation of Privilege: Hierbei erhöht ein Nutzer seine Rechte in einem System, indem beispielsweise ein Programmierfehler ausgenutzt wird. [71, S. 114ff.]

Die einzelnen Komponenten von Anwendungen oder Netzwerken werden in Diagrammen nachgebildet, die den Datenfluss darstellen. Auf die einzelnen Komponenten des Diagramms wird anschließend STRIDE angewendet und mit den STRIDE-Kategorien Bedrohungen und Schwachstellen gesucht. [71, S. 114ff.] [72]

Bei DREAD handelt es sich ebenfalls um ein Threat-Modeling-Konzept, das von Microsoft entwickelt wurde. Bedrohungen werden hier anhand von fünf Kategorien auf einer Skala von null bis zehn bewertet. Die einzelnen Kategorien sind nachfolgend dargestellt:

- Damage: Dies beschreibt den Gesamtschaden, der durch eine Bedrohung entstehen kann.
- Reproducibility: Dies gibt an, wie einfach der Angriff reproduziert werden kann.
- Exploitability: Die Ausnutzbarkeit beschreibt, wie einfach eine Schwachstelle oder Bedrohung ausgenutzt werden kann.
- Affected users: Dies beschreibt, welche und wie viele Endnutzer betroffen sind.
- Discoverability: Die Entdeckbarkeit gibt an, wie wahrscheinlich es ist, dass ein Angreifer die Bedrohung entdeckt. [73]

Die Bewertungskriterien für die einzelnen Kategorien sind in Tabelle 3 dargestellt.

Tabelle 3: Kriterien zur Bewertung der DREAD-Kategorien [73]

DREAD-Kategorie	Bewertungsgrundlage	Bewertung
Damage (Schaden)	Kein Schaden	0
	Informationen werden offengelegt	5
	Nicht-sensible Daten von Personen werden beeinträchtigt	8
	Nicht-sensible administrative Daten werden beeinträchtigt	9
	Zerstörung des Systems, Verlust der Daten oder Verlust der Verfügbarkeit des Systems	10
Reproducibility (Reproduzierbarkeit)	Fast unmöglich oder schwierig	0
	Komplex	5
	Einfach	7,5
	Sehr einfach	10
Exploitability (Ausnutzbarkeit)	Fortgeschrittene technische Fähigkeiten werden benötigt	2,5
	Verfügbare Tools werden benötigt	5
	Ein Anwendungsproxy wird benötigt	9
	Es wird nur ein Browser benötigt	10
Affected Users (Betroffene Nutzer)	Keine Nutzer sind betroffen	0
	Nur einzelne Nutzer sind betroffen	2,5
	Nur wenige Nutzer sind betroffen	6
	Administrative Nutzer sind betroffen	8
	Alle Nutzer sind betroffen	10
Discoverability (Auffindbarkeit)	Schwer zu entdecken	0
	Kann mit offenen Anfragen entdeckt werden	5
	Ist öffentlich bekannt oder gefunden	8
	Ist leicht aufzufinden	10

Die Ergebnisse der einzelnen Kategorien werden zu einer Gesamtbewertung aufsummiert. Für dieses Gesamtergebnis gibt es letztendlich die vier Kategorien

- Gering bei einer Gesamtbewertung von eins bis zehn,
- Mittel bei einer Gesamtbewertung von elf bis 24,
- Hoch bei einer Gesamtbewertung von 25 bis 39 und
- Kritisch bei einer Gesamtbewertung von 40 bis 50,

um die Kritikalität der Bedrohung zu bestimmen. [73]

Da STRIDE einerseits zur Identifizierung von Bedrohungen genutzt wird und DREAD andererseits zur Bewertung von Bedrohungen können diese kombiniert werden.

3 Vergleich der Konzepte

Die zuvor beschriebenen Standards werden nun verglichen. Dies geschieht einerseits im Hinblick auf ihre KMU-Tauglichkeit. Dazu wird eine von Mark Le Corre entwickelte Methode zur KMU-Tauglichkeitsprüfung angewendet. Andererseits wird das Vorgehen in der Risikoanalyse in den Fokus genommen und die Standards in Bezug auf die einzelnen Schritte der Risikoanalyse verglichen.

3.1 KMU-Tauglichkeit nach Le Corre

Mark Le Corre hat in seiner Bachelorarbeit „Analyse von IT-Notfallmanagement-Standards- und Normen im Kontext von KMU“ [74] eine Methode zur KMU-Tauglichkeitsprüfung für Standards und Normen entwickelt. Seine Methode beachtet die Kriterien der „Vollständigkeit“, „Aufbau“, „Lesbarkeit und Verständlichkeit“, „Wirtschaftlichkeit“ und „Prüfbarkeit der Anforderungen“ und bewertet diese Bereiche mit Punkten, aus denen sich letztendlich ein Prozentwert der KMU-Tauglichkeit ergibt. [74, S. 30ff.]

Zur Entwicklung der Kompatibilitätskriterien für KMU hat er einen Leitfaden zur Erstellung von Normen Europäischer Komitees, ein Positionspapier des Zentralverbands des Deutschen Handwerks sowie Vorgaben zur Normungsarbeit zu Hilfe genommen. [74, S. 30ff.]

Das erste Kriterium beschäftigt sich mit der „Vollständigkeit der Einleitung“. Diese sollte Angaben zum Anwendungsbereich im ersten Kapitel des Dokuments und Verweise auf relevante Standards oder Normen haben, die mit dem Standard in Beziehung stehen. Diese Kriterien werden mittels einer Sichtung des Standards überprüft. [74, S. 35]

Das Kriterium „Aufbau“ stellt Anforderungen an die Übersichtlichkeit, Darstellung eines Versionsverlaufs sowie Nennung von Zielen und Zielgruppen des Standards. Darüber hinaus werden die Erstellungsmotivation und die Möglichkeit, Informationen im Standard schnell zu finden, bewertet. Dies kann mit einem Abgleich der Texte mit den Kriterien erfolgen. [74, S. 36]

Zur Bewertung der „Lesbarkeit und Verständlichkeit“ nimmt die Methode den Flesch-Index von Rudolf Flesch (s. Formel 1) sowie den Flesch-Reading-Ease (FRE) für deutschsprachige Texte von Toni Amstad (s. Formel 2) zur Hand. Diese berechnen die Einfachheit der Lesbarkeit eines Textes auf Basis der durchschnittlichen Länge der Sätze (dLS) und der durchschnittlichen Silbenzahl der Worte (dSW). Ergebnisse der FRE-Berechnung haben Werte zwischen Null und 100, wobei größere Werte auf einen leichter lesbaren Text deuten. In der Bachelorarbeit gibt es keine genauen Angaben zur Bewertung der FRE-Werte. Daher werden im Einklang mit der Bewertung von Herrn Le Corre FRE-Werte unter 20 mit einem

Punkt bewertet, FRE-Werte zwischen 20 und 25 mit zwei Punkten, FRE-Werte zwischen 25 und 30 mit drei Punkten und FRE-Werte über 30 mit vier Punkten. [74, S. 36ff.]

$$FRE = 206{,}835 - (1{,}015 * dLS) - (84{,}6 * dSW)$$

Formel 1: Flesch-Reading-Ease (nach [75], [74, S. 36f.])

$$\boldsymbol{FRE\ (deutsch) = 180 - dLS - (58{,}5 * dSW)}$$

Formel 2: Flesch-Reading-Ease (von Toni Amstad für deutsche Texte) (nach [76], [74])

Weiterhin sind hier Aspekte wie die Erklärung von Abkürzungen, das Vorliegen des Standards in deutscher Sprache, ausreichende Erklärungen und Beispiele sowie die Vermeidung von Querverweisen relevant. [74, S. 36ff.]

Bei der „Wirtschaftlichkeitsprüfung“ werden einerseits die Verfügbarkeit und die Kosten zur Anschaffung des Standards bewertet. Andererseits wird das Vorliegen von vereinfachten Berechnungsmodellen bewertet. In Fragen der Risikoanalyse könnte das die Berechnung von Eintrittswahrscheinlichkeit und Schaden von Risiken betreffen. [74, S. 38ff.]

Abschließend wird die „Prüfbarkeit von Anforderungen“ bewertet. Dies umfasst die Definition des Geltungsbereiches des Standards sowie das Vorliegen von überprüfbaren Anforderungen, die vom Anwender zu erfüllen sind. [74, S. 41]

Tabelle 4 zeigt die Anzahl der Punkte, die für die einzelnen Bereiche vergeben werden können.

Tabelle 4: Aspekte und Punktebereiche der KMU-Tauglichkeitsprüfung nach Le Corre [74, S. 45]

Kompatibilitätskriterien	**Aspekt**	**Punktebereich**
Vollständigkeit	- Die im Anwendungsbereich genannten Inhalte sind vollständig	- 0, 4
Aufbau	- Erstellungsmotivation - Benennung Normenziel sowie Zielgruppe - relevante Informationen schnell auffindbar - nachvollziehbare Versionsänderungen	- 0, 4 - 0, 2, 4 - 1 bis 4 - 0, 4

Lesbarkeit und Verständlichkeit	- leichte Lesbarkeit - Abkürzungen sind erklärt - Nutzung von Beispielen, weiteren Erklärungen oder Veranschaulichungen - Vermeidung von Querverweisen innerhalb der Normen - Vermeidung von Verweisungen auf andere Normen, ggf. Text zitieren - deutsche Sprache	- 1 bis 4 - 0, 4 - 1 bis 4 - 1 bis 4 - 1 bis 4 - 0, 4
Wirtschaftlichkeit	- Normen-Zugänglichkeit - Verhältnismäßigkeit der entstehenden Kosten durch Normeinführung - vereinfachte Rechenverfahren verwenden	- 0, 4 - 1 bis 4 - 0, 4
Prüfbarkeit der Anforderungen	- Definierter Anwendungsbereich - Anforderungen als Leistungsmerkmale ausgedrückt	- 0, 4 - 0, 4

Bei der Anwendung der Methode werden, wenn nötig, weitere Differenzierung bei der Punktevergabe vorgenommen und beispielsweise beim Punktebereich „0, 4“ Werte zwischen „0“ und „4“ vergeben.

3.1.1 BSI-Standard 200-3 „Risikoanalyse“

Im Folgenden werden die in dieser Arbeit betrachteten Standards Mit der Methode von Herrn Le Corre bewertet. Begonnen wird mit dem BSI-Standard 200-3.

Vollständigkeit (Bewertung: 4 von 4 Punkten)

Der Anwendungsbereich des Standards wird in den Kapiteln 1.2 „Zielsetzung“ und 1.4 „Adressatenkreis“ genannt. Hier wird beschrieben, wann und wie die Risikoanalyse im Rahmen des IT-Grundschutzes zum Einsatz kommt. Die in Kapitel 1.3 „Abgrenzung, Begriffe und Einordnung in den IT-Grundschutz“ aufgezeigten Schritte der Risikoanalyse werden in den Kapitel vier bis sieben ausgeführt. [3, S. 5ff.] *Bewertung: 4 von 4 Punkten*

Aufbau (Bewertung: 15 von 16 Punkten)

Die Erstellungsmotivation ist direkt zu Beginn des Kapitels 1.2 „Zielsetzung“ zu finden. [3, S. 5] *Bewertung: 4 von 4 Punkten*

Die Zielgruppe des Standards wird in Kapitel 1.4 „Adressatenkreis“ genannt. Die Ziele des Standards werden wiederum in Kapitel 1.2 „Zielsetzung“ beschrieben. [3, S. 5ff.] *Bewertung: 4 von 4 Punkten*

Der Standard hat ein Inhaltsverzeichnis und ein Literaturverzeichnis, die beim finden relevanter Informationen helfen. Einige Begriffe werden im Kapitel 1.3 „Abgrenzung, Begriffe und Einordnung in den IT-Grundschutz“ erklärt. Ein eigenständiges Verzeichnis, das Begriffe oder Abkürzungen erklärt, ist nicht vorhanden. Kapitel 1.3 zeigt ebenfalls die einzelnen Schritte der Risikoanalyse auf und verweist auf die jeweiligen Kapitel. [3, S. 6] *Bewertung: 3 von 4 Punkten*

Der Versionsverlauf des Standards ist in Kapitel 1.1 „Versionshistorie“ zu finden. [3, S. 5] *Bewertung: 4 von 4 Punkten*

Lesbarkeit und Verständlichkeit (Bewertung: 15 von 24 Punkten)

Zur Bestimmung der Sätze, Wörter und Silben im Standard wird die Webseite „https://wordcount.com/de/syllable-counter“ [77] genutzt. Für den BSI-Standard ergeben sich daraus 484 Sätze, 9354 Wörter und 21316 Silben. Mit 19,3 Wörtern pro Satz und 2,3 Silben pro Wort liegt der deutsche FRE-Wert nach Amstad bei 27,4. *Bewertung: 3 von 4 Punkten*

Der Standard hat kein Abkürzungsverzeichnis und beinhaltet insgesamt wenige Abkürzungen. Manche Abkürzungen wie „C“, „I“ und „A“ für die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit werden erklärt, andere wie „ISMS“ werden nicht erklärt. *Bewertung: 1 von 4 Punkten*

Der Standard hat in nahezu jedem Kapitel Hinweise oder Beispiele. Die Beispiele sind in Form von Tabellen und Abbildungen dargestellt und beschreiben die einzelnen Schritte der Risikoanalyse für ein fiktives Musterunternehmen. *Bewertung: 4 von 4 Punkten*

Im Standard gibt es 18 Querverweise auf Kapitel, Tabellen, Abbildungen und Beispiele bei 53 Textseiten. *Bewertung: 1 von 4 Punkten*

Da der BSI-Standard 200-3 nur ein Standard der IT-Grundschutz-Reihe ist, wird auf weitere Standards dieser verwiesen. Von diesen werden insgesamt vier erwähnt. Darüber hinaus wird auf drei ISO-Normen verwiesen. *Bewertung: 2 von 4 Punkten*

Der Standard ist in der deutschen Sprache verfügbar. *Bewertung: 4 von 4 Punkten*

Wirtschaftlichkeit (Bewertung: 8 von 12 Punkten)

Der Standard kann auf der Webseite des BSI [78] heruntergeladen werden. *Bewertung: 4 von 4 Punkten*

Der Standard kann kostenlos heruntergeladen werden. *Bewertung: 4 von 4 Punkten*

Der Standard enthält keine Berechnungsmodelle zur Bestimmung des Risikos. Stattdessen setzt er zur Reduktion der Komplexität auf eine qualitative Betrachtung der Risiken. [3, S. 26] *Bewertung: 0 von 4 Punkten*

Prüfbarkeit der Anforderungen (Bewertung: 8 von 8 Punkten)

Der Anwendungsbereich wird in der Einleitung definiert. *Bewertung: 4 von 4 Punkten*

In Bezug auf Anforderungen, die als Leistungsmerkmale ausgedrückt werden sollen, nennt der Standard die Schritte der Risikoanalyse und erklärt, wie diese durchgeführt werden sollen. In der Phase „Erstellung einer Gefährdungsübersicht“ ist beispielsweise eine Liste von Gefährdungen angegeben, deren Relevanz für das Risikoobjekt geprüft werden muss. Bei der Konsolidierung des Sicherheitskonzepts werden Aspekte genannt, die beachtet werden müssen. *Bewertung: 4 von 4 Punkten*

3.1.2 B3S „Medizinische Versorgung“

Im Nachfolgenden werden die Kriterien auf den B3S „Medizinische Versorgung“ angewendet. In der Arbeit von Herrn Le Corre wird dieser bereits in der Version 1.1 untersucht. In dieser Arbeit wird die Version 1.2 betrachtet.

Vollständigkeit (Bewertung: 3 von 4 Punkten)

Im Gegensatz zur Version 1.1 beschreibt der B3S Gesundheit den Anwendungsbereich des Standards im ersten Kapitel nach dem Vorwort, genauer in den Kapiteln 2.2 „Grundlegendes zur Anwendung des B3S“ und 2.2.1 „Anwendungsbereich des B3S“. Die Ausführungen zum Anwendungsbereich befinden sich weiterhin nicht, wie gefordert, im ersten Kapitel. Sie befinden sich nun aber an einer früheren Stelle im Standard und werden weiter ausgeführt. *Bewertung: 3 von 4 Punkten*

Aufbau (Bewertung: 10 von 16 Punkten)

Wie bereits von Herrn Le Corre beschrieben, sind im Vorwort und im Kapitel „Branchenspezifischer Sicherheitsstandard (B3S) für die medizinische Versorgung“ Information zur Erstellungsmotivation zu finden. In Version 1.2 des Standards werden diese weiter ausgeführt. *Bewertung: 3 von 4 Punkten*

Das Ziel und die Zielgruppe des Standards werden in Kapitel 2.1 „Zielsetzung und Adressaten des B3S“ beschrieben. Er richtet sich an Krankenhäuser, die als Kritische Infrastruktur gelten, und an kleinere Krankenhäuser mit dem Ziel der Absicherung nach § 391 SGB V. [9, S. 8] *Bewertung: 4 von 4 Punkten*

Das Inhaltsverzeichnis und das Glossar helfen beim schnellen Finden von Informationen. Da sich die Kapiteleinleitungen im Vergleich zur vorherigen Version nicht grundlegend

geändert haben, wird die Bewertung von Herrn Le Corre übernommen. *Bewertung: 3 von 4 Punkten*

Es ist lediglich die aktuelle Version des Standards auf dem Deckblatt angegeben. Eine Auflistung der bisherigen Versionen des Standards liegt nicht vor. *Bewertung: 0 von 4 Punkten*

Lesbarkeit und Verständlichkeit (Bewertung: 16 von 24 Punkten)

Der Text des Standards wird ab dem Vorwort ohne Kopf- und Fußzeile auf der Seite „https://wordcount.com/de/syllable-counter“ eingelesen. Das Tool kommt auf eine Anzahl von 1163 Sätzen, 23009 Wörtern und 55069 Silben. Daraus ergeben sich ca. 19,8 Wörter pro Satz und ca. 2,4 Silben pro Wort. Der daraus berechnete deutsche FRE-Wert zur Lesbarkeit ist mit 20,2 geringer als der von Herrn Le Corre berechnete Wert für die Version 1.1. Gründe dafür könnten, neben Änderungen im Text, die unterschiedlichen Einlese-Tools sein. *Bewertung: 2 von 4 Punkten*

Im B3S verwendete Abkürzungen wie „ISMS“ werden erklärt. Im Kapitel „Glossar“ werden einige Abkürzungen erklärt und definiert. Es gibt jedoch kein Abkürzungsverzeichnis, das alle Begriffe umfasst. *Bewertung: 2 von 4 Punkten*

Der Standard enthält einige Beispiele und Veranschaulichungen. Im Vergleich zur Vorgängerversion gibt es vier statt fünf Abbildungen. Die Tabelle ist weiterhin vorhanden. Da es in diesem Aspekt keine grundlegenden Änderungen gab, wird die Bewertung übernommen. *Bewertung: 3 von 4 Punkten*

Insgesamt gibt es im Standard sieben Verweise mit „siehe“ oder „vgl.“. *Bewertung: 3 von 4 Punkten*

Andere Normen und Standards werden besonders in den ersten Kapiteln erwähnt. Im weiteren Verlauf gibt es zahlreiche Verweise auf Normen und Standards am Seitenrand. Erwähnt wird hier der IT-Grundschutz sowie einige ISO-Normen. In der „Übersicht der referenzierten Normen und Standards“ sind acht Normen aufgelistet. *Bewertung: 2 von 4 Punkten*

Der Standard ist in deutscher Sprache geschrieben. *Bewertung: 4 von 4 Punkten*

Wirtschaftlichkeit (Bewertung: 8 von 12 Punkten)

Die Deutsche Krankenhausgesellschaft bietet den Standard online an [79]. *Bewertung: 4 von 4 Punkte*

Das Herunterladen des Standards ist kostenfrei möglich. *Bewertung: 4 von 4 Punkten*

Der Standard beinhaltet keine Berechnungsmodelle. Risiken werden hier qualitativ mit der Einteilung in Klassen bestimmt. *Bewertung: 0 von 4 Punkten*

Prüfbarkeit der Anforderungen (Bewertung: 8 von 8 Punkten)

Die Definition des Anwendungsbereiches befindet sich im zweiten Kapitel. In Kapitel 2.2 „Grundlegendes zur Anwendung“ ist dieser dargelegt. *Bewertung: 4 von 4 Punkten*

Im B3S Gesundheit werden Anforderungen als Leistungsmerkmale ausgedrückt. In weiten Teilen des Standards werden klare Anforderungen gestellt, die vom Anwender erfüllt oder geprüft werden müssen. *Bewertung: 4 von 4 Punkten*

3.1.3 OCTAVE-S

Nachfolgend wird die Methode auf den OCTAVE-S-Standard angewendet.

Vollständigkeit (Bewertung: 3 von 4 Punkten)

Der Anwendungsbereich wird im ersten Band im ersten Kapitel beschrieben. In diesem Band gibt es jedoch noch ein weiteres Kapitel, das sich mit dem Anwendungsbereich beschäftigt. Daher kann nicht die volle Punktzahl vergeben werden. Die hier eingeführte Methode wird im dritten Band genau beschrieben. Die Bände vier bis neun umfassen die dazugehörigen Arbeitsblätter. *Bewertung: 3 von 4 Punkten*

Aufbau (Bewertung: 12 von 16 Punkten)

Die Motivation des Standards wird bereits in der Inhaltsangabe genannt und im ersten Band weiter ausgeführt. *Bewertung: 4 von 4 Punkten*

Bereits in der Inhaltsangabe werden Ziel und Zielgruppe des Konzepts genannt. Dies wird im ersten Band weiter ausgeführt. Hier werden Ergebnisse, zu denen die Anwendung führen soll und Voraussetzungen für die Anwendbarkeit auf die eigene Institution genannt. [61, S. 1ff.] *Bewertung: 4 von 4 Punkten*

Der Standard besteht aus zehn Bänden, die jeweils eigene Inhaltsverzeichnisse haben. es sind keine Verzeichnisse für Abkürzungen oder Begriffe vorhanden. Abkürzungen werden erklärt. Fachbegriffe werden im dritten Band jeweils am Beginn einzelner Unterabschnitte definiert. *Bewertung: 1 von 4 Punkten*

Beim betrachteten Standard handelt es sich um die Version 1.0. Die Vorgängerversion 0.9 wird erwähnt. Änderungen zu dieser werden ebenfalls erwähnt. Ein Versionsverlauf ist nicht Teil des Standards. *Bewertung: 3 von 4 Punkten*

Lesbarkeit und Verständlichkeit (Bewertung: 14 von 24 Punkten)

Der Text der ersten drei Bände sowie die Beschreibungen des Beispielszenarios werden ohne Kopf- und Fußzeile auf der Seite „https://wordcount.com/de/syllable-counter“ eingelesen. Die Anzahl der Sätze beträgt 1491, die der Wörter 29600 und die der Silben 48958.

Mit 19,9 Wörtern pro Satz und 1,9 Silben pro Wort liegt der FRE-Wert für die englische Sprache bei 28,0. *Bewertung: 3 von 4 Punkten*

Verwendete Abkürzungen werden in der Regel erklärt. Es gibt jedoch kein Abkürzungsverzeichnis. *Bewertung: 2 von 4 Punkten*

Im letzten Band ist ein Anwendungsbeispiel für den kompletten OCTAVE-S-Standard zu finden. Auch in den einzelnen Arbeitsschritten sind teilweise Beispiele angegeben. Insgesamt sind nur zwei Abbildungen im Standard ausgewiesen. In der Methodenbeschreibung und den Arbeitsblättern gibt es jedoch weitere Darstellungen mit veranschaulichendem Charakter. *Bewertung: 4 von 4 Punkten*

Die einzelnen Arbeitsschritte verweisen auf die jeweiligen Arbeitsblätter. Auch in vorherigen Kapitel wird dreimal auf ein anderes Kapitel verwiesen. *Bewertung: 1 von 4 Punkten*

Im Standard wird lediglich auf einen Standard und drei weitere Dokumente der OCTAVE-Reihe verwiesen. Diese Verweise sind lediglich in den ersten beiden Bänden zu finden. *Bewertung: 4 von 4 Punkten*

Der Standard ist in nur englischer Sprache verfügbar. *Bewertung: 0 von 4 Punkten*

Wirtschaftlichkeit (Bewertung: 8 von 12 Punkten)

Der „OCTAVE-S Implementation Guide, Version 1.0” [62] kann auf der Seite der Carnegie Mellon University heruntergeladen werden. *Bewertung: 4 von 4 Punkten*

Das Herunterladen des Standards ist kostenlos möglich. *Bewertung: 4 von 4 Punkten*

Der Standard beinhaltet keine Berechnungsmodelle für Risiken. Auch in den optionalen Schritten zur Wahrscheinlichkeitsbestimmung von Bedrohungen wird nur eine qualitative Bewertung vorgenommen. *Bewertung: 0 von 4 Punkten*

Prüfbarkeit der Anforderungen (Bewertung: 8 von 8 Punkten)

Der Anwendungsbereich wird im ersten Band definiert. Dem Anwender werden klare Anhaltspunkte dafür gegeben, ob der OCTAVE-S für seine Organisation geeignet ist. *Bewertung: 4 von 4 Punkten*

Der Standard nennt Ziele und Ergebnisse, welche mit seiner Anwendung erreicht werden sollen und überprüft werden können. In den einzelnen Phasen werden Schritte zur Erreichung dieser Ziele erklärt. Hier werden ebenfalls immer wieder überprüfbare Aspekte genannt. *Bewertung: 4 von 4 Punkten*

3.1.4 ISO/IEC 27005

Nachfolgend wird die Methode auf den Entwurf der Norm DIN EN ISO/IEC 27005 aus dem Jahr 2024 angewendet.

Vollständigkeit (Bewertung: 4 von 4 Punkten)

Der Anwendungsbereich der Norm ist im ersten Kapitel beschrieben. Dieser umfasst einen Leitfaden zur Umsetzung von Anforderungen aus der ISO/IEC 27001 bezüglich Informationssicherheitsrisiken und ein Vorgehen zur Handhabung von Informationssicherheitsrisiken [20, S. 8]. *Bewertung: 4 von 4 Punkten*

Aufbau (Bewertung: 15 von 16 Punkten)

Die Erstellungsmotivation der Norm ist in der Einleitung beschrieben. *Bewertung: 4 von 4 Punkten*

Die Zielgruppe der Norm ist ebenfalls in der Einleitung zu finden. Dabei handelt es sich um Organisationen, die Anforderungen der ISO/IEC 27001 umsetzen möchten, oder allgemein Personen, die in das Risikomanagement in der Informationssicherheit eingebunden sind. Darüber hinaus ist im Kapitel 1 „Anwendungsbereich“ angegeben, dass sich die Norm an Organisationen jeder Art und Größe richtet. Auch das Ziel der Norm ist hier angegeben. [20] *Bewertung: 4 von 4 Punkten*

Zum schnellen Auffinden von Informationen gibt es ein Inhaltsverzeichnis, Verzeichnisse für Bilder und Tabellen sowie ein Kapitel, in dem Begriffe erläutert werden. Darüber hinaus gibt es ein Kapitel, das den Aufbau der Norm beschreibt. *Bewertung: 4 von 4 Punkten*

Die Vorgängerversion, die von der Norm ersetzt werden soll, wird erwähnt. Auch Änderungen zu dieser Version werden aufgelistet. Eine Übersicht, die mehrere Vorgängerversionen einschließt, ist nicht vorhanden. *Bewertung: 3 von 4 Punkten*

Lesbarkeit und Verständlichkeit (Bewertung: 15 von 24 Punkten)

Die ISO-Norm wird ebenfalls auf der Seite „https://wordcount.com/de/syllable-counter“ eingelesen. Dabei wird mit dem Vorwort begonnen und die Anhänge mit einbezogen. Nach Angaben der Seite hat die Norm 873 Sätze, 21024 Wörter und 48958 Silben. Sie hat damit etwa 19,8 Wörter pro Satz und 2,4 Silben pro Wort. Der sich daraus ergebende deutsche FRE-Wert ist 19,7. *Bewertung: 1 von 4 Punkten*

In der Norm sind generell wenige Abkürzungen zu finden. Vorhandene Abkürzungen werden erklärt. Ein Abkürzungsverzeichnis ist nicht Teil der Norm. *Bewertung: 2 von 4 Punkten*

Die Norm umfasst sechs Abbildungen und 13 Tabellen, die mit Beispielen und Veranschaulichungen eine Hilfestellung liefern. Die meisten dieser befinden sich im 20-setigen Anhang. *Bewertung: 4 von 4 Punkten*

In der Norm sind acht Querverweise mit „siehe“ vorhanden. *Bewertung: 3 von 4 Punkten*

Auf andere Normen wird im Vorwort, in der Einleitung, im ersten Kapitel „Anwendungsbereich“, im zweiten Kapitel „Normative Verweisungen“ und im dritten Kapitel „Begriffe“ verwiesen. Im fünften Kapitel („Handhabung von Informationssicherheitsrisiken“) wird auf ISO 31000 verwiesen. In den folgenden Kapiteln wird jeweils Bezug auf die entsprechenden Anforderungen der ISO 27001 genommen. Im Literaturverzeichnis werden elf Normen aufgezählt. *Bewertung: 1 von 4 Punkten*

Die Norm ist in deutscher Sprache verfügbar. *Bewertung: 4 von 4 Punkten*

Wirtschaftlichkeit (Bewertung: 9 von 12 Punkten)

Die Norm kann bei DIN Media im Webshop käuflich erworben werden. [80] *Bewertung: 4 von 4 Punkten*

Die Norm kostet im Webshop von DIN Media am 13.08.2024 als PDF 175,20 Euro. [80] *Bewertung: 1 von 4 Punkten*

Im Anhang der Norm werden Ansätze zur quantitativen Risikobestimmung aufgezeigt. Hier wird eine einfache Multiplikation von Wahrscheinlichkeit mit Folgen zur Bestimmung des Risikos und logarithmische Skalen als Beispiele genannt. *Bewertung: 4 von 4 Punkten*

Prüfbarkeit der Anforderungen (Bewertung: 8 von 8 Punkten)

Der Anwendungsbereich wird im ersten Kapitel der Norm definiert. Bewertung: *4 von 4 Punkten*

Die Anforderungen werden in der Norm als Leistungsmerkmale ausgedrückt. Für die in der ISO-Norm 27001 gestellten Anforderungen werden konkret auszuführende Aktionen beschrieben und eine Anleitung zur Ausführung dieser Schritte gegeben. Es werden überprüfbare Kriterien und Ergebnisse für die einzelnen Schritte der Norm genannt. *Bewertung: 4 von 4 Punkten*

3.1.5 Ergebnisse

In Tabelle 5 sind die Ergebnisse der KMU-Tauglichkeitsprüfung nach Le Corre aufgelistet. Das beste Ergebnis konnte die ISO/IEC-Norm 27005 mit 79,7 Prozent erreichen. Kurz darauf folgt der BSI-Standard 200-3 mit 78,1 Prozent. Die geringste KMU-Kompatibilität nach Le Corre weisen der B3S „Medizinische Versorgung“ und der OCTAVE-S auf. Bei letzterem ist zu beachten, dass dieser nur in der englischen Sprache verfügbar ist. Im Vergleich zur KMU-Tauglichkeitsprüfung der Version 1.1 des B3S „Medizinische Versorgung“ mit dem Ergebnis von 68,75 Prozent, erzielt der Standard bei der Prüfung der Version 1.2 mit 70,3 Prozent ein leicht besseres Ergebnis [74, S. 57]. Eine Berechnung des Risikos wird nur in der ISO-Norm beschrieben. Die anderen Standard behandeln Risiken qualitativ.

Tabelle 5: Ergebnisse der KMU-Tauglichkeitsprüfung für die Risikoanalyse-Standards

	Aspekte	**BSI 200-3**	**B3S**	**OCTAVE-S**	**ISO 27005**
Vollständigkeit der Einleitung	Die im Anwendungsbereich genannten Inhalte sind vollständig	4	3	3	4
Aufbau	Erstellungsmotivation	4	3	4	4
	Benennung Normenziel sowie Zielgruppe	4	4	4	4
	relevante Informationen schnell auffindbar	3	3	1	4
	nachvollziehbare Versionsänderungen	4	0	3	3
Lesbarkeit und Verständlichkeit	leichte Lesbarkeit	3	2	3	1
	Abkürzungen sind erklärt	1	2	2	2
	Nutzung von Beispielen, weiteren Erklärungen oder Veranschaulichungen	4	3	4	4
	Vermeidung von Querverweisen innerhalb der Normen	1	3	1	3
	Vermeidung von Verweisungen auf andere Normen, ggf. Text zitieren	2	2	4	1
	deutsche Sprache	4	4	0	4
Wirtschaftlichkeit	Normen-Zugänglichkeit	4	4	4	4
	Verhältnismäßigkeit der entstehenden Kosten durch Normeinführung	4	4	4	1
	vereinfachte Rechenverfahren verwenden	0	0	0	4
Prüfbarkeit der Anforderungen	Definierter Anwendungsbereich	4	4	4	4
	Anforderungen als Leistungsmerkmale ausgedrückt	4	4	4	4
	Gesamt (von 64)	**50**	**45**	**45**	**51**
	KMU-Tauglichkeit	**78,1 %**	**70,3 %**	**70,3 %**	**79,7 %**

3.2 Vergleich der Risikoanalysekonzepte

In diesem Kapitel wird das Vorgehen in der Risikoanalyse der einzelnen Standards verglichen. Dazu werden die Ausführungen der Standard in Bezug auf die sieben Schritte

- Vorbereitungshandlungen,
- Ermittlung der Risikoobjekte,
- Identifizieren von Risiken,
- Einschätzen von Risiken,
- Bewerten von Risiken,
- Behandeln von Risiken und
- anschließende Aufgaben

des Risikomanagements analysiert. Beim BSI-Standard und der ISO-Norm wird auf das jeweilige Kapitel verwiesen, beim B3S „medizinische Versorgung“ auf die jeweiligen Anforderungen und bei OCTAVE-S auf die Prozessschritte, die in Tabelle 2 zu sehen sind.

3.2.1 Vorbereitungshandlungen

Dieser Schritt umfasst Maßnahmen zur Vorbereitung auf die Risikoanalyse.

BSI-Standard 200-3

Zur Vorbereitung auf die Risikoanalyse des BSI-Standards (Kap. 2) muss eine Richtlinie verfasst werden. Diese enthält unter anderem Bestimmungen zu Risikoakzeptanzkriterien, Verantwortlichkeiten und Berichtspflichten. [3, S. 10]

B3S „Medizinische Versorgung“

Im B3S Gesundheit werden im Vorfeld einige Festlegungen gefordert. So zum Beispiel die Wahl einer standardisierten Risikoanalyse-Methodik, die konsistent eingesetzt wird (ANF-0190). Auch eine Risikorichtlinie, Bewertungskriterien und Akzeptanzkriterien müssen aufgestellt werden. [9, S. 43ff.]

OCTAVE-S

Im zweiten Band von OCTAVE-S werden die Vorbereitungshandlungen beschrieben. Hervorgehoben werden hierbei die Einholung der Unterstützung der Geschäftsführung, die Zusammenstellung des Analyseteams, die Definition des Anwendungsbereiches und die Durchführungsplanung der Evaluation. [63]

Zur Einschätzung von Auswirkungen und Eintrittswahrscheinlichkeiten von Bedrohungen werden im Standard Kriterien aufgestellt. Zur Bewertung von Auswirkungen (Prozess 1.1) werden Kriterien für die Bereiche Reputation, Gesundheit, gesetzliche Strafen, finanzielle

Auswirkungen, Produktivität und Andere für die Kategorien Gering, Mittel und Hoch aufgestellt. [56, S. 11]

Zur Vorbereitung auf die Bewertung der Eintrittswahrscheinlichkeit von Bedrohungen muss der Anwender Zeitabschnitte bestimmen, in denen ein Eintreten einer Bedrohung als gering, mittel oder hoch eingeschätzt wird (Prozess 4.2). [56, S. 53ff.]

ISO/IEC 27005

Zum Risikomanagement der ISO/IEC 27005 werden einige Maßnahmen zur Vorbereitung und zur Durchführung während des Prozesses genannt. Dazu gehören unter anderem das Aufstellung von Anforderungen interessierter Parteien (Kap. 6.2), die Aufgaben der Unternehmensleitung (Kap. 10.2) und die Dokumentation des Risikomanagements (Kap. 10.4). [20]

Bevor das Risikomanagement durchführt wird, muss ein geeignetes Verfahrens gewählt werden (Kap. 6.5), das durchgängig angewendet wird. Damit soll unter anderem die Vergleichbarkeit zwischen verschiedenen Risiken und verschiedenen Analysezeitpunkten erreicht werden. [20, S. 24f.]

Auch die Aufstellung von Kriterien anhand derer über die Akzeptanz eines Risikos entschieden wird (Kap. 6.4.2), muss in der Vorbereitung erfolgen. Der Standard nennt dazu eine Reihe von Faktoren, die bei der Entwicklung von Kriterien als Hilfestellung dienen können. Im Anhang wird ein Beispiel einer Skala für die Bewertung der Risikoakzeptanz aufgeführt. [20, S. 19ff.]

STRIDE/DREAD

Zur Vorbereitung auf die Bedrohungsmodellierung mit STRIDE/DREAD muss ein Geltungsbereich mit den zu analysierenden Komponenten der Organisation festgelegt werden. Diese Komponenten müssen in einem Datenfluss-Diagramm dargestellt werden. [71]

3.2.2 Ermittlung der Risikoobjekte

Dieser Schritt gibt an, wie die Risikoobjekte ermittelt werden.

BSI-Standard 200-3

Bei den im Rahmen der Risikoanalyse des BSI-Standards 200-3 analysierten Schutzobjekte handelt es sich um Objekte, die bei der Bearbeitung des BSI-Standards 200-2 vorgemerkt werden. Das sind Risikoobjekte mit erhöhtem und sehr hohem Schutzbedarf und Objekte, die nicht mit Bausteinen des IT-Grundschutz-Kompendiums modelliert werden können. Für die restlichen Objekte wurde bereits eine Risikoanalyse durch das BSI durchgeführt, deren Ergebnisse sich in den Bausteinen des IT-Grundschutz-Kompendiums wiederfinden. [3]

B3S „Medizinische Versorgung“

In Kapitel 5.2.1 des Standards wird die Ermittlung von Risikoobjekten (ANF-0193) und die Bestimmung von deren Risikoeigentümern (ANF-0194) gefordert. Unterstützen können dabei die Beschreibung und Auflistung branchentypischer IT-Systeme und Anwendungen. [9, S. 45]

Neben den allgemeinen Schutzzielen der Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität (ANF-0197) werden die branchenspezifischen Schutzziele „Patientensicherheit“ und „Behandlungseffektivität“ etabliert. Mit der „Patientensicherheit“ soll die Gesundheit der Patienten geschützt werden. Die „Behandlungseffektivität“ bezieht sich auf das „zielgerichtete Zusammenwirken“ von Prozessen und Informationen bei der Behandlung von Patienten. Zur Bewertung dieser beiden Schutzziele werden jeweils drei Kategorien vorgegeben. Eine geringe, mittlere oder hohe Gefährdung eines Risikoobjektes liegen jeweils vor, wenn die Beeinträchtigung der Schutzziele sehr unwahrscheinlich, unwahrscheinlich oder wahrscheinlich ist (ANF-0198, ANF-0199). Für die Einschätzung der Anforderungen eines Risikoobjektes in Bezug auf die allgemeinen Schutzziele werden keine Kategorien vorgeschlagen, aber die Einbeziehung der beiden branchenspezifischen Schutzziele gefordert. [9, S. 9] [9, S. 45f.]

OCTAVE-S

Die Ermittlung der Risikoobjekte erfolgt bei OCTAVE-S, indem zunächst IT-Systeme, Informationen und Anwendungen auf dem entsprechenden Arbeitsblatt aufgelistet werden (Prozess 1.2). [56, S. 13f.]

Von diesen werden drei bis fünf kritische Assets ausgewählt (Prozess 2.1) und deren Anforderungen in Bezug auf die Schutzziele Verfügbarkeit, Vertraulichkeit und Integrität bestimmt (Prozess 2.2). Diese Assets werden im weiteren Verlauf des Standard analysiert. [56, S. 21ff.]

ISO/IEC 27005

Die ISO-Norm stellt zwei Ansätze zur Risikoidentifizierung zur Auswahl. Nur einer dieser beiden, der „wertbasierte Ansatz“, stellt Risikoobjekte an den Beginn der Betrachtung und benötigt damit eine Auflistung von Risikoobjekten als Ausgangsbasis. Die Erstellung einer solchen Liste wird in Kapitel 7.2.1 „Identifizierung und Beschreibung von Informationssicherheitsrisiken“ gefordert. [20, S. 26ff.]

STRIDE/DREAD

Die Ermittlung der Risikoobjekte bei STRIDE/DREAD wird bereits bei den Vorbereitungsmaßnahmen beschrieben.

3.2.3 Identifizieren von Risiken

In diesem Schritt werden Risiken identifiziert.

BSI-Standard 200-3

Im BSI-Standard erfolgt die Identifizierung von Risiken (Kap. 4), indem für ein Risikoobjekt alle elementaren Gefährdungen des IT-Grundschutz-Kompendiums geprüft werden. Wenn eine Gefährdung für ein Zielobjekt relevant ist, wird diese notiert. Im Anschluss daran werden zusätzliche Gefährdungen ermittelt. Das Ergebnis ist eine Liste konkreter Gefährdungen für das Risikoobjekt. [3, S. 16ff.]

B3S „Medizinische Versorgung“

Zur Identifikation von Bedrohungen und Schwachstellen verweist der B3S „Medizinische Versorgung“ in der Anforderungen „ANF-0201“ auf den IT-Grundschutz des BSI. Mit dessen „All-Gefahrenansatz“ soll anhand der elementaren Gefährdungen des IT-Grundschutz-Kompendiums Bedrohungen ermittelt werden. Abgesehen von diesem Verweis auf den IT-Grundschutz ist das Vorgehen nicht weiter ausgeführt. Das macht das Heranziehen und Kenntnisse über den IT-Grundschutz des BSI erforderlich. Die daraus ermittelten Bedrohungen sollen anschließend in Gefährdungsprofile gruppiert werden. Als Beispiel werden die Profile „Personen mit Netzzugang“, „Personen mit physischem Zugang“, „technische Bedrohungen“ und „weitere Bedrohungen“ genannt. [9, S. 47]

OCTAVE-S

Im Standard OCTAVE-S werden Bedrohungen für die Assets im zweiten Prozess der ersten Phase ermittelt (Prozess 2.3). Hier werden für Bedrohungen anhand verschiedener Merkmale Bedrohungsbäume entwickelt. Die Äste der Bäume werden markiert, wenn die Merkmalsausprägung für das Asset eine Bedrohung darstellt. Von diesen Bedrohungsbäumen gibt es vier Typen:

- menschlicher Akteur mit Netzzugang,
- menschlicher Akteur mit physischem Zugang,
- Systemprobleme und
- andere Probleme.

Diese vier Gruppen werden auch Bedrohungsprofile genannt. An dieser Stellen werden auch die Stärke des Motivs des Täters und bisherige Erfahrungen mit der Bedrohung abgefragt. [56, S. 25ff.]

Darüber hinaus werden in der zweiten Phase Schwachstellen in der Infrastruktur identifiziert, indem die Zugriffswege auf die Assets innerhalb der Organisation ermittelt und verbundene Systeme in Komponentenklassen eingeordnet werden (Prozess 3.1). [56, S. 33ff.]

ISO/IEC 27005

Die Identifizierung von Risiken (Kap. 7.2) besteht nach der ISO/IEC 27005 aus den Schritten der „Identifizierung und Beschreibung von Informationssicherheitsrisiken“ und der Zuteilung von Verantwortlichen für die Risiken, den Risikoeigentümern. [20, S. 26ff.]

Ziel der Risikoidentifizierung ist eine Liste von Risiken, die die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit betreffen, mit ihren Risikoeigentümern aufzustellen. Die Norm beschreibt dazu zwei Ansätze. Den „wertbasierten Ansatz“ und den „ereignisbasierten Ansatz“. [20, S. 26ff.]

Der wertbasierte Ansatz geht von Risikoobjekten aus, deren Schwachstellen von Bedrohungen ausgenutzt werden können. Auf diese Weise werden Risiken bei diesem Ansatz identifiziert. Im Gegensatz dazu werden beim ereignisbasierten Ansatz Risiken identifiziert, indem Ereignisse und ihre Folgen betrachtet werden. [20, S. 26ff.]

Die Norm stellt weitere Erläuterungen und Beispiele im Hinblick auf beide Ansätze sowie eine Auflistung von typischen Bedrohungen und Schwachstellen im Anhang zur Verfügung. [20, S. 60ff.]

STRIDE/DREAD

Bei STRIDE/DREAD werden Risiken mit den sechs Kategorien von STRIDE identifiziert. Dies geschieht, indem auf die einzelnen Komponenten des Datenfluss-Diagramms die STRIDE-Kategorien angewendet und Bedrohungen und Schwachstellen gesucht werden. Bei den Kategorien handelt es sich um das Vortäuschen der Identität, die Manipulation, die Nichtanerkennung, die Veröffentlichung von Informationen, Denial-of-Service und die Erhöhung von Rechten [81]. [71, S. 114ff.]

3.2.4 Einschätzen von Risiken

Hier werden die Faktoren eingeschätzt, anhand derer später das Risiko bewertet wird.

BSI-Standard 200-3

Die Risikoeinschätzung (Kap. 5.1) erfolgt im BSI-Standard, indem die Eintrittswahrscheinlichkeit und die Schadenshöhe, die von einer Gefährdung ausgeht, eingeschätzt werden. Vorgeschlagen wird ein qualitatives Vorgehen mit jeweils vier Kategorien. Darüber hinaus werden Vor- und Nachteile eines quantitativen Vorgehens beschrieben. [3, S. 26f.]

B3S „Medizinische Versorgung“

Im B3S „Medizinische Versorgung“ werden Risiken anhand der Eintrittswahrscheinlichkeit und dem möglichen Schaden eingeschätzt. Der mögliche Schaden soll qualitativ in Klassen

aufgeteilt werden (ANF-0205). Vorgeschlagen wird eine Einteilung von „gering“ bis „gravierend“ (ANF-0207). Eine Anzahl der Klassen wird nicht vorgeschlagen. [9, S. 47f.]

Die Eintrittswahrscheinlichkeit wird ebenfalls qualitativ eingeschätzt (ANF-0202). Ein Vorschlag für Kategorien der Eintrittswahrscheinlichkeit wird nicht gemacht. Unterstützen bei der Einschätzung können einige Faktoren, die in der „ANF-0209“ aufgeführt werden. Genannt werden hier zum Beispiel Erfahrungen über bisheriger Vorfälle, die eigenen Angriffserkennungsmaßnahmen oder das „Common Vulnerability Scoring System“ (CVSS) zur Einschätzung der erforderlichen Fähigkeiten des Angreifers. [9, S. 47f.]

OCTAVE-S

Die Einschätzung der Auswirkungen der Bedrohungen erfolgt im OCTAVE-S zu Beginn der dritten Phase (Prozess 4.1). Hier werden die Kriterien zur Bewertung von Auswirkungen herangezogen und für jeden aktiven Ast eines Bedrohungsbaumes die Auswirkung Gering, Mittel oder Hoch für die sechs Bereiche der Auswirkungen angeben. [56, S. 49ff.]

Die Einschätzung der Eintrittswahrscheinlichkeit ist optional. Hier wird anhand der zuvor entwickelten Kriterien die Eintrittswahrscheinlichkeit jeder Bedrohung bewertet (Prozess 4.3). [56, S. 57ff.]

Zu den bereits ermittelten Zugriffspfaden und Komponentenklassen von Systemen, die mit den kritischen Assets verbunden sind, werden ebenfalls die Sicherheitsvorkehrungen bewertet (Prozess 3.2). [56, S. 41ff.]

Im Standard werden nicht nur Einschätzungen in Bezug auf die Bedrohungen vorgenommen, sondern auch eine allgemeine Bewertung der Sicherheitspraktiken. Hier wird das Verhalten der Organisation in den insgesamt 15 Sicherheitsbereichen bewertet (Prozess 1.3 und Prozess 5.1). [56, S. 15ff.]

ISO/IEC 27005

In der ISO/IEC-Norm 27005 entsprechen diese Schritte der Beurteilung von potentiellen Folgen (Kap. 7.3.2) und der „Beurteilung der Wahrscheinlichkeit“ von Risiken (Kap. 7.3.3). Diese sind zusammen mit der „Bestimmung des Risikoniveaus“ Teile der Analyse von Risiken (Kap. 7.3) der ISO-Norm. Wie bereits erwähnt unterscheidet sich der Begriff „Risikoanalyse“ in der ISO-Norm von dem anderer deutschsprachiger Standards. [20, S. 29ff.]

Zur Einschätzung der Folgen und der Eintrittswahrscheinlichkeit schlägt die Norm mehrere Möglichkeiten vor. Einerseits eine qualitative Einschätzung mit Kategorien, andererseits ein quantitatives Vorgehen. Bei letzterer werden die Folgen und die Eintrittswahrscheinlichkeit numerisch angegeben. Dies kann zum Beispiel mit den entstehenden Kosten und einer Wahrscheinlichkeit des Auftretens vorgenommen werden. Ein Zwischenweg ist mit dem semiquantitativen Vorgehen möglich. Hierbei werden die qualitativen Kategorien mit numerischen Werten belegt. [20, S. 29ff.]

Als Hilfestellung bietet die Norm eine Vielzahl von Beispielen, Faktoren und Kriterien, die bei der Beurteilung zu beachten sind. Im Anhang werden Beispiele für Kategorien einem qualitativen Vorgehen vorgeschlagen sowie logarithmische Skalen für ein quantitatives Vorgehen. [20]

STRIDE/DREAD

Bei STRIDE/DREAD erfolgt die Einschätzung der Risiken mit den fünf Kategorien von DREAD. Der Schaden, die Reproduzierbarkeit, die Ausnutzbarkeit, betroffene Nutzer und die Auffindbarkeit einer Bedrohung werden nach einem Schema bewertet. Dabei können jeweils Werte von null bis zehn vergeben werden. Die Bewertungskriterien für die einzelnen Kategorien sind in Tabelle 3 zu sehen. [73]

3.2.5 Bewerten von Risiken

Bei der Risikobewertung werden die Faktoren, anhand derer das Risiko bestimmt wird, zu einem Risikowert zusammengefasst.

BSI-Standard 200-3

Die Bewertung des Risikos (Kap. 5.2) erfolgt im BSI-Standard, indem zunächst eine Risikomatrix auf der Basis von Eintrittshäufigkeit und Schadenshöhe der Gefährdung aufgespannt wird. Den Feldern dieser Matrix werden vom Anwender Risikokategorien zugewiesen. Vorgeschlagen werden hier ebenfalls vier Kategorien. Das Risiko ergibt sich also aus der Kombination von Eintrittswahrscheinlichkeit und Schadenshöhe. [3, S. 27f.]

B3S „Medizinische Versorgung“

Der B3S-Standard fordert die Bildung von Risikoklassen und die Erstellung einer Risikomatrix auf der Basis von Eintrittswahrscheinlichkeit und Schadenshöhe (ANF-0210). Die Anzahl und die Zuteilung der Risikoklassen bleibt auch hier dem Anwender überlassen. [9, S. 47f.]

Die Priorisierung der Risikobewertung soll anhand von Kritikalitätsklassen erfolgen (ANF-0203) [9, S. 47]. Systeme werden in drei Klassen kategorisiert, je nachdem wie lange ihr Ausfall kompensiert werden kann, ohne dass die „Medizinische Leistungserbringung“ relevant beeinträchtigt wird. [9, S. 50f.]

Bewertet wird hier demnach, inwieweit die Beeinträchtigung der Verfügbarkeit eines einzelnen Systems einen Einfluss auf die medizinische Versorgung und die kritische Dienstleistung hat.

OCTAVE-S

Im OCTAVE-S-Standard werden in der dritten Phase (Prozess 5.2) Kriterien genannt, anhand derer die Ansätze zur Behandlung der Risiken gewählt werden. Diese Kriterien umfassen die ermittelten Informationen zum Asset, die Bedrohungsprofile, Informationen zur verbundenen Infrastruktur und die Bewertung der Sicherheitspraktiken. Einen Ansatz, der all diese Faktoren oder einen Teil dieser Faktoren in einem Risikowert oder in Risikokategorien zusammenfasst, gibt der Standard nicht vor. Damit bleibt die Gewichtung der einzelnen Faktoren dem Anwender überlassen. [56, S. 76ff.]

ISO/IEC 27005

In der ISO/IEC-Norm 27005 erfolgt die Bewertung der Risiken im Kapitel 7.3.4 „Bestimmung des Risikos“ und im Kapitel 7.4 „Bewertung der Informationssicherheitsrisiken“. [20, S. 32]

Zur Bestimmung des Risikoniveaus sollen die eingeschätzten Folgen und die Eintrittswahrscheinlichkeit herangezogen werden. Auch hier werden Beispiele und Kriterien als Hilfestellung genannt. Bei einem qualitativen Vorgehen werden Risikokategorien vorgeschlagen, die in eine Risikomatrix eingetragen werden können. Für ein Risikoniveau in numerischer Form wird der Erwartungswert der finanziellen Verluste als Kombination von Folgen und Eintrittswahrscheinlichkeit genannt. [20]

Im Kapitel zur Bewertung der Risiken werden diese mit den Risikoakzeptanzkriterien verglichen und für die Risikobehandlung priorisiert. [20, S. 32f.]

STRIDE/DREAD

die Bewertung erfolgt bei STRIDE/DREAD, indem die Ergebnisse für die einzelnen STRIDE-Kategorien aufsummiert werden. Als finale Bewertung wird die Bedrohung in eine der vier Kategorien Gering, Mittel, Hoch oder Kritisch eingeordnet. [73]

3.2.6 Behandeln von Risiken

Dieser Schritt enthält das Vorgehen zur Behandlung von Risiken und nennt Behandlungsoptionen.

BSI-Standard 200-3

Im BSI-Standard werden Risiken in Abhängigkeit von Risikoakzeptanzkriterien und Risikoniveau behandelt. Als Optionen zur Behandlung werden die Reduktion, die Vermeidung, der Transfer und die Akzeptanz von Risiken vorgeschlagen. Je nachdem wie die Risikoakzeptanzkriterien definiert sind und wie hoch das Risikoniveau ist, müssen zur Behandlung Optionen gewählt werden, um das Risikoniveau zu verringern. Der Standard nennt Kriterien, wann welche Behandlungsoption gewählt werden sollte und in welchen Quellen Maßnahmen zur Risikoreduktion zu finden sein könnten. (Kap. 6) [3, S. 33ff.]

B3S „Medizinische Versorgung“

Die Risikobehandlung erfolgt, indem Behandlungsoptionen auf der Basis von Akzeptanzkriterien und Risikoklassen ausgewählt werden (ANF-0212). Als Behandlungsoptionen werden die Minderung, Vermeidung und Akzeptanz von Risiken genannt (ANF-0213). [9, S. 49]

Der Transfer von Risiken wird nicht als Option genannt. Dies liegt daran, dass der Risikotransfer nicht der Erfüllung des Ziels des Standards, also der Aufrechterhaltung der kritischen Dienstleistung, dient. [55]

OCTAVE-S

Zur Behandlung der Risiken werden im OCTAVE-S-Standard die Schritte zur „Auswahl von Ansätzen zum Umgang mit Risiken“ (Prozess 5.2) und die Erstellung von Plänen zum Umgang mit Risiken (Prozess 5.3) aufgeführt. Zur Behandlung werden die Optionen der Risikoakzeptanz, Risikoentschärfung und das Zurückstellen von Risiken bereitgestellt. Diese werden für jeden aktiven Ast des Baums ausgewählt. Die Risiken werden hier aber nicht einzeln behandelt. Es werden vielmehr circa drei Sicherheitsbereiche ausgewählt, mit deren Verbesserung viele Risiken behandelt werden können. [56, S. 75ff.]

Nachdem die Behandlungsansätze für Risiken ausgewählt wurden, werden die Pläne für die gewählten Sicherheitsbereiche zum Umgang mit den Risiken entwickelt. Hierbei werden konkrete Handlungen bestimmt, mit denen die Risiken gemildert und die Sicherheitsbereiche verbessert werden sollen. Für jeden Sicherheitsbereich stellt der Standard eine Liste mit möglichen Maßnahmen bereit. [56, S. 83ff.]

ISO/IEC 27005

Die Behandlung der bewerteten Risiken (Kap. 8) umfasst bei der ISO/IEC-Norm 27005 die Optionen der Vermeidung, Änderung, Beibehaltung und Teilung. Diese entsprechen den vier Behandlungsoptionen des IT-Grundschutzes. Für die zu behandelnden Risiken müssen Optionen ausgewählt und Maßnahmen geplant werden. Als Quellen für Maßnahmen werden der Anhang der ISO-Norm 27001 und branchenspezifische Normen genannt. [20, S. 34ff.]

STRIDE/DREAD

Die Behandlung von Risiken ist nicht direkt Teil von STRIDE oder DREAD. Dazu müssen diese zum Beispiel in ein Risikomanagement oder einen Threat-Modeling-Prozess eingebunden sein.

3.2.7 Anschließende Aufgaben

Dieser Schritt gibt Aufschluss über Aufgaben, die im Anschluss an die Risikoanalyse durchzuführen sind.

BSI-Standard 200-3

Im Anschluss an die Risikoanalyse werden im BSI-Standard neue Sicherheitsmaßnahmen in der Konsolidierungsphase (Kap. 7) überprüft. Dazu werden einige Kriterien genannt, die zu prüfen sind. Im Anschluss daran sind die Schritte des BSI-Standards 200-3 abgeschlossen und der Standard 200-2 wird fortgesetzt. [3, S. 39ff.]

B3S „Medizinische Versorgung“

Im Anschluss an die Behandlungsphase werden im B3S „Medizinische Versorgung“ Risiken kommuniziert und überwacht. Die Leitung des Krankenhauses muss regelmäßig Berichte über die Risikosituation erhalten (ANF-0216). Darin sollen halbjährlich bis jährlich Überwachungsergebnisse, Restrisiken und Entwicklungen der Risiken thematisiert werden. [9, S. 50]

OCTAVE-S

Im Anschluss an die Behandlungsphase werden im OCTAVE-S-Standard Veränderungen der Sicherheitsbereiche dokumentiert (Prozess 5.4). Die abschließenden Schritte der Implementierung der Maßnahmen, Ausweitung der Evaluation um weitere Assets oder Sicherheitsbereiche und der Planung der nächsten Durchführung von OCTAVE-S werden angesprochen (Prozess 5.5), aber nicht konkret begleitet. [56, S. 87ff.]

ISO/IEC 27005

Nach der Auswahl von Behandlungsoptionen steht bei der ISO/IEC 27005 die Aufstellung eines Behandlungsplans an (Kap. 8.6). Dieser umfasst Kriterien und Angaben, die zur Umsetzung der gewählten Risikobehandlungsoptionen relevant sind. Darüber hinaus wird Bedeutung der Risikoeigentümer beim Behandlungsplan und der Umgang mit Restrisiken erwähnt. [20, S. 39ff.]

Weitere Aufgaben, die den Risikomanagementzyklus schließen, umfassen die Kommunikation und Konsultation (Kap. 10.3), Überwachung und Überprüfung (Kap. 10.5), Korrekturmaßnahmen (Kap. 10.7) und die Fortlaufende Verbesserung (Kap. 10.8). Zu diesen Aufgaben werden jeweils Erklärungen zur Umsetzung und zu beachtende Kriterien genannt. [20, S. 45ff.]

STRIDE/DREAD

Weiterführende Schritte müssen bei STRIDE/DREAD im Rahmen eines Risikomanagements oder eines Threat-Modeling-Prozesses durchgeführt werden.

3.2.8 Diskussion und Zusammenfassung

In Tabelle 6 sind die Ergebnisse anhand der Kapitel, Anforderungen und Prozessschritte der Standards zusammengefasst dargestellt. Zu beachten ist, dass die Basis für die einzelnen Schritte anhand derer die Konzepte gegenübergestellt werden der IT-Grundschutz des BSI ist. Sie gilt sowohl für die Struktur als auch die Namen der Risikoanalyseschritte.

Tabelle 6: Vergleich der Risikoanalysekonzepte

Vorbereitungs-handlungen	**BSI 200-3**	**B3S Gesundheit**
	Richtlinie mit Angaben zu Risikoneigung, Risikoakzeptanzkriterien, Verantwortlichkeiten und Berichtspflichten (Kap. 2).	Informations-Risikorichtlinie (ANF-0189) erstellen. Risikoanalyse-Methodik auswählen (ANF-0190). Kriterien zur Bewertung von Risiken aufstellen (ANF-0202). Akzeptanzkriterien für Risiken vorgeben (ANF-0212).
	ISO 27005	**OCTAVE-S**
	Anforderungen interessierter Parteien (Kap. 6.2) Risikoakzeptanzkriterien (Kap. 6.4.2) Wahl des Risikomanagement-verfahrens (Kap. 6.5) Führung und Verpflichtung (Kap. 10.2) Dokumentation (Kap. 10.4)	Band 2: Vorbereitungshandlungen P1.1: Kriterien zur Bewertung von Auswirkungen P4.2: Entwicklung von Kriterien zur Bewertung der Eintrittswahrscheinlichkeit von Bedrohungen
	STRIDE/DREAD	
	Geltungsbereich mit betrachteten Komponenten der Organisation festlegen und Datenfluss-Diagramm erstellen.	
Ermittlung der Risikoobjekte	**BSI 200-3**	**B3S Gesundheit**
	Bei Bearbeitung des BSI-Standards 200-2 vorgemerkte Risikoobjekte.	Risikoobjekte müssen ermittelt werden (ANF-0193).
	ISO 27005	**OCTAVE-S**
	Auflistung von Risikoobjekten wird in Kap. 7.2.1 gefordert.	P1.2: Assets der Organisation ermitteln P2.1: Auswahl kritischer Assets P2.2: Schutzziele der Assets identifizieren
	STRIDE/DREAD	
	Zu analysierende Risikoobjekte werden bei Vorbereitungsmaßnahmen erhoben.	

<table>
<tr><td rowspan="5">Identifizieren von Risiken</td><td>BSI 200-3</td><td>B3S Gesundheit</td></tr>
<tr><td>Ermittlung der Relevanz elementarer Gefährdungen und Ermittlung zusätzlicher Gefährdungen für das Risikoobjekt (Kap. 4)</td><td>Verweis auf All-Gefahrenansatz des BSI-Grundschutzes mit elementaren Gefährdungen und Einteilung in Bedrohungsprofile (ANF-0201).</td></tr>
<tr><td>ISO 27005</td><td>OCTAVE-S</td></tr>
<tr><td>Identifizierung von Informationssicherheitsrisiken (Kap. 7.2) mit ereignisbasiertem oder wertbasiertem Ansatz</td><td>P2.3: Bedrohungen für kritische Assets ermitteln
P3.1: Zugriffswege auf Assets ermitteln</td></tr>
<tr><td colspan="2">STRIDE/DREAD</td></tr>
<tr><td colspan="2">Bedrohungen werden anhand der sechs STRIDE-Kategorien (Vortäuschen der Identität, Manipulation, Nichtanerkennung, Veröffentlichung von Informationen, Denial-of-Service und Erhöhung von Rechten) ermittelt, indem diese auf das Datenfluss-Diagramm angewendet werden.</td></tr>
<tr><td rowspan="5">Einschätzen von Risiken</td><td>BSI 200-3</td><td>B3S Gesundheit</td></tr>
<tr><td>Einschätzung von Eintrittshäufigkeit und Schaden der Gefährdung (Kap. 5.1)</td><td>Qualitative Einschätzung von Eintrittswahrscheinlichkeit (ANF-0210), Schaden (0205) und Kritikalität (ANF-0203).</td></tr>
<tr><td>ISO 27005</td><td>OCTAVE-S</td></tr>
<tr><td>Beurteilung potentieller Folgen (Kap. 7.3.2)
Folgekriterien (Kap. 6.4.3.2)
Beurteilung der Wahrscheinlichkeit (Kap. 7.3.3)
Wahrscheinlichkeitskriterien (Kap. 6.4.3.3)</td><td>P4.1: Bewertung potentieller Auswirkungen der Bedrohungen
P4.3: Eintrittswahrscheinlichkeit der Bedrohungen bewerten (optional)
P3.2: Analyse von technologiebasierten Prozessen in Bezug auf die Assets
P1.3: Bewertung der Sicherheitspraktiken der Organisation
P5.1: Beschreiben der aktuellen Schutzstrategie</td></tr>
<tr><td colspan="2">STRIDE/DREAD</td></tr>
<tr><td colspan="2">Jede Bedrohung wird mit den fünf DREAD-Kategorien (Schaden, Reproduzierbarkeit, Ausnutzbarkeit, betroffene Nutzer und Auffindbarkeit) bewertet.</td></tr>
</table>

Bewerten von Risiken	**BSI 200-3**	**B3S Gesundheit**
	Risikomatrix auf Basis von Eintrittshäufigkeit und Schaden mit Risikokategorien als Felder der Matrix (Kap. 5.2)	Priorisierung anhand von Kritikalität (ANF-0203). Risikoklassen in Risikomatrix auf Basis von Eintrittswahrscheinlichkeit und Schaden bilden (ANF-0210)
	ISO 27005	**OCTAVE-S**
	Bestimmung des Risikoniveaus (Kap. 7.3.4) Kriterien zur Bestimmung des Risikoniveaus (Kap. 6.4.3.4) Bewertung von Informationssicherheitsrisiken (Kap. 7.4)	„P5.2: Auswahl von Ansätzen im Umgang mit Risiken“ verweist auf ermittelte Informationen und nennt Kriterien zur Auswahl von Risikobehandlungsoptionen. Es wird jedoch kein alleiniger Risikowert bestimmt.
	STRIDE/DREAD	
	Die einzelnen Bewertungen der DREAD-Kategorien werden zu einem Gesamtergebnis aufsummiert.	
Behandeln von Risiken	**BSI 200-3**	**B3S Gesundheit**
	Auswahl von Behandlungsoptionen (vermeiden, reduzieren, transferieren, akzeptieren) auf Basis von Akzeptanzkriterien und Risikoniveau (Kap. 6)	Auswahl von Behandlungsoptionen (vermeiden, reduzieren, akzeptieren) auf Basis von Akzeptanzkriterien und Risikoklasse (ANF-0212, ANF-0213)
	ISO 27005	**OCTAVE-S**
	Prozess zur Informationssicherheitsrisikobehandlung (Kap. 8) mit der Vermeidung, Änderung, Beibehaltung und Teilung von Risiken als Behandlungsoptionen.	P5.2: Auswahl von Ansätzen im Umgang mit Risiken P5.3 Pläne zum Umgang mit Risiken entwickeln
	STRIDE/DREAD	
	Behandlung ist nicht direkt von STRIDE/DREAD. Dafür es in ein Risikomanagement oder einen Threat-Modeling-Prozess eingebunden sein.	
Anschließende Aufgaben	**BSI 200-3**	**B3S Gesundheit**
	Konsolidierung des Sicherheitskonzepts (Kap. 7) und Fortführung des BSI-Standards 200-2	Kommunikation und Überwachung von Risiken. Risikoberichte an Krankenhausleitung (ANF 0216).

	ISO 27005	OCTAVE-S
	Risikobehandlungsplan (Kap. 8.6) Kommunikation und Konsultation (Kap. 10.3) Überwachen und Überprüfen (Kap. 10.5) Korrekturmaßnahme (Kap. 10.7) Fortlaufende Verbesserung (Kap. 10.8)	P5.4: Auswirkungen auf die Schutzstrategie erheben P5.5: weitere Schritte identifizieren
	STRIDE/DREAD	
	Weiterführende Schritte können im Rahmen eines Risikomanagements oder eines Threat-Modeling-Prozesses durchgeführt werden.	

Die Identifikation von Risiken des BSI-Standards basiert auf den elementaren Gefährdungen seines IT-Grundschutz-Kompendiums. Mit dieser Vorgehensweise setzt das BSI einen Maßstab, auf den auch andere Standards, wie der B3S „medizinische Versorgung“ zurückgreifen. Die Gruppierung von Bedrohungen in Bedrohungsprofilen wird bei den Standards OCTAVE-S und B3S „Medizinische Versorgung“ vorgenommen. Die ISO-Norm beschreibt zur Risikoidentifikation zwei Ansätze. Das ereignisbasierte und das wertbasierte Vorgehen. Der BSI-Standard, der B3S und OCTAVE-S stellen Risikoobjekte an den Beginn der Betrachtung und schätzen Risiken basierend auf Bedrohungen und Schwachstellen ein. Somit verfolgen diese drei Standards einen wertbasierten Ansatz.

Bei allen der untersuchten Standards, außer OCTAVE-S, werden Risiken auf Basis von Schadenshöhe und Eintrittswahrscheinlichkeit ermittelt. Beim OCTAVE-S-Standard wird ebenfalls die potentielle Schadenshöhe eingeschätzt. Die Bewertung der Eintrittswahrscheinlichkeit ist hier jedoch nur optional. Es wird somit kein Risikowert bestimmt, der auf der Schadenshöhe und der Eintrittswahrscheinlichkeit beruht. Dafür werden weitere Faktoren herangezogen und bewertet, die dem Anwender bei der Entscheidung über die Behandlung der Risiken helfen soll. Der Fokus des Standards liegt auf organisatorischen und strategischen Wegen zur Verbesserung der Sicherheit.

Zur Behandlung von Risiken nennen der BSI-Standard und die ISO/IEC-Norm 27005 jeweils vier Optionen. Das sind beim BSI-Standard das Vermeiden, Reduzieren, Transferieren und Akzeptieren von Risiken. Die ISO-Norm beinhaltet die gleichen Behandlungsoptionen, nennt diese aber teilweise anders. Der B3S „Medizinische Versorgung“ nennt, abgesehen vom „Risikotransfer“, die gleichen Optionen. OCTAVE-S nennt die Optionen der Akzeptanz und Entschärfung von Risiken sowie die Zurückstellung von Risiken. Der Transfer von Risiken wird hier nicht erwähnt.

Während die Standards des BSI, der B3S und die ISO-Norm basierend auf dem PDCA-Zyklus in einen Informationssicherheitsmanagementrahmen eingebettet sind, deckt der OCTAVE-S nur einen Teil des Zyklus ab und erfordert daher einen Managementrahmen. Darüber hinaus ist bei der Bearbeitung von OCTAVE-S, abgesehen von Ergänzungen zur ersten Phase nachdem die zweite Phase abgeschlossen ist, kein zurückkehren zu vorherigen Arbeitsschritten vorgesehen. Im Gegensatz dazu beschreiben die anderen Standards ein Vorgehen der Risikoanalyse, bei dem eine Rückkehr zu einer vorherigen Phase möglich und je nach Zwischenergebnis erforderlich ist.

Der B3S „Medizinische Versorgung“ etabliert mit Kritikalitätsklassen und zusätzlichen Schutzzielen neue Aspekte, die Vorgehen an Krankenhäuser anpassen. Weitere Individualisierungen wie zum Beispiel Vorschläge passender Schadensklassen könnten weitere Hilfestellungen für Anwender bieten. Während der B3S an einigen Stellen auf den IT-Grundschutz des BSI und weitere Normen verweist, erfordert der BSI-Standard, OCTAVE-S und die ISO-Norm keine Anwendung von Standards außerhalb der eigenen Reihe.

Die Kombination von STRIDE und DREAD stellt eine Alternative oder Ergänzung zu den Schritten der Identifizierung, Einschätzung und Bewertung von Risiken dar. Diese könnten in das Risikomanagement eines Standards eingebunden werden oder unabhängig von diesen als Teil eines Threat-Modeling-Prozesses agieren, der die Risikobehandlung und Managementaufgaben behandelt.

4 Evaluation am Beispiel einer Zahnarztpraxis

Die praktische Anwendung der Standards wird am Beispiel einer Zahnarztpraxis erprobt. Dazu werden die Standards des BSI und OCTAVE-S bearbeitet und Aspekte des B3S „Medizinische Versorgung“ sowie der ISO/IEC-Norm 27005 beachtet. Abschließend wird die Kombination von STRIDE und STREAD angewendet.

Die in Rheinland-Pfalz gelegene Zahnarztpraxis versorgt etwa 900 Patienten pro Quartal. Tätig sind in der Praxis elf Personen. Darunter der Inhaber, eine angestellte Zahnärztin, sechs zahnmedizinische Fachangestellte und ein Zahntechniker, eine Reinigungskraft und eine Verwaltungsaushilfe. Mit einem Jahresumsatz unter 900.000 Euro und einer kumulierten Vollzeitmitarbeiterzahl von unter zehn fällt die Zahnarztpraxis nach § 267a HGB unter die Definition der Kleinstunternehmen. Die Praxis besteht aus drei Behandlungszimmern, einem Büro, einer Anmeldung, einem Wartezimmer und einem Keller, in dem sich ein Aufenthaltsraum, ein Dentallabor und ein Materiallager befinden. Seit dem Jahr 2015 ist sie an das Internet angebunden. Die Praxis teilt sich das Gebäude mit einem Privathaushalt.

Aufgrund des zunehmenden Einsatzes von Informationstechnik und der Vernetzung mit dem Internet steigt die Abhängigkeit der Zahnarztpraxis von diesen. Besonders zur Sicherung der Patientenversorgung und ihrer Daten sollen aktuelle Sicherheitspraktiken in der Praxis überprüft und Maßnahmen zur Etablierung eines angemessenen Sicherheitsniveaus getroffen werden.

4.1 IT-Grundschutz

Im Folgenden wird die Bearbeitung des IT-Grundschutzes und die Ergebnisse der einzelnen Phasen beschrieben. Dabei soll besonders auf die Schritte der Sicherheitskonzeption und der Risikoanalyse eingegangen werden.

4.1.1 Initiierung und Organisation des Sicherheitsprozesses

In der Initiierungsphase werden grundlegende Rahmenbedingungen erfasst und definiert. Dazu gehört die Definition des Geltungsbereiches, welche sich über die gesamte Zahnarztpraxis mit allen Geschäftsprozessen, Anwendungen und IT-Systemen erstreckt. Die Unternehmensführung erklärt sich zur Übernahme der Gesamtverantwortung bereit und bestimmt den Autor dieser Arbeit zum Informationssicherheitsbeauftragten.

Der Schutz der Patientendaten und der IT-Systeme auf denen diese gespeichert sind, stellt für die Zahnarztpraxis eine wichtige Aufgabe dar. Daher ist die Wahrung der Verfügbarkeit, Integrität und Vertraulichkeit der Geschäftsinformationen im Rahmen eines ISMS in der

Standard-Vorgehensweise und der Einführung von Maßnahmen zum Schutz dieser notwendig. Mit diesen Maßnahmen sollen auch gesetzliche Vorgaben, darunter besonders

- die Richtlinie nach § 390 SGB V „IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung“,
- die Datenschutz-Grundverordnung (DSGVO) und
- das Bundesdatenschutzgesetz (BDSG),

eingehalten und finanzielle Schäden vermieden werden.

Zusammengefasst sind diese Aspekte in der Leitlinie zur Informationssicherheit (s. Anhang A).

4.1.2 Strukturanalyse

Als Ausgangsbasis müssen zunächst die zu schützenden Objekte erhoben werden. Dazu dient die Strukturanalyse. Diese umfasst die Auflistung von Geschäftsprozessen, Anwendungen, IT-Systemen und Räumen. Die einzelnen Schutzobjekte wurden im Rahmen einer Begehung der Praxis erhoben. Die wichtigsten dieser werden nachfolgend kurz beschrieben und anschließend in ihren Kategorien tabellarisch dargestellt. Verantwortlich für die Prozesse und Zielobjekte ist der Praxisinhaber.

Im Eingangsbereich der Praxis befindet sich die Anmeldung. Hier befindet sich ein Client-PC, ein Kartenlesegerät und ein Multifunktionsdrucker. Über den Client wird unter anderem auf die Praxisverwaltungssoftware DiosZX, auf die Röntgensoftwares und den E-Mail-Client zugegriffen. Die Schnittstelle zur Telematikinfrastruktur easyTI wird auf dem Client betreiben. In den Behandlungszimmern befinden sich jeweils ein Client-PC. Diese greifen auf die DiosZX und die Röntgensoftwares zu. Im Büro befinden sich ein Client-PC, der Server, ein NAS-System für Backups, zwei Röntgengeräte und ein Drucker. Der Client nutzt ebenfalls DiosZX, die Röntgensoftwares, easyTI und den E-Mail-Client. Auf dem Server befinden sich wiederum zwei virtuelle Server. Der erste dieser Server dient als Domänencontroller. Der zweite stellt die Anwendung DiosZX sowie Netzlaufwerke, auf denen sich Daten wie Röntgenbilder befinden, zur Verfügung. Auf dem physischen Server werden mit der Anwendung Veeam Backups der beiden virtuellen Server angelegt.

Erfassung der Geschäftsprozesse

Zunächst werden die wichtigsten Geschäftsprozesse der Zahnarztpraxis beschrieben. Diese umfassen die Kernprozesse zur Behandlung von Patienten sowie unterstützende Prozesse und werden durch eine Befragung in Erfahrung gebracht. In Tabelle 7 sind sie mit einer eindeutigen Nummer (GP), dem Namen, einer Beschreibung und der Prozess-Art dargestellt.

Tabelle 7: erhobene Geschäftsprozesse der Zahnarztpraxis

Kürzel	Name	Beschreibung	Prozess-Art
GP001	Termin-vereinbarung	Termine mit Patienten werden telefonisch oder im persönlichen Gespräch vereinbart. Die Terminplanung findet in einem Terminbuch statt.	unterstützender Prozess
GP002	Patienten-aufnahme	Die Aufnahme der Patienten erfolgt in der Anmeldung. Hierbei muss ggf. die Gesundheitskarte des Patienten eingelesen werden. Von Neupatienten werden alle Daten erfasst. Bei bekannten Patienten werden Daten überprüft. Hier wird auch der Versicherungsstatus überprüft und ggf. Formulare ausgefüllt	unterstützender Prozess
GP003	Untersuchung und Behandlung	Die Patienten werden in den Behandlungszimmern untersucht und behandelt. Röntgenbilder werden in den Behandlungszimmern und im Büro erstellt. Dieser Prozess benötigt Zugriff auf die Gesundheitsdaten des Patienten und die Funktionsfähigkeit der Röntgengeräte.	Kernprozess
GP004	Aufbereitung von Material/Werkzeug und Praxishygiene	Die Aufbereitung umfasst die Reinigung von Oberflächen, Materialien und Werkzeug. Zur Aufbereitung von Material wird ein Aufbereitungsgerät verwendet. Dieses speichert Aufbereitungsvorgänge auf einem USB-Stick	unterstützender Prozess
GP005	Labortätigkeiten	Dieser Prozess umfasst die Arbeiten des zahntechnischen Eigenlabors	unterstützender Prozess
GP006	Personalmanagement/-verwaltung	Dieser Prozess beinhaltet die Verwaltung, Einstellung und Entlassung von Personal sowie die Gehaltszahlung und die Dienstplanung	unterstützender Prozess

GP007	Dokumentation	Behandlungszimmer: Erfassung durchgeführter Maßnahmen. Empfang/Büro: Kontrolle	unterstützender Prozess
GP008	Abrechnung	Erstellung von Abrechnungsdateien für KZV und Erstellung von Patientenrechnungen zur Übermittlung an eine Factoring Gesellschaft	unterstützender Prozess
GP009	Einkauf/Materialbestellung	Dieser Prozess umfasst die Bestellung von Materialen, Werkzeugen und Geräte	unterstützender Prozess
GP010	IT-Betrieb	Dieser Prozess beschäftigt sich mit der Bereitstellung der IT-Systeme der Praxis. Er wird hauptsächlich von externen Dienstleistern oder dem Inhaber bereitgestellt	unterstützender Prozess
GP011	Wartung und Unterweisung	Dieser Geschäftsprozess umfasst die regelmäßige Wartung von Geräten und die regelmäßige Unterweisung von Mitarbeitern	unterstützender Prozess
GP012	Kommunikation mit Laboren und Kollegen	Dieser Geschäftsprozess umfasst die Kommunikation mit Laboren, Kollegen und Standesorganisationen	unterstützender Prozess

Erfassung der Anwendungen

Die Erfassung der Anwendungen beinhaltet die wichtigsten Anwendungen einer Organisation. Das sind die Anwendungen, deren Daten, Informationen und Programme, die bei den Schutzzielen der Vertraulichkeit, Integrität und Verfügbarkeit den höchsten Bedarf haben. Bei den Anwendungen in Tabelle 8 handelt es sich um eine reduzierte Darstellung. Die komplette Auflistung ist in Anhang B zu finden. Allgemeine Anwendungen haben das Kürzel „A“ und medizinische Anwendungen das Kürzel „Am“. Daneben sind der Name der Anwendung, die Anzahl der Systeme, auf denen sie benutzt wird, sowie weitere Informationen zu finden. [82, S. 14ff.]

Tabelle 8: erhobene Anwendungen der Zahnarztpraxis

Kürzel	Name	Anzahl	Plattform/Anbieter
A001	Textverarbeitung, Präsentation, Tabellenkalkulation	2	Microsoft Office 365
A002	E-Mail-Client	2	Microsoft Outlook
A003	Webbrowser	2	Microsoft Edge
A004	PDF-Reader	2	Adobe Acrobat Reader DC
A005	Fernwartung	4	TeamViewer
A006	Backup		

A006a	Veeam	1	Veeam Backup & Replication
A006b	Hyper Backup	1	Synology
A007	Voice over IP	1	Fritz!Box
A008	Active Director Domain Services	1	Active Directory
A009	Fileserver	3	Datei-/Speicherdienste
Am001	Praxisverwaltung	4	DiosZX
Am002	Schnittstelle Telematikinf-rastruktur	2	easyTI
Am003	Abrechnungshilfe	4	DAISY
Am004	Röntgensoftware		
Am004a	Sidexis	3	Sidexis 4
Am004b	VistaScan	3	
Am006	Monitorprüfung	1	RadiCS
Am007	Digitale Planungshilfe	1	DPF3

Erfassung der IT-Systeme und Kommunikationsverbindungen

Die Erhebung der IT-Systeme umfasst alle im Netz vorhandenen oder aktiven IT-Systeme. Dabei steht „C“ für Client, „D“ für Drucker, „N“ für Netzkomponente, „M“ für medizinische IT-Systeme, „S“ für Server und „T“ für Telekommunikationskomponenten. Die in der Zahnarztpraxis erhobenen IT-Systeme sowie andere Systeme („O“) und Kommunikationsverbindungen („K“) sind in der Tabelle 9 mit einem Kürzel, dem Namen, der Anzahl und der Plattform oder dem Hersteller zu sehen. Auch diese Darstellung ist verkürzt. Die komplette Auflistung ist in Anhang B zu sehen. Die Anzahl der IT-Systeme gibt an, ob ähnliche Systeme gruppiert wurden. Dies wurde zum Beispiel bei den Clients der Behandlungszimmer gemacht, da diese eine gleiche Umgebung und einen gleichen Schutzbedarf aufweisen.

Tabelle 9: erhobene IT-Systeme, andere Systeme und Kommunikationsverbindungen der Zahnarztpraxis

Kürzel	Name	Anzahl	Plattform/Hersteller
C001	Client Anmeldung	1	Windows 11
C002	Clients Behandlungszimmer	3	Windows 11
C003	Client Büro	1	Windows 11
D001	Multifunktionsdrucker (Anmel-dung)	1	Drucker-/Faxkombigerät von HP
D002	Drucker (Büro)	1	OKI C841
N001	Router zum Internet	1	DSL Router
N002/M001	Ti-Konnektor	1	secunet
N003	Switch (Keller)	1	TP-Link
N004	Switch (Büro)	1	TP-Link

N005	Switch (Anmeldung)	1	TP-Link
N007	Heizkörpersteuerung	1	TP-Link Access Point
M002	Kartenlesegerät	2	cherry
M003	Röntgen (Orthophos SL)	1	
M004	Röntgen (Vistascan)	1	
M005	Aufbereitungsgerät MELAG Vacuclave 118	1	
S001	Server	1	Windows Server 2022
S001a	Domänen-Controller	1	Windows Server 2022
S001b	Fileserver	1	Windows Server 2022
S002	Backupspeicher	2	SynologyNAS
T001	Telefonanlage	1	Auerswald
T002	Telefon (VoIP)	1	Fritz!Fon
T003	Telefon (ISDN)	2	
O001	Thermostate	5	Honeywell
O002	KZV-Abrechnungsstick	1	
O003	USB-Stick (Aufbereitungsgerät)	1	
K001	Internetanschluss		
K002	Verbindungen zwischen Netzkomponenten innerhalb der Praxis		Kupferkabel
K003	Verbindungen zwischen Switches und dem Server		Kupferkabel
K004	Verbindungen zwischen Switches und Clients		Kupferkabel
K005	Verbindungen zwischen Switches und Medizingeräten		Kupferkabel
K006	Verbindung zwischen Router und Telefon		DECT
K007	WLAN Heizkörpersteuerung		

Erfassung der Räume

Bei der Strukturanalyse werden auch die Räume der Organisation erhoben. Dabei sind insbesondere Räume von Interesse, in denen sich IT-Systeme oder Kommunikationsverbindungen befinden.

Alle Räume der Zahnarztpraxis sind in einem Gebäude. In Tabelle 10 sind die diese aufgelistet.

Tabelle 10: erhobene Räume der Zahnarztpraxis

Kürzel	Name	Anzahl
GB01	Praxisgebäude	1
R001	Anmeldung	1
R002	Wartezimmer	1
R003	Behandlungszimmer	3
R004	Aufbereitungsraum	1
R005	Büro	1
R006	Labor	1
R007	Aufenthaltsraum	1
R008	Heimarbeitsplatz	1
R009	Keller/Materialla-ger/Umkleide	1

externe Dienstleister

Zu den externen Dienstleister gehört ein IT-Hardware-Dienstleister. Für die Medizinsoftware DiosZX steht der Support des Spitta-Verlags zur Verfügung und in Fragen der Telematikinfrastruktur die Firma VisionmaxX. Darüber hinaus wird mit auswärtigen Dentallaboren, Dentalbedarfslieferanten und einem Steuerberater gearbeitet.

Netzplan und Abhängigkeiten

Die wichtigsten erhobenen Systeme des Informationsverbunds werden in einem Netzplan grafisch dargestellt. Dieser ist in Abbildung 10 zu sehen. Die drei Behandlungszimmer werden hier mit ihren Clients zu einer Gruppe zusammengefasst.

Die Abhängigkeiten zwischen Geschäftsprozessen, IT-Systemen und Anwendungen sind in Anhang C dargestellt.

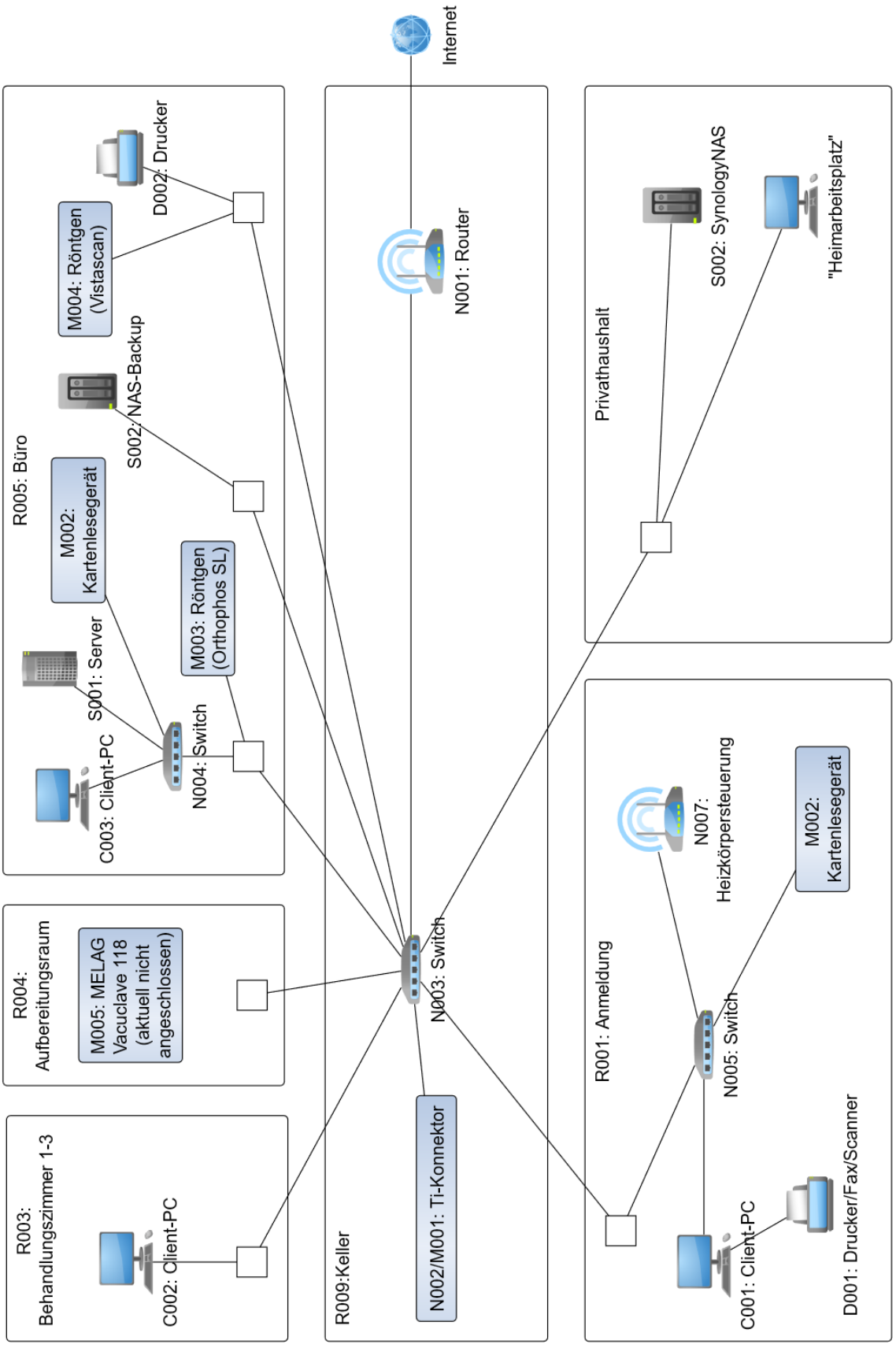

Abbildung 10: Netzplan der Zahnarztpraxis

4.1.3 Schutzbedarfsfeststellung

In der Schutzbedarfsfeststellung werden für die einzelnen Zielobjekte, die im vorherigen Schritt erhoben werden, der Schutzbedarf für die Vertraulichkeit, Integrität und Verfügbarkeit bestimmt. Zunächst werden jedoch Schutzbedarfskategorien definiert.

Für den Informationsverbund wird die vorgeschlagene qualitative Bewertung mit drei Kategorien übernommen. Dabei handelt es sich um die Kategorien „normal“, „hoch“ und „sehr hoch“. Bei der Schutzbedarfskategorie „normal“ sind die Schadensauswirkungen begrenzt und überschaubar. Bei der Schutzbedarfskategorie „hoch“ können sie beträchtlich sein. Schadensauswirkungen, die bis zu einer existenzielles Bedrohung gehen können, werden in der Kategorie „sehr hoch“ erfasst. [18, S. 104ff.]

Im Folgenden werden jeweils für die fünf Schadensszenarien

- „Verstoß gegen Gesetzte/Vorschriften/Verträge“,
- „Beeinträchtigung des informationellen Selbstbestimmungsrechts“,
- „Beeinträchtigung der persönlichen Unversehrtheit“,
- „Beeinträchtigung der Aufgabenerfüllung“,
- „negative Innen- oder Außenwirkung“ und
- „finanzielle Auswirkungen“

die Schutzbedarfskategorien „normal“ (s. Tabelle 11), „hoch“ (s. Tabelle 12) und „sehr hoch“ definiert. (s. Tabelle 13). [18, S. 104ff.]

Tabelle 11: Schadensszenarien für die Schutzbedarfskategorie „normal“

Schutzbedarfskategorie „normal“	
Gesetze/Vorschriften/Verträge	Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen allenfalls geringfügige juristische Konsequenzen oder Konventionalstrafen.
Selbstbestimmungsrecht	Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten nur geringfügige Auswirkungen auf die davon Betroffenen und würden von diesen toleriert.
persönliche Unversehrtheit	Die persönliche Unversehrtheit wird nicht beeinträchtigt.
Aufgabenerfüllung	Die Arbeit der Zahnarztpraxis wird in einem tolerablen Maß beeinträchtigt. Die Ausfallzeit darf zwischen 24 und 72 Stunden liegen (ggf. darüber).
Innen-/Außenwirkung	Es droht ein geringer Ansehensverlust bei Kunden und Geschäftspartnern.
Finanzielle Auswirkungen	Der mögliche finanzielle Schaden liegt unter 1.000 Euro.

Tabelle 12: Schadensszenarien für die Schutzbedarfskategorie „hoch“

Schutzbedarfskategorie „hoch“	
Gesetze/Vorschriften/Verträge	Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen schwerwiegende juristische Konsequenzen oder hohe Konventionalstrafen. (z.B. Honorarkürzungen)
Selbstbestimmungsrecht	Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten beträchtliche Auswirkungen auf die davon Betroffenen und würden von diesen nicht toleriert werden.
persönliche Unversehrtheit	Die persönliche Unversehrtheit kann nicht absolut ausgeschlossen werden.
Aufgabenerfüllung	Die Arbeit der Zahnarztpraxis wird erheblich beeinträchtigt. Ausfallzeiten dürfen maximal 24 Stunden betragen.
Innen-/Außenwirkung	Das Ansehen des Unternehmens bei Kunden und Geschäftspartnern wird erheblich beeinträchtigt.
Finanzielle Auswirkungen	Der mögliche finanzielle Schaden liegt zwischen 1.000 und 30.000 Euro.

Tabelle 13: Schadensszenarien für die Schutzbedarfskategorie „sehr hoch“

Schutzbedarfskategorie „sehr hoch“	
Gesetze/Vorschriften/Verträge	Bei Verstößen gegen Gesetze, Vorschriften oder Verträge drohen juristische Konsequenzen oder Konventionalstrafen, die die Existenz des Unternehmens gefährden.
Selbstbestimmungsrecht	Beeinträchtigungen des informationellen Selbstbestimmungsrechts und der Missbrauch personenbezogener Daten hätten ruinöse Auswirkungen auf die gesellschaftliche oder wirtschaftliche Stellung der davon Betroffenen.
persönliche Unversehrtheit	Die persönliche Unversehrtheit wird sehr stark und mit bleibenden Folgen beeinträchtigt.
Aufgabenerfüllung	Die Arbeit der Zahnarztpraxis wird so stark beeinträchtigt, dass Ausfallzeiten, die über eine Stunden hinausgehen, nicht toleriert werden können.
Innen-/Außenwirkung	Das Ansehen des Unternehmens bei Kunden und Geschäftspartnern wird grundlegend und nachhaltig beschädigt.
Finanzielle Auswirkungen	Der mögliche finanzielle Schaden liegt über 30.000 Euro.

Auf Basis der definierten Schutzbedarfskategorien kann der Schutzbedarf der Vertraulichkeit, Integrität und Verfügbarkeit für die Schutzobjekte festgestellt werden. Die Begründungen für die Auswahl der jeweiligen Schutzkategorie sind im Anhang D zu finden. Zunächst wird der Schutzbedarf der Geschäftsprozesse ermittelt (s. Tabelle 14).

Tabelle 14: Schutzbedarfsfeststellung der Geschäftsprozesse

Kürzel	Name	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
GP001	Terminvereinbarung	sehr hoch	hoch	hoch
GP002	Patientenaufnahme	sehr hoch	sehr hoch	sehr hoch
GP003	Untersuchung und Behandlung	sehr hoch	sehr hoch	sehr hoch
GP004	Aufbereitung von Material/Werkzeug und Praxishygiene	normal	sehr hoch	sehr hoch
GP005	Labortätigkeiten	sehr hoch	hoch	hoch
GP006	Personalmanagement/-verwaltung	hoch	normal	normal
GP007	Dokumentation	sehr hoch	sehr hoch	normal
GP008	Abrechnung	sehr hoch	normal	normal
GP009	Einkauf/Materialbestellung	normal	hoch	normal
GP010	IT-Betrieb	sehr hoch	hoch	sehr hoch
GP011	Wartung und Unterweisung	normal	normal	normal
GP012	Kommunikation mit Laboren und Kollegen	sehr hoch	hoch	normal

Anschließend wird der Schutzbedarf der Anwendungen ermittelt. Dieser ist in Tabelle 15 zu sehen.

Tabelle 15: Schutzbedarfsfeststellung der Anwendungen

Kürzel	Name	Schutzbedarf Vertraulichkeit	Schutzbedarf Integrität	Schutzbedarf Verfügbarkeit
A001	Textverarbeitung, Präsentation, Tabellenkalkulation	sehr hoch	normal	normal
A002	E-Mail-Client	sehr hoch	hoch	normal
A003	Webbrowser	normal	normal	normal
A004	PDF-Reader	sehr hoch	normal	normal
A005	Fernwartung	sehr hoch	hoch	sehr hoch
A006, A006a, A006b	Backup, Veeam, Hyper Backup	sehr hoch	sehr hoch	hoch

A007	Voice over IP	sehr hoch	sehr hoch	normal
A008	Active Directory Domain Services	hoch	hoch	sehr hoch
A009	Fileserver	sehr hoch	sehr hoch	sehr hoch
Am001	Praxisverwaltung	sehr hoch	sehr hoch	hoch
Am002	Schnittstelle Telematikinfrastruktur	sehr hoch	sehr hoch	hoch
Am003	Abrechnungshilfe	normal	normal	normal
Am004, Am004a, Am004b	Röntgensoftware, Sidexis, VistaScan	sehr hoch	hoch	sehr hoch
Am006	Monitorprüfung	normal	normal	normal
Am007	Digitale Planungshilfe	normal	normal	normal

Auf Basis des Schutzbedarfes der Geschäftsprozesse und Anwendungen kann der Schutzbedarf der IT-Systeme, Kommunikationsverbindungen und Räume ermittelt werden. Abhängigkeiten des Schutzbedarfes zwischen verschiedenen Gruppen von Schutzobjekten können mit der Vererbung des Schutzbedarfes dargestellt werden. Dabei gibt es drei Fälle. Beim Maximumprinzip („M“) kann der Schutzbedarf der Anwendung oder des Geschäftsprozesses, für den das IT-System oder die Kommunikationsverbindung genutzt wird, übernommen werden. Beim Verteilungseffekt („V“) verteilt sich der Schutzbedarf von zum Beispiel einer Anwendung auf mehrere IT-Systeme, womit der Schutzbedarf des IT-Systems geringer ist, als der der Anwendung. Der Kumulationseffekt („K“) tritt auf, wenn zum Beispiel auf einem IT-System mehrere Anwendungen laufen. Dann kann der Schutzbedarf des IT-Systems größer sein als der der einzelnen Anwendungen. [82, S. 42f.]

Tabelle 16 zeigt den Schutzbedarf der IT-Systeme, anderen Systeme und Kommunikationsverbindungen.

Tabelle 16: Schutzbedarfsfeststellung der IT-Systeme, anderen Systeme und Kommunikationsverbindungen

Kürzel	**Name**		**Schutzbedarf Vertraulichkeit**		**Schutzbedarf Integrität**		**Schutzbedarf Verfügbarkeit**
C001	Client Anmeldung	M	sehr hoch	M	sehr hoch		hoch
C002	Clients Behandlungszimmer	M	sehr hoch	M	sehr hoch		hoch
C003	Client Büro	M	sehr hoch	M	sehr hoch	M	sehr hoch
D001	Multifunktionsdrucker (Anmeldung)		sehr hoch		normal		normal
D002	Drucker (Büro)		sehr hoch		normal		normal
N001	Router zum Internet	M	sehr hoch	M	sehr hoch		hoch

N002/M001	Ti-Konnektor	M	sehr hoch	M	sehr hoch	M	hoch
N003	Switch (Keller)	M	sehr hoch	M	sehr hoch	M	sehr hoch
N004	Switch (Büro)	M	sehr hoch	M	sehr hoch	M	sehr hoch
N005	Switch (Anmeldung)	M	sehr hoch	M	sehr hoch	M	hoch
N007	Heizkörpersteuerung		normal		normal		normal
M002	Kartenlesegerät		sehr hoch		normal	V	hoch
M003	Röntgen (Orthophos SL)	M	sehr hoch	M	hoch	M	sehr hoch
M004	Röntgen (Vistascan)	M	sehr hoch	M	hoch	M	sehr hoch
M005	Aufbereitungsgerät MELAG Vacuclave 118		normal	M	sehr hoch		hoch
S001	Server		sehr hoch	M	sehr hoch	M	sehr hoch
S001a	Domänen-Controller	M	hoch	M	hoch	M	sehr hoch
S001b	Fileserver	M	sehr hoch	M	sehr hoch	M	sehr hoch
S002	Backupspeicher	M	sehr hoch	M	sehr hoch	M	hoch
T001	Telefonanlage	M	sehr hoch		sehr hoch		normal
T002	Telefon (VoIP)	M	sehr hoch	M	sehr hoch		normal
T003	Telefon (ISDN)		sehr hoch	M	sehr hoch		normal
O001	Thermostat		normal		normal		normal
O002	KZV-Abrechnungsstick		hoch	M	normal		normal
O003	USB-Stick (Aufbereitungsgerät)		normal	M	sehr hoch	M	hoch
K001	Internetanschluss		sehr hoch	M	sehr hoch		hoch
K002	Verbindungen zwischen Netzkomponenten innerhalb der Praxis		sehr hoch	M	sehr hoch	M	sehr hoch
K003	Verbindungen zwischen Switches und dem Server		sehr hoch	M	sehr hoch	M	sehr hoch
K004	Verbindungen zwischen Switches und Clients		sehr hoch	M	sehr hoch	M	sehr hoch

K005	Verbindungen zwischen Switches und Medizingeräten		sehr hoch	M	sehr hoch	M	sehr hoch
K006	Verbindung zwischen Router und VoIP-Telefon		sehr hoch	M	sehr hoch	M	normal
K007	WLAN Heizkörpersteuerung		normal	M	normal		normal

Abschließend wird der Schutzbedarf der Räume und Gebäude bestimmt (s. Tabelle 17).

Tabelle 17: Schutzbedarfsfeststellung der Räume und Gebäude

Kürzel	Name		Schutzbedarf Vertraulichkeit		Schutzbedarf Integrität		Schutzbedarf Verfügbarkeit
GB001	Praxisgebäude	M	sehr hoch	M	sehr hoch		sehr hoch
R001	Anmeldung	M	sehr hoch	M	sehr hoch	M	sehr hoch
R002	Wartezimmer		normal		normal		normal
R003	Behandlungszimmer	M	sehr hoch	M	sehr hoch	M	sehr hoch
R004	Aufbereitungsraum		normal	M	sehr hoch	M	hoch
R005	Büro	M	sehr hoch	M	sehr hoch	M	sehr hoch
R006	Labor	M	sehr hoch	M	hoch	M	hoch
R007	Aufenthaltsraum		normal		normal		normal
R008	Heimarbeitsplatz	M	sehr hoch	M	normal	M	normal
R009	Keller/Materiallager/ Umkleide	M	sehr hoch	M	sehr hoch	M	sehr hoch

4.1.4 Modellierung

Nachdem die Strukturanalyse und die Schutzbedarfsfeststellung durchgeführt wurden, erfolgt der Schritt der Modellierung. In dieser werden die Objekte des Informationsverbundes mit den Bausteinen des IT-Grundschutz-Kompendiums nachgebildet. Zunächst werden die Prozess-Bausteine aufgelistet, die auf den gesamten Informationsverbund anzuwenden sind.

- ISMS.1 Sicherheitsmanagement
- ORP.1 Organisation
- ORP.2 Personal
- ORP.3 Sensibilisierung und Schulung zur Informationssicherheit

- ORP.4 Identitäts- und Berechtigungsmanagement
- ORP.5 Compliance Management (Anforderungsmanagement)
- CON.1 Kryptokonzept
- CON.2 Datenschutz
- CON.3 Datensicherungskonzept
- CON.6 Löschen und Vernichten
- CON.9 Informationsaustausch
- OPS.1.1.1 Allgemeiner IT-Betrieb
- OPS.1.1.2 Ordnungsgemäße IT-Administration
- OPS.1.1.3 Patch- und Änderungsmanagement
- OPS.1.1.4 Schutz vor Schadprogrammen
- OPS.1.1.5 Protokollierung
- OPS.1.1.6 Software-Tests und -Freigaben
- OPS.1.2.2 Archivierung
- OPS.1.2.5 Fernwartung
- OPS.2.3 Nutzung von Outsourcing
- DER.1 Detektion von sicherheitsrelevanten Ereignissen
- DER.2.1 Behandlung von Sicherheitsvorfällen
- DER.2.2 Vorsorge für IT-Forensik
- DER.2.3 Bereinigung weitereichender Sicherheitsvorfälle
- DER.3.1 Audits und Revisionen
- DER.4 Notfallmanagement

Im Anschluss daran werden die System-Bausteine in Tabelle 18 dargestellt. System-Bausteine werden jeweils auf einen oder mehrere in der Strukturanalyse erhobenen Zielobjekte angewendet. In der Tabelle sind die relevanten Bausteine mit den Zielobjekten und der Anzahl der Zielobjekte aufgelistet.

Tabelle 18: Modellierung der System-Bausteine

Baustein-Kürzel	Baustein	Anzahl	Zielobjekt(e)
APP.1.1	Office-Produkte	1	A001
APP.1.2	Web-Browser	1	A003
APP.2.1	Allgemeiner Verzeichnisdienst	1	A008
APP.2.2	Active Directory Domain Services	1	A008
APP.3.1	Webanwendungen und Webservices	1	Am002
APP.3.3	Fileserver	1	A009
APP.5.3	Allgemeiner E-Mail-Client und -Server	1	A002
APP.6	Allgemeine Software	19	A001-Am007

SYS.1.1	Allgemeiner Server	3	S001, S001a, S001b
SYS.1.2.3	Windows Server	3	S001, S001a, S001b
SYS.1.5	Virtualisierung	1	S001
SYS.1.8	Speicherlösungen	1	S002
SYS.2.1	Allgemeiner Client	3	C001, C002, C003
SYS.2.2.3	Clients unter Windows	3	C001, C002, C003
SYS.4.1	Drucker, Kopierer und Multifunktionsgeräte	2	D001, D002
SYS.4.4	Allgemeines IoT-Gerät	1	O001
SYS.4.5	Wechseldatenträger	2	O002, O003
NET.1.1	Netzarchitektur und -design	1	Gesamter Informationsverbund
NET.2.1	WLAN-Betrieb	1	K007
NET.2.2	WLAN-Nutzung	1	O001
NET.3.1	Router und Switches	5	N001, N003, N004, N005, N006
NET.3.2	Firewall	1	N002/M001
NET.4.1	TK-Anlagen	1	T001
NET.4.2	VoIP	1	K006
NET.4.3	Faxgeräte und Faxserver	1	D001
INF.1	Allgemeines Gebäude	1	GB001
INF.2	Rechenzentrum sowie Serverraum	1	R005
INF.5	Raum sowie Schrank für technische Infrastruktur	1	R009
INF.7	Büroarbeitsplatz	3	R001, R002, R005
INF.8	Häuslicher Arbeitsplatz	1	R008
INF.10	Besprechungs-, Veranstaltungs- und Schulungsräume	1	R007
INF.12	Verkabelung	1	GB001, R001, R003, R004, R005, R009

Nicht modellierte Zielobjekte werden hier für die Risikoanalyse vorgemerkt. Das sind die Kartenlesegeräte (M002), die Röntgengeräte (M003 und M004), das Aufbereitungsgerät (M005) und die Telefone (T002 und T003).

4.1.5 IT-Grundschutz-Check

Im IT-Grundschutz-Check wird überprüft, welche der Sicherheitsanforderungen der zuvor ausgewählten Bausteine bereits erfüllt sind. Dies wird für alle Bausteine eines Zielobjektes und für die Bausteine, die auf den gesamten Informationsverband angewendet werden, durchgeführt. Beispielhaft werden dafür einige Anforderungen des Bausteins „SYS.1.1 Allgemeiner Server“ für das in der Risikoanalyse behandelte Zielobjekt „S001b Fileserver“ in Tabelle 19 aufgelistet und deren Erfüllungsgrad notiert.

Tabelle 19: Auszug aus dem IT-Grundschutz-Check für den Baustein „SYS.1.1 Allgemeiner Server“ des Zielobjektes „S001b Fileserver“

Baustein-Anforderung	Titel	Inhalt	Typ	Umsetzung
SYS.1.1.A1	Zugriffsschutz und Nutzung	Bei virtualisierten Servern MUSS der Zugriff auf die Ressourcen der Instanz und deren Konfiguration ebenfalls auf die berechtigten Personen begrenzt werden.	Basis	Teilweise
SYS.1.1.A1	Zugriffsschutz und Nutzung	Server DÜRFEN NICHT zur Erledigung von Aufgaben und Tätigkeiten verwendet werden, die grundsätzlich auf einem Client-System aus- und durchgeführt werden können.	Basis	Ja
SYS.1.1.A1	Zugriffsschutz und Nutzung	Insbesondere DÜRFEN vorhandene Anwendungen, wie Webbrowser, auf dem Server NICHT für das Abrufen von Informationen aus dem Internet oder das Herunterladen von Software, Treibern und Updates verwendet werden.	Basis	Ja
SYS.1.1.A11	Festlegung einer Sicherheitsrichtlinie für Server	Ausgehend von der allgemeinen Sicherheitsrichtlinie der Institution SOLLTEN die Anforderungen an Server in einer separaten Sicherheitsrichtlinie konkretisiert werden.	Standard	Nein

SYS.1.1.A16	Sichere Installation und Grundkonfiguration von Servern	Der vollständige Installations- und Konfigurationsvorgang SOLLTE soweit wie möglich innerhalb einer gesonderten und von Produktivsystemen abgetrennten Installationsumgebung vorgenommen werden.	Standard	Nein

4.1.6 Risikoanalyse nach BSI-Standard 200-3

Im Rahmen der Modellierung wurden einige Zielobjekte identifiziert, die nicht mit den Bausteinen des IT-Grundschutz-Kompendiums nachgebildet werden können. Diese müssen in der Risikoanalyse behandelt werden und sind nachfolgend aufgelistet:

- M002 Kartenlesegerät
- M003 Röntgen (Orthophos SL)
- M004 Röntgen (VistaScan)
- M005 Aufbereitungsgerät MELAG Vacuclave 118
- T002 Telefon (VoIP)
- T003 Telefon (ISDN)

Darüber hinaus müssen alle Zielobjekte, die nach der Schutzbedarfsfeststellung in einem der Schutzziele einen hohen oder sehr hohen Schutzbedarf aufweisen, einer Risikoanalyse unterzogen werden.

Bevor die Risikoanalyse für die Zielobjekte jedoch durchgeführt werden kann, müssen Kategorien zur Einschätzung von Eintrittshäufigkeit und Schadensauswirkungen definiert werden. Diese sind in Tabelle 20 und Tabelle 21 dargestellt.

Tabelle 20: Definition der Eintrittshäufigkeitskategorien

selten	Ereignis könnte nach heutigem Kenntnisstand höchstens alle fünf Jahre eintreten.
mittel	Ereignis tritt einmal alle fünf Jahre bis einmal im Jahr ein.
häufig	Das Ereignis tritt einmal im Jahr bis einmal pro Monat ein.
sehr häufig	Ereignis tritt mehrmals im Monat ein.

Tabelle 21: Definition der Schadensauswirkungskategorien

vernachlässigbar	Die Schadensauswirkungen sind gering und können vernachlässigt werden. Finanziell z.B. unter 100 Euro.
begrenzt	Die Schadensauswirkungen sind begrenzt und überschaubar. Finanziell z.B. zwischen 100 und 1.000 Euro.
beträchtlich	Die Schadensauswirkungen können beträchtlich sein. Finanziell z.B. zwischen 1.000 und 30.000 Euro.
existenzbedrohend	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen. Finanziell z.B. über 30.000 Euro.

Aus der Kombination von Schadenshöhe und Eintrittshäufigkeit ergibt sich das Risiko. Die Definition der Risikokategorien ist in Abbildung 11 festgelegt. Eine Institution muss entscheiden, wann ein Risiko akzeptabel ist und wann es behandelt werden muss. Für die Zahnarztpraxis bedeutet das, dass geringe Risiken akzeptiert werden sollen. Weitere Risiken sollen, wenn möglich, gemildert werden. Davon sollen sehr hohe und hohe Risiken bevorzugt behandelt werden.

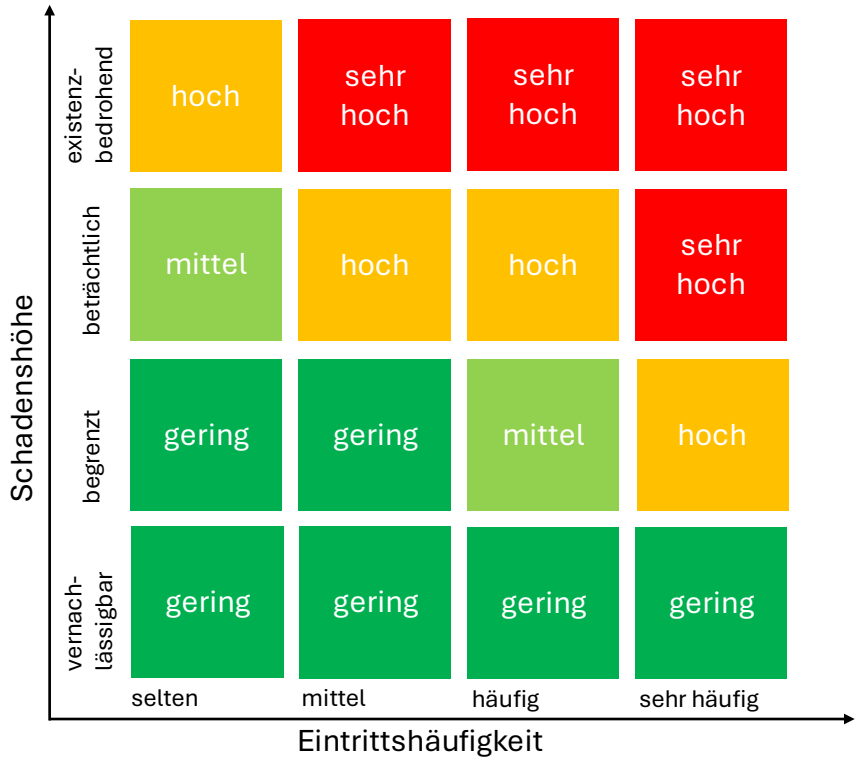

Abbildung 11: Definition der Risikokategorien

Beispielhaft wird im Folgenden die Risikoanalyse der Schutzobjekte „S001b Fileserver“ und „Am002 Schnittstelle Telematikinfrastruktur“ dargestellt.

4.1.6.1 Risikoanalyse des IT-Systems „S001b Fileserver"

Der Fileserver weist in den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit einen sehr hohen Schutzbedarf auf. Die Risikoanalyse beginnt mit der Ermittlung relevanter und zusätzlicher Gefährdungen. Daraufhin werden deren Risiken eingestuft. Die Risikoeinstufung wird beispielhaft für eine Gefährdung detailliert beschrieben. Mit dieser setzt sich auch die anschließende Risikobehandlung auseinander.

Erstellung der Gefährdungsübersicht

Zunächst werden die für das Zielobjekt „S001b Fileserver" relevanten Bausteine herangezogen und die darin angegebenen elementaren Gefährdungen aufgelistet. Nach den Kreuzreferenztabellen der Bausteine „SYS.1.1 Allgemeiner Server" und „SYS.1.2.3 Windows Server" sind folgende elementaren Gefährdungen für das Zielobjekt relevant.

- G 0.8 Ausfall oder Störung der Stromversorgung
- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation von Hard- oder Software
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.27 Ressourcenmangel
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.37 Abstreiten von Handlungen
- G 0.39 Schadprogramme
- G 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.43 Einspielen von Nachrichten
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen

Anschließend werden die verbliebenen elementaren Gefährdungen danach überprüft, ob sie für das Zielobjekt relevant sind. Nur Gefährdungen, die „direkt relevant" sind, werden in der Risikoanalyse beachtet. (s. Tabelle 22)

Tabelle 22: Relevanz der verbleibenden elementaren Gefährdungen für das Zielobjekt "S001b Fileserver"

Elementare Gefährdung	Relevanz
G 0.1 Feuer	Indirekt relevant
G 0.2 ungünstige klimatische Bedingungen	Indirekt relevant
G 0.3 Wasser	Indirekt relevant
G 0.4 Verschmutzung, Staub, Korrosion	Indirekt relevant
G 0.5 Naturkatastrophen	Indirekt relevant
G 0.6 Katastrophen im Umfeld	Nicht relevant
G 0.7 Großereignisse im Umfeld	Nicht relevant
G 0.9 Ausfall oder Störung von Kommunikationsnetzen	Indirekt relevant
G 0.10 Ausfall oder Störung von Versorgungsnetzen	Indirekt relevant
G 0.11 Ausfall oder Störung von Dienstleistungsunternehmen	Indirekt relevant
G 0.12 elektromagnetische Störstrahlung	Indirekt relevant
G 0.13 Abfangen kompromittierender Strahlung	Indirekt relevant
G 0.15 Abhören	Indirekt relevant
G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten	Indirekt relevant
G 0.24 Zerstörung von Geräten oder Datenträgern	Indirekt relevant
G 0.33 Personalausfall	Indirekt relevant
G 0.34 Anschlag	Indirekt relevant
G 0.35 Nötigung, Erpressung oder Korruption	Direkt relevant
G 0.36 Identitätsdiebstahl	Indirekt relevant
G 0.38 Missbrauch personenbezogener Daten	Direkt relevant
G 0.41 Sabotage	Indirekt relevant
G 0.42 Social Engineering	Direkt relevant
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	Direkt relevant
G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe	Direkt relevant

Nach den elementaren Gefährdungen werden zusätzliche Gefährdungen ermittelt. Diese sollen die elementaren Gefährdungen für den Anwendungsfall konkretisieren. Da der Schutzbedarf der drei Schutzziele sehr hoch ist, werden zusätzliche Gefährdungen gesucht, die alle drei Schutzziele betreffen.

Eine zusätzliche Gefährdungen für den Fileserver S001b ist die „Manipulation von Patientendaten durch andere Patienten“ (G z.1). Patienten könnten unbefugt in Räume eindringen oder wenn sie während der Behandlung alleine in einem Zimmer sind, Daten anderer Patienten manipulieren. Diese Gefährdung konkretisiert „G 0.22 Manipulation von Informationen“ und „G 0.44 Unbefugtes Eindringen in Räumlichkeiten“.

Eine weitere Gefährdung für das Zielobjekt ist das „Ausspähen von Patientendaten durch andere Patienten“ (G z.2). Patienten könnten unbefugt in Räume eindringen oder wenn sie während der Behandlung alleine in einem Zimmer sind, auf IT-Systeme zugreifen und

Daten anderer Patienten einsehen. Diese Gefährdung konkretisiert „G 0.14 Ausspähen von Informationen (Spionage)“ und „G 0.44 Unbefugtes Eindringen in Räumlichkeiten“.

Risikoeinstufung

Nach der Aufstellung der Gefährdungsübersicht werden die Eintrittshäufigkeit und potentielle Schadenshöhe der Gefährdung eingeschätzt und auf dieser Basis das Risiko bewertet. In Tabelle 23 sind alle Gefährdungen mit den Einschätzungen zu Eintrittshäufigkeit und Schadenshöhe und der Bewertung des Risikos dargestellt. Die Einschätzung und Bewertung dieser erfolgt anhand der zuvor definierten Kategorien. Da es sich beim betrachteten Zielobjekt um einen virtuellen Server handelt, wird bei einigen der Gefährdungen, die aus den IT-Grundschutz-Bausteinen hervorgehen, auf das Hostsystem verwiesen. Diese Gefährdungen sind für den virtuellen Server nur indirekt relevant und sollten vom physischen Server übergeordnet betrachtet werden.

Tabelle 23: Risikoeinstufung des Schutzobjektes „S001b Fileserver“

Elementare Gefährdung	Eintrittshäufigkeit	Schadenshöhe	Risiko
G 0.8 Ausfall oder Störung der Stromversorgung	Verweis auf Hostsystem S001: Gefährdung sollte bei dessen Risikoanalyse betrachtet werden.		
G 0.14 Ausspähen von Informationen (Spionage)	mittel	beträchtlich	hoch
G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten	Verweis auf Hostsystem S001: Gefährdung sollte auf diesem betrachtet werden.		
G 0.18 Fehlplanung oder fehlende Anpassung	mittel	existenzbedrohend	sehr hoch
G 0.19 Offenlegung schützenswerter Informationen	häufig	beträchtlich	hoch
G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle	selten	beträchtlich	mittel
G 0.21 Manipulation von Hard- oder Software	selten	existenzbedrohend	hoch
G 0.22 Manipulation von Informationen	selten	existenzbedrohend	hoch
G 0.23 Unbefugtes Eindringen in IT-Systeme	mittel	existenzbedrohend	sehr hoch
G 0.25 Ausfall von Geräten oder Systemen	Verweis auf Hostsystem S001: Gefährdung sollte bei dessen Risikoanalyse betrachtet werden.		
G 0.26 Fehlfunktion von Geräten oder Systemen	Verweis auf Hostsystem S001: Gefährdung sollte bei dessen Risikoanalyse betrachtet werden.		
G 0.27 Ressourcenmangel	selten	begrenzt	gering

G 0.28 Software-Schwachstellen oder -Fehler	mittel	existenzbedrohend	sehr hoch
G 0.29 Verstoß gegen Gesetze oder Regelungen	mittel	existenzbedrohend	sehr hoch
G 0.30 unberechtigte Nutzung oder Administration von Geräten und Systemen	selten	existenzbedrohend	hoch
G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen	mittel	beträchtlich	hoch
G 0.32 Missbrauch von Berechtigungen	hoch	beträchtlich	hoch
G 0.35 Nötigung, Erpressung oder Korruption	selten	beträchtlich	mittel
G 0.37 Abstreiten von Handlungen	mittel	begrenzt	gering
G 0.38 Missbrauch personenbezogener Daten	mittel	beträchtlich	hoch
G 0.39 Schadprogramme	mittel	existenzbedrohend	sehr hoch
G 0.40 Verhinderung von Diensten (Denial of Service)	selten	beträchtlich	mittel
G 0.42 Social Engineering	mittel	beträchtlich	hoch
G 0.43 Einspielen von Nachrichten	selten	beträchtlich	mittel
G 0.44 Unbefugtes Eindringen in Räumlichkeiten	mittel	beträchtlich	hoch
G 0.45 Datenverlust	mittel	begrenzt	gering
G 0.46 Integritätsverlust schützenswerter Informationen	mittel	existenzbedrohend	sehr hoch
G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe	mittel	beträchtlich	hoch
G z.1 Manipulation von Patientendaten durch andere Patienten	selten	existenzbedrohend	hoch
G z.2 Ausspähen von Patientendaten durch andere Patienten	mittel	beträchtlich	hoch

Bei der Eintrittswahrscheinlichkeit und Schadenshöhe ist zu beachten, dass diese im Vergleich zum folgenden Beispiel nicht mit demselben Detailgrad eingeschätzt wurden.

Beispielhaft wird die Einschätzung der Gefährdung G z.2 „Ausspähen von Patientendaten durch andere Patienten“ erläutert. Diese Gefährdung betrifft die Vertraulichkeit von Gesundheitsdaten. Unzureichende Sicherheitsvorkehrungen können einer anderen Person Zugriff auf diese ermöglichen. Darunter könnte eine fehlende Bildschirmsperre fallen, wenn ein Patient alleine im Behandlungszimmer ist. Konkret kann die vom Fileserver bereitgestellte Anwendung DiosZX genannt werden. Zugriff auf das Programm und deren Daten haben alle Clients. Während der Behandlungszeit wird die Anwendung dauerhaft genutzt und ist auf den Clients der Behandlungszimmern geöffnet. Mit fehlenden Sicherheitsvorkehrungen könnte ein Verstoß gegen Art. 32 DSGVO vorliegen. Dieser fordert das Ergreifen von Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Verfügbarkeit bei der Verarbeitung personenbezogener Daten. Die Schadenshöhe wird als „beträchtlich“ eingeschätzt. Als Datenbasis dienen dafür Geldbußen von DSGVO-Verstößen auf der Webseite „DSGVO-Portal.de“ [83]. In dieser Auflistung sind einige Verstöße von Zahnarzt- und Arztpraxen vorhanden, bei denen das Bußgeld 1.000 Euro übersteigt.

Die Einschätzung der Eintrittshäufigkeit erweist sich als schwierig, da bisher kein Fall dieser Art in der Zahnarztpraxis bekannt ist. Als Schwachstellen, die hierbei ausgenutzt werden können, kommen eine fehlende Bildschirmsperre sowie schwache Passwörter in Betracht. Aufgrund der sehr leichten Ausnutzbarkeit der Schwachstellen sollte die Eintrittshäufigkeit jedoch mindestens als „mittel“ eingeschätzt werden.

Aus der Kombination einer mittleren Eintrittshäufigkeit und einer beträchtlichen Schadenshöhe ergibt sich ein hohes Risiko (Abbildung 12).

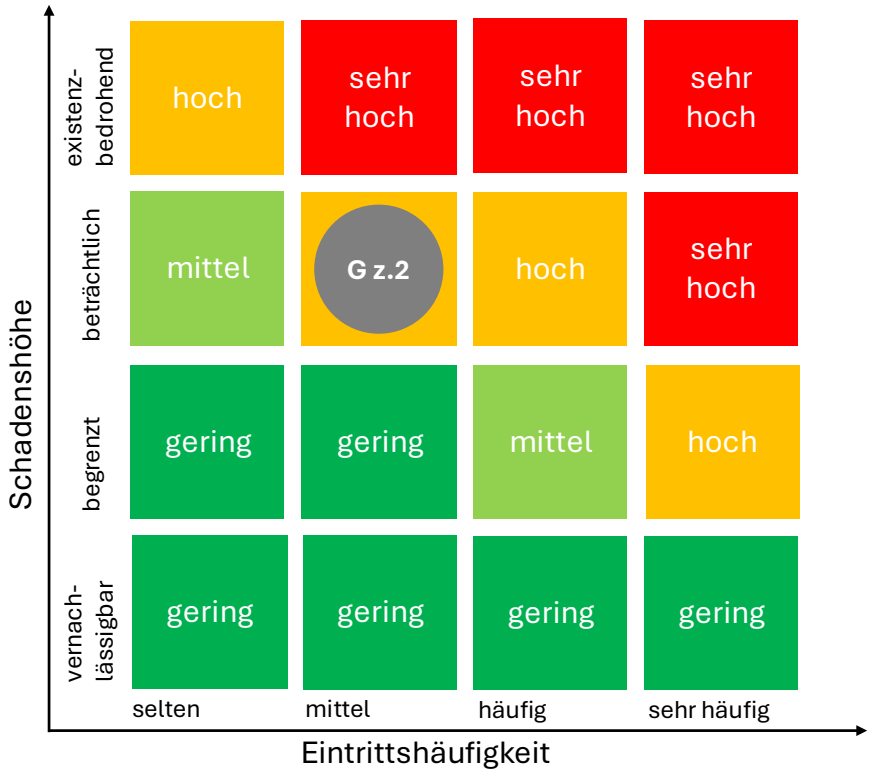

Abbildung 12: Risikobewertung der Gefährdung G z.2 für das IT-System „S001b Fileserver“

Risikobehandlung

Nachdem das aus einer Gefährdung hervorgehende Risiko bewertet wurde, muss über dessen Behandlung entschieden werden. Hier stehen die Optionen der Risikovermeidung, der Risikoreduktion, des Risikotransfers und der Risikoakzeptanz zur Verfügung.

Da das Risiko der Gefährdung „G z.2“ als hoch eingeschätzt wird, sollte es nicht akzeptiert werden. Zur Behandlung des Risikos wird die Reduktion des Risikos gewählt. Hierbei werden durch Maßnahmen die Eintrittshäufigkeit oder die Schadenshöhe verringert.

Als Maßnahme sollen sich die Benutzer der Clients abmelden, wenn sie den Raum verlassen. Dies ist besonders wichtig wenn sich ein Patient alleine im Raum befindet. Ebenso sollte der Bildschirm nach einer gewissen Zeit automatisch gesperrt werden.

Darüber hinaus soll eine Passwortrichtlinie in der Zahnarztpraxis etabliert werden, die die Nutzung schwacher Passwörter verhindert.

Mit diesen Maßnahmen soll die Ausnutzbarkeit der Schwachstellen erheblich reduziert und somit die Eintrittswahrscheinlichkeit der Gefährdung auf „selten“ reduziert werden. Eine Reduktion der Eintrittshäufigkeit führt dazu, dass die Gefährdung bei gleichbleibender Schadenshöhe nur noch ein mittleres Risikoniveau aufweist.

Direkte finanzielle Kosten entstehen nicht durch die Maßnahmen. Jedoch wird der Arbeitsaufwand mit diesen zusätzlichen Arbeitsschritten erhöht und womöglich Anforderungen an Hygienerichtlinien erschwert oder verletzt.

4.1.6.2 Risikoanalyse der Anwendung „Am002 Schnittstelle Telematikinfrastruktur“

Die Anwendung „Am002 Schrittstelle Telematikinfrastruktur“ (easyTI) weist für die Schutzziele Vertraulichkeit und Integrität einen sehr hohen Schutzbedarf auf. Für die Verfügbarkeit ist der Schutzbedarf hoch. Zunächst erfolgt eine Auflistung der relevanten Gefährdungen, dann wird für eine Gefährdung die Risikoeinstufung und die -behandlung durchgeführt.

Erstellung der Gefährdungsübersicht

Zunächst werden die für die Anwendung relevanten elementaren Gefährdungen bestimmt. Für die Anwendung wurden in der Modellierung die Bausteine „APP.3.1 Webanwendungen und Webservices“ und „APP.6 Allgemeine Software“ als relevant identifiziert. Auf Basis dieser und der Prüfung der verbliebenen elementaren Gefährdungen werden nachfolgenden die direkten Gefährdungen aufgelistet.

- G 0.11 Ausfall oder Störung von Dienstleistungsunternehmen
- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.15 Abhören
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation von Hard- oder Software
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.27 Ressourcenmangel
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.35 Nötigung, Erpressung oder Korruption
- G 0.36 Identitätsdiebstahl
- G 0.37 Abstreiten von Handlungen
- G 0.38 Missbrauch personenbezogener Daten
- G 0.39 Schadprogramme
- G 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.42 Social Engineering
- G 0.43 Einspielen von Nachrichten
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen
- G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

Für die Anwendung wurden keine zusätzlichen Gefährdungen ermittelt.

Risikoeinstufung

Im Folgenden wird beispielhaft die Risikoeinstufung für die elementare Gefährdung „G 0.45 Datenverlust“ vorgenommen.

Die Eintrittshäufigkeit wird auf Basis bisheriger Erfahrungen mit der Anwendung bestimmt. In der Zahnarztpraxis kam es im Frühjahr 2024 zu einem Datenverlust aufgrund einer defekten Datenbank bei fehlender Datensicherung. Berichte über Beschädigungen der Datenbank nach einem Windows-Update gab es bereits im Jahr 2021 [84]. Daher wird die Eintrittshäufigkeit als „mittel“ eingeschätzt.

Aufgrund des Schadensereignisses in der Praxis mussten zahlreiche Telefonate mit Krankenkassen geführt und Patientenkarten erneut eingelesen werden. Aufgrund dieser Erfahrung und der Projektion dieser auf einen kompletten Datenverlust in Bezug auf die Anwendung, wird die Schadenshöhe als „beträchtlich“ eingeschätzt.

Daraus ergibt sich ein hohes Risikoniveau, das in Abbildung 13 dargestellt ist.

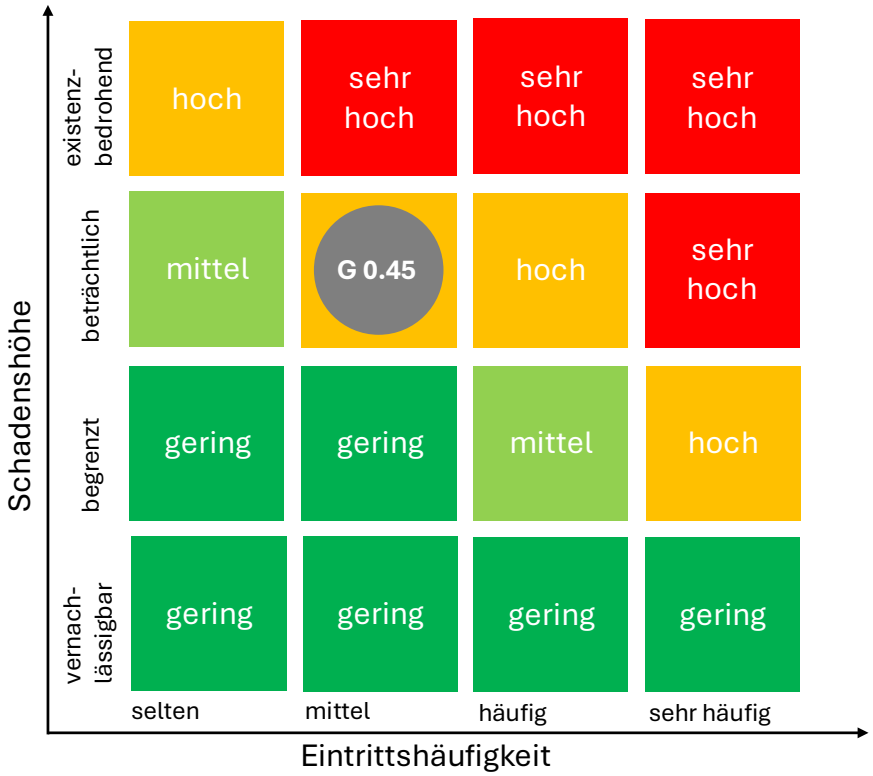

Abbildung 13: Risikobewertung der Gefährdung G 0.45 für die Anwendung Am002

Risikobehandlung

Dem Risiko, das aus der Gefährdung „G 0.45 Datenverlust“ für die Anwendung „easyTI“ hervorgeht, soll mit der Risikoreduktion begegnet werden. Dies soll in zwei Schritten erfolgen.

Zunächst soll ein weiterer virtueller Server eingerichtet werden, auf dem die Anwendung „easyTi“ in Absprache mit dem Hardware-Dienstleister und dem zuständigen Software-Dienstleister nach der Anleitung des Benutzerhandbuches [85] installiert wird.

Anschließend soll das gegenwärtige Datensicherungskonzept um den virtuellen Server ergänzt werden. Darüber hinaus soll das Datensicherungskonzept um Maßnahmen zur Erfüllung der Anforderungen des Bausteins „CON.3 Datensicherungskonzept“ ergänzt werden.

Bei der Erweiterung des Datensicherungskonzeptes soll das bisher genutzte private NAS-System als zweiten Backupspeicher durch ein zusätzliches NAS-System ersetzt werden. Dieses soll räumlich getrennt vom ersten Backupspeicher positioniert werden. Ebenfalls soll die Verschlüsselung von Backups, die Lagerung von Backup-Datenträgern außerhalb des Praxisgebäudes und die Testung der Wiederherstellung des Backups mit in das Konzept einbezogen werden.

Mit diesen Maßnahmen soll der Schaden, der mit dem Verlust von Daten der Anwendung einhergeht, reduziert werden. Dieser wird folglich aufgrund der Maßnahmen auf ein begrenztes Schadensniveau eingeschätzt. Bei gleichbleibender Eintrittshäufigkeit ist das Risiko eines Datenverlustes somit gering (s. Abbildung 14).

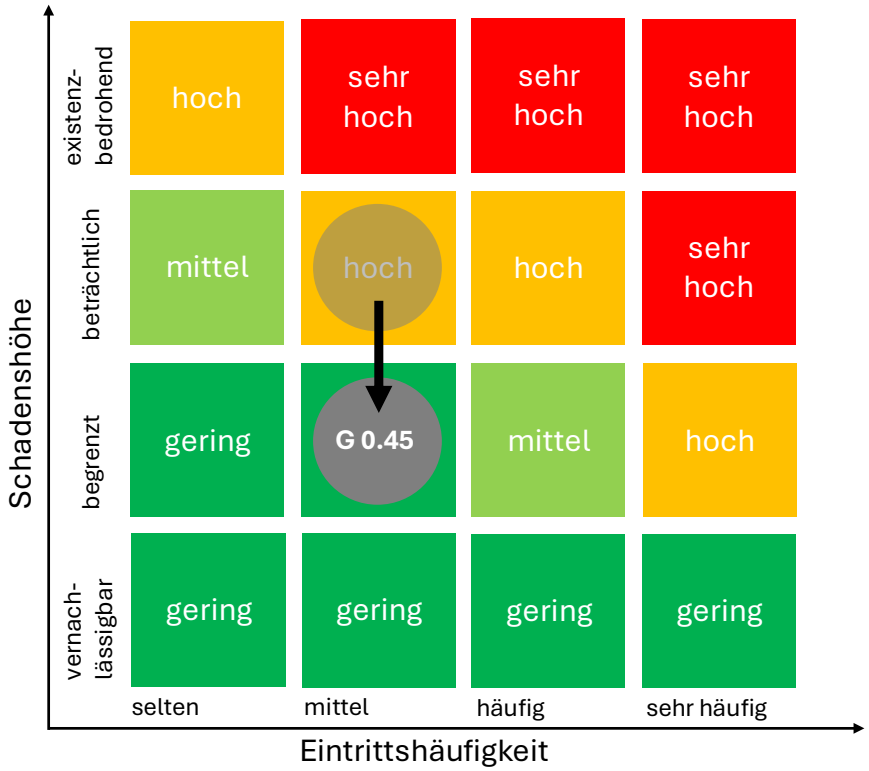

Abbildung 14: Veränderung des Risikos der Gefährdung „G 0.45 Datenverlust“ für die Anwendung „Am002 Schnittstelle Telematikinfrastruktur“

Die Umsetzung der Maßnahmen führt zu einem einmaligen Aufwand bei den Dienstleistern und in der Praxis.

4.1.7 Weitere Maßnahmen

Basierend auf dem IT-Grundschutz-Check und der Risikoanalyse werden Maßnahmen geplant, mit deren Umsetzung die Anforderungen des IT-Grundschutz-Kompendiums erfüllt und die Risiken gemildert werden sollen. Nachfolgend werden einige Maßnahmen aufgelistet und beschrieben (s. Tabelle 24).

Tabelle 24: Maßnahmen zur Erfüllung von Anforderungen und Reduktion der Risiken

Kürzel	Zielobjekt(e)	Baustein(e)/ Anforderung(en)	Maßnahme
M.1	C001-C003	aus Risikoanalyse	Mitarbeiter sollen sich bei Verlassen eines Raums vom Client abmelden.
M.2	C001-C003	aus Risikoanalyse	Bei allen Clients soll eine automatische Bildschirmsperre nach einer angemessenen Zeit aktiviert sein
M.3	Informationsverbund	aus Risikoanalyse	Es soll eine Richtlinie für sichere Passwörter etabliert werden. Die Nutzung einer biometrischen Authentifizierung oder einer zwei-Faktor-Authentifizierung sollen geprüft werden.
M.4	C001, S001, Am002	aus Risikoanalyse	Die Anwendung „easyTI“ soll auf einem eigenständigen virtuellen Server bereitgestellt werden.
M.5	Informationsverbund	CON.3 Datensicherungskonzept	Das gegenwärtige Datensicherungskonzept soll zur Erfüllung der Anforderungen des Bausteins „CON.3 Datensicherungskonzept“ u.a. erweitert werden um - ein neues NAS-System, - eine Verschlüsselung der Backups - eine Lagerung von Backups außer Haus und - regelmäßige Wiederherstellungstests
M.6	Informationsverbund	NET.1.1 Netzwerkarchitektur und -design	Zur Segmentierung soll das Netz zunächst in drei Bereiche geteilt werden: - Praxisnetz - Heizkörpersteuerung - Privathaushalt Weitere Sicherheitsvorkehrungen innerhalb des Praxisnetzes sollen geprüft werden.
M.7	N006, M006		Entfernen nicht genutzter IT-Systeme

M.8	N002/M001 Ti-Konnektor	NET.3.2 Firewall	Der Ti-Konnektor soll seriell betrieben werden.
M.9	Informations-verbund	ORP.3 Sensibilisierung und Schulung zur Informationssicherheit	Die Mitarbeiter sollen regelmäßig in Fragen der Informationssicherheit sensibilisiert und geschult werden.
M.10	Informations-verbund	OPS.1.1.3 Patch- und Änderungs-management	Es soll ein Konzept etabliert werden, mit dem Updates für Anwendungen und System verwaltet und regelmäßig durchgeführt werden.

Die Änderungen in der Netzwerksegmentierung und in der Betriebsart des Ti-Konnektors sind in Abbildung 15 dargestellt.

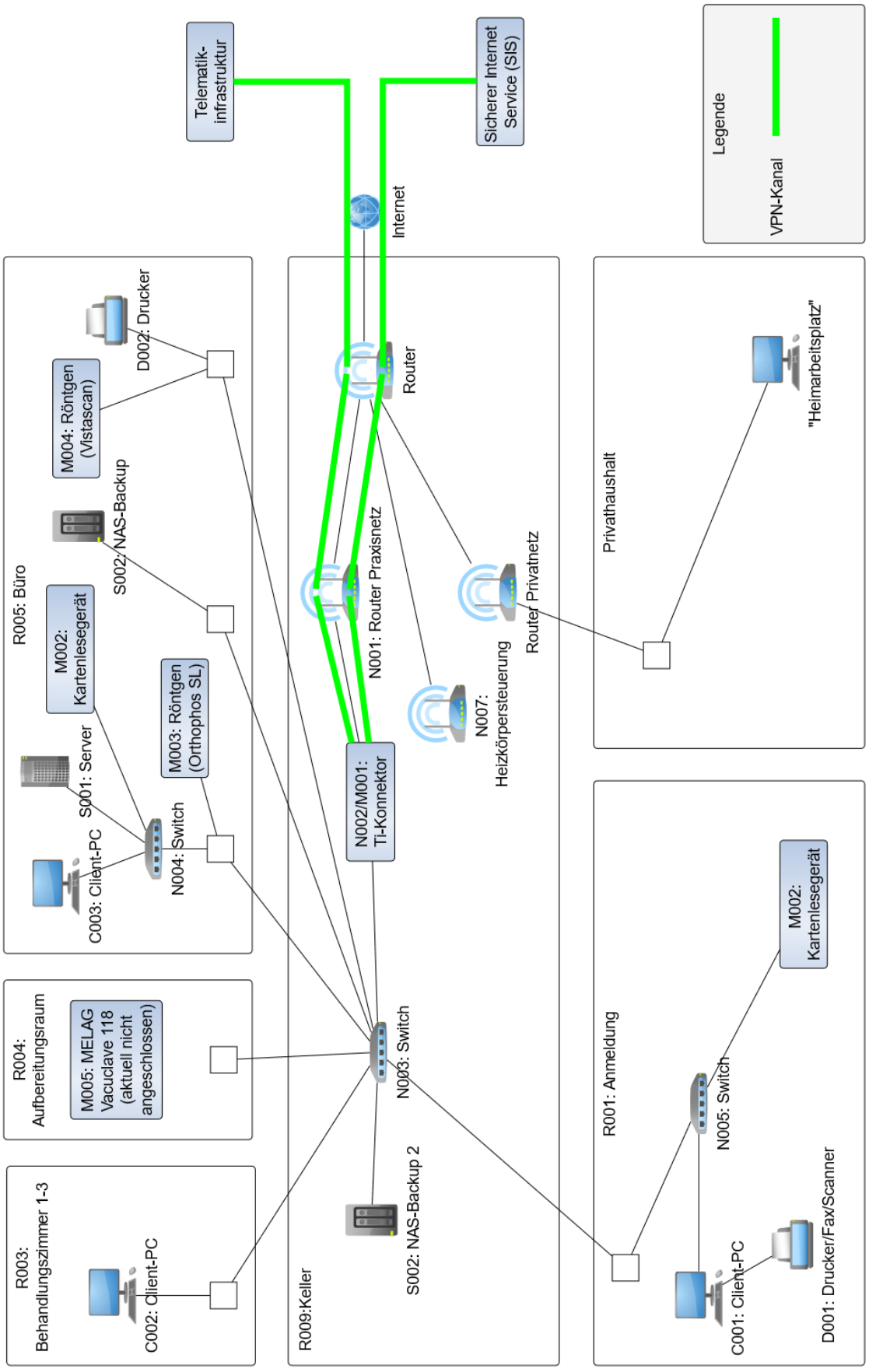

Abbildung 15: Netzplan nach Einführung der Maßnahmen mit VPN zu TI und SIS (nach [86])

Im Vergleich zu Abbildung 10, die den Netzplan ohne Maßnahmen darstellt, soll mit der Segmentierung des Netzwerks das Praxisnetz vom Privatbereich getrennt werden. Die zusätzliche Trennung der Heizkörpersteuerung führt dazu, dass im Praxisnetz kein WLAN betrieben wird. Zur Umsetzung der Maßnahme ist eventuell die Anschaffung weiterer Router und die Konsultation der IT-Dienstleister notwendig. Die Router sind wie in Abbildung 15 zu sehen anzuordnen. Für die Router sind, sofern weiterhin Geräte von AVM genutzt werden, die entsprechenden Anleitungen zur Einrichtung einer Router-Kaskade und zur VoIP-Einrichtung in dieser zu berücksichtigen. Im nächsten Schritt kann die Einrichtung eines Paketfilters vor dem Server zur weiteren Absicherung geprüft werden.

In der Strukturanalyse wurde festgestellt, dass der Ti-Konnektor parallel betrieben wird. Das heißt, dass er zu den anderen IT-Systemen parallel in das Netzwerk integriert ist. In dieser Variante stellt der Konnektor nur die Anbindung an die Telematikinfrastruktur dar. Seine Sicherheitsfunktionen werden jedoch nicht genutzt. Die Alternative ist der Reihenbetrieb, auch serieller Betrieb genannt. Diese Betriebsform ist in Abbildung 15 dargestellt. Hier läuft der gesamte Datenverkehr der Praxis durch den Ti-Konnektor. Dieser befindet sich somit zwischen dem Router und den anderen IT-Systemen der Praxis. Damit wird das Praxisnetz durch die Firewall- und Schutzfunktionen des Konnektors abgesichert. [87]

Die Telematikinfrastruktur (Ti) ist ein von der gematik GmbH betriebenes Netz mit dem Ziel des einfachen und sicheren Informationsaustausches zwischen Akteuren des Gesundheitswesens. Sie umfasst Anwendungen wie das Versichertenstammdatenmanagement, die elektronische Patientenakte und die Kommunikation im Medizinwesen (KIM). Letztere dient der Kommunikation unter den Akteuren im Gesundheitswesen. Mit dieser E-Mail-basierten Anwendung können Patientendaten wie Röntgenbilder Ende-zu-Ende-verschlüsselt ausgetauscht werden. Mit dem Ti-Konnektor ist auch der Zugang zum „Sicheren Internet Service“ (SIS) möglich. Dieser bietet Sicherheitsleistungen wie die eines Virenscanners, das Blocken von schadhaften Webseiten an und wird beim Reihenbetrieb zum Zugang ins Internet benötigt. Zur Telematikinfrastruktur und zum SIS werden jeweils eingeständige VPN-Kanäle (in der Abbildung grün dargestellt) aufgebaut. [88] [89, S. 26]

Der Aufwand zur Umstellung auf einen seriellen Betrieb des Konnektors beläuft sich auf die Einrichtung durch den Hardware-Dienstleister und den entsprechenden Software-Dienstleister sowie monatliche Kosten für den SIS von geschätzten 80 Euro.

Im Anschluss an die Aufstellung der Maßnahmen muss deren Zusammenwirken überprüft werden. Dabei ist zu beachten, dass es sich bei diesem Kapitel um keine abgeschlossene Auflistung der Maßnahmen handelt. Zur Umsetzung der Maßnahmen muss der Aufwand und die Kosten sowie die Integrationsfähigkeit und Akzeptanz im Praxisalltag geprüft werden.

Die letzte Phase des IT-Grundschutzes ist der Aufrechterhaltung und der Verbesserung des IT-Grundschutzes gewidmet. Hier werden die Maßnahmen überprüft und Anpassungen für den nächsten Zyklus vorgenommen.

4.2 OCTAVE-S

Im Folgenden wird die Bearbeitung des OCTAVE-S-Standards in der Zahnarztpraxis anhand der drei Phasen aufgezeigt („Entwicklung von Asset-basierten Bedrohungsprofilen“, „Schwachstellen in der Infrastruktur identifizieren“ und „Entwicklung von Schutzstrategie und Sicherheitsplänen“). Die optionalen Schritte der Wahrscheinlichkeitsbestimmung von Bedrohungen, welche bei allen anderen Standards erforderlich ist, werden nicht ausgeführt. Das Team zur Bearbeitung des Standards besteht aus dem Praxisinhaber und dem Ersteller dieser Arbeit. Als Geltungsbereich für die Analyse wird die gesamte Zahnarztpraxis bestimmt. Die bearbeiteten Arbeitsblätter des Standards befinden sich im Anhang.

4.2.1 Phase 1: Entwicklung von Asset-basierten Bedrohungsprofilen

Die erste Phase umfasst das Identifizieren von Informationen der Organisation und die Erstellung von Bedrohungsprofilen für kritische Asset.

Prozess 1: Identifizieren der Informationen der Organisation

Der erste Prozess beginnt mit der Entwicklung von Kriterien zur Bewertung von Auswirkungen (Prozess 1.1). Anhand des Arbeitsblattes „Impact Evaluation Criteria Worksheet“ aus dem vierten Band werden in einer Befragung des Praxisinhabers Grenzen für die Kategorien Gering, Mittel und Hoch für die Bereiche Ansehen, Gesundheit, gesetzliche Strafen, finanzielle Auswirkungen, Produktivität und Andere bestimmt. So werden beispielsweise die Auswirkungen von einmaligen finanziellen Verlusten von unter 1.000 Euro als gering eingeschätzt, Verluste zwischen 1.000 Euro und 30.000 Euro als mittel und Verluste von über 30.000 Euro als hoch. Ein Beispiel aus dem Bereich der Produktivität ist die Auswirkung „Einschränkung bei ausgelagerten Arbeiten und Materialbeschaffung“. Einen geringen Einfluss hat diese, wenn die Arbeit nur geringfügig eingeschränkt ist. Bei bis zu drei Terminen pro Woche, die verschoben werden müssen, ist die Auswirkung mittel. Bei mehr als drei Terminen ist die Auswirkung hoch. Die gesamte Definition der Auswirkungskategorien ist in Anhang E (Volume 4, S. 5ff., „Step 1“) zu sehen.

Im nächsten Schritt (Prozess 1.2) werden die Assets der Zahnarztpraxis erhoben (Asset Identification Worksheet, s. Anhang E, S. 19ff., „Step 2“). Diese umfassen Systeme, Anwendungen, Informationen und Menschen. Systeme und Anwendungen wurden aus dem IT-Grundschutz übertragen. Die wichtigsten Systeme sind nachfolgend aufgelistet:

- Clients in Anmeldung, Büro und Behandlungszimmer
- Router
- Ti-Konnektor
- Röntgen: Vistascan, Orthophos SL
- Kartenlesegerät
- Server
- Backupspeicher

Anschließend sind die wichtigsten Anwendungen dargestellt:

- Backupsoftware
- Praxisverwaltung: DiosZX
- Schnittstelle Telematikinfrastruktur: easyTI
- Röntgen: Sidexis, VistaScan

Zu den erhobenen Informationen gehören Patientendaten. Diese sind in DiosZX als Behandlungsdaten, in Sidexis als Röntgenbilder, im Terminbuch, in Formularen und Einverständniserklärungen und in easyTI zu finden. Auch bei der Kommunikation mit Kollegen, der Kassenzahnärztlichen Vereinigung und der Zahnärztekammer werden Patientendaten ausgetauscht. Mitarbeiterdaten umfassen zum Beispiel die Arbeitszeiterfassung und die Dienstplanung und werden an den Steuerberater gesendet.

Darüber hinaus werden die in der Praxis tätigen Personen mit ihren Fähigkeiten und den Assets, die sie nutzen, aufgelistet. Dies ist in Tabelle 25 zu sehen.

Tabelle 25: Mitarbeiter der Zahnarztpraxis mit Fähigkeiten und genutzten Assets

Person(en)	**Fähigkeiten**	**Genutzt Assets (Systeme)**	**Andere Assets**
Praxisinhaber (1)	- Behandlung - Abrechnung - Organisation - Kommunikation	Alles	Alles
Angestellte Zahnärztin (1)	- Behandlung - Kommunikation	Alles	u.a. DiosZX, easyTI, Sidexis, Vistascan, E-Mail-Client, Patientendaten
Zahntechniker (1)	- Laborarbeiten	keine	Laborauftrag
Zahnmedizinische Fachangestellte (6)	- Behandlungsassistenz - Hygiene - Kommunikation - Bestellung - Röntgenprüfung	Alles	u.a. DiosZX, easyTI, Sidexis, Vistascan, E-Mail-Client, Patientendaten
Reinigungskraft (1)	- Reinigung	Keine	Keine
Verwaltungsaushilfe (1)	- Ordnen und Archivieren von Unterlagen	keine	Patientendaten, Mitarbeiterdaten, Kommunikation mit Externen

Externe Dienstleister sind Fremdlabore, ein Abrechnungsunternehmen, ein Steuerberater, Software- und Hardware-Dienstleister und Dentalbedarfslieferanten.

Der letzte Schritt der ersten Prozessen (Prozess 1.3) behandelt die Bewertung der aktuellen Sicherheitspraktiken der Praxis (Security Practices Worksheet, s. Anhang E, S. 29ff., „Step 3a“, „Step 3b“, „Step 4“). Hier werden zu den 15 Sicherheitsbereichen Fragen gestellt. Mit diesen soll eingeschätzt werden, wie gut sich die Organisation in dem jeweiligen Bereich verhält. Abschließend wird eine Bewertung mit den Kategorien „Grün“, „Gelb“ und „Rot“ vorgenommen. Bei der Bewertung der Zahnarztpraxis konnte festgestellt werden, dass sich die Praxis um einige dieser Bereiche bisher nicht gekümmert hat. Die drei Bereiche „Sicherheitsmanagement“, „kollaboratives Sicherheitsmanagement“ und „Verwaltung von Netzwerk und Systemen“ werden mit dem gelben Status bewertet, was einer mittleren Bewertung entspricht. Die restlichen zwölf Bereiche werden mit einem roten Status bewertet. Dies entspricht einer niedrigen Bewertung. Keiner der Bereiche hat einem grünen Status bekommen. Besonders kritisch zu bewerten sind die Bereiche des „Schwachstellenmanagements“ und des „Managements von Vorfällen“. Diese Bereiche spielten in den Sicherheitspraktiken der Zahnarztpraxis bisher keine Rolle. Auch wenn die Einrichtung von Hardware und Software teilweise von Dienstleistern übernommen wird, obliegt die Verantwortung beim Praxisinhaber.

Prozess 2: Erstellen von Bedrohungsprofilen

Im zweiten Prozess werden im „Critical Asset Selection Worksheet“ (s. Anhang E, S. 61ff., „Step 5“) zunächst zwei kritische Asset ausgewählt (Prozess 2.1). Dabei handelt es sich um den Server als Zentrale des Praxisnetzwerkes und die Anwendung DiosZX als die zentrale Verwaltungsanwendung. Der Server stellt wichtige Anwendungen zur Verfügung und speichert Patientendaten. Betrachtet wird hier der gesamte Server inklusive der beiden virtuellen Server. DiosZX wird bei der Behandlung und Abrechnung genutzt und verwaltet Patientendaten.

Für jedes der ausgewählten Assets wird ein „Critical Asset Worksheet“ (s. Anhang F und Anhang G) für den jeweiligen Typ des Asset angelegt. Auf diesen werden die Nutzer und Verantwortlichen für das Asset sowie Assets, die mit dem Gewählten in Verbindung stehen, notiert („Step 6“ bis „Step 9“).

Sowohl der Server als auch DiosZX werden vom Praxisinhaber, der angestellten Zahnärztin und den zahnmedizinische Fachangestellten genutzt. Verantwortlich für den Server ist der Praxisinhaber. Eingerichtet wurde er vom Hardware-Dienstleister. Auf dem Server sind Mitarbeiter- und Patientendaten gespeichert. Anwendungen, die von ihm genutzt oder betrieben werden sind DiosZX, DAISY, Veeam, Active Directory, Hyper-V, „Datei-/Speicherdienste“ und TeamViewer. Vernetzt ist das Server mit den Clients und den Druckern. Verantwortlich für DiosZX ist der Praxisinhaber und der Dienstleister Spitta-Verlag. Die Anwendung wird vom Server bereitgestellt und den Clients genutzt. Darüber hinaus werden über das Kartenlesegerät Patientendaten eingelesen.

Im nächsten Schritt werden die für das Asset relevanten Schutzziele und das wichtigste Schutzziel ermittelt (Prozess 2.2, „Step 10“ und „Step 11“). Sowohl für den Server als auch

für DiosZX sind die drei Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit relevant. Unter der Beachtung möglicher Konsequenzen, die die Verletzung der Vertraulichkeit, Integrität und Verfügbarkeit nach sich ziehen können, wird sowohl für den Server als auch für DiosZX die Verfügbarkeit als wichtigstes Schutzziel gewählt.

Im letzten Schritt dieses Prozesses werden die Bedrohungen ermittelt (Prozess 2.3). Dazu werden in den „Risk Profile Worksheets“ für das jeweilige Asset die Bedrohungsprofile erstellt. Dies geschieht für die vier Kategorien „menschlicher Akteur mit Netzzugang“, „menschlicher Akteur mit physischem Zugang“, „Systemprobleme“ und „andere Probleme“ jeweils auf einem eigenen Arbeitsblatt. Im Anschluss werden mögliche Tätertypen identifiziert und die Stärke deren Motivs bestimmt. Danach wird dokumentiert, wie oft eine Bedrohung bisher aufgetreten ist und es werden Beispiele für die Bedrohungen gesucht. Die gesamten Bedrohungsprofile sind in Anhang F (S. 9ff., „Step 12“ bis „Step 16“) und Anhang G (S. 9ff., „Step 12“ bis „Step 16“) zu sehen. [56, S. 19ff.]

Für den Server wird der direkte Zugriff über den im Büro stehenden Monitor als physisch angesehen. Der Netzzugang auf den Server erfolgt über das interne Netzwerk, zum Beispiel über die Clients, oder von außerhalb des Praxisgebäudes. Ebenso wird der Zugriff auf DiosZX direkt über den Server als physisch angesehen und eine Nutzung über die Clients als ein Zugriff per Netzzugang.

Bei der Belegung der Äste der Bedrohungsbäume unterschieden sich die beiden Assets nicht. Es sind jeweils dieselben Äste aktiv. Daher gilt die folgende Ausführung für den Server und DiosZX. Für menschliche Akteure mit einem Netzzugang und physischen Zugang (s. Abbildung 16) werden alle Bedrohungen als relevant erachtet. Bei Systemproblemen (s. Abbildung 17) gilt dies ebenfalls für Malware und Softwaredefekte. Bei Hardwaredefekten und Systemabstürzen werden nur der Verlust von Daten und die Unterbrechung des Zugangs als relevant erachtet. Bedrohungen, die durch die Offenlegung oder Veränderung von Daten entstehen, werden hier nicht beachtet. In die Kategorie der anderen Probleme fallen die Stromversorgung, Telekommunikationsprobleme, Probleme bei Drittparteien, Naturkatastrophen und Probleme durch die physische Ausrichtung von Gebäuden oder Geräten. Als Bedrohung kommen für die Stromversorgung und Naturkatastrophen der Verlust von Daten und die Unterbrechung des Zugangs zu den Assets in Betracht. Für Telekommunikationsprobleme und Probleme bei Drittenparteien kommt die Unterbrechung des Zugangs in Betracht. Durch die physische Ausrichtung von Monitoren, die Daten der Assets anzeigen, ist eine Offenlegung von Informationen möglich.

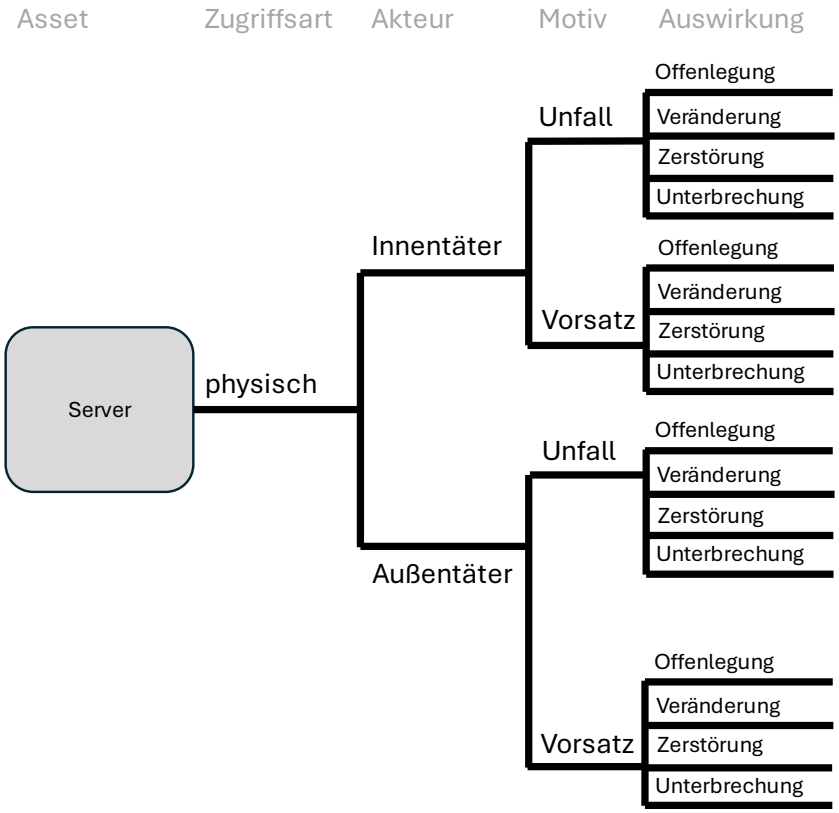

Abbildung 16: Bedrohungsprofil für menschliche Akteure mit physischem Zugang

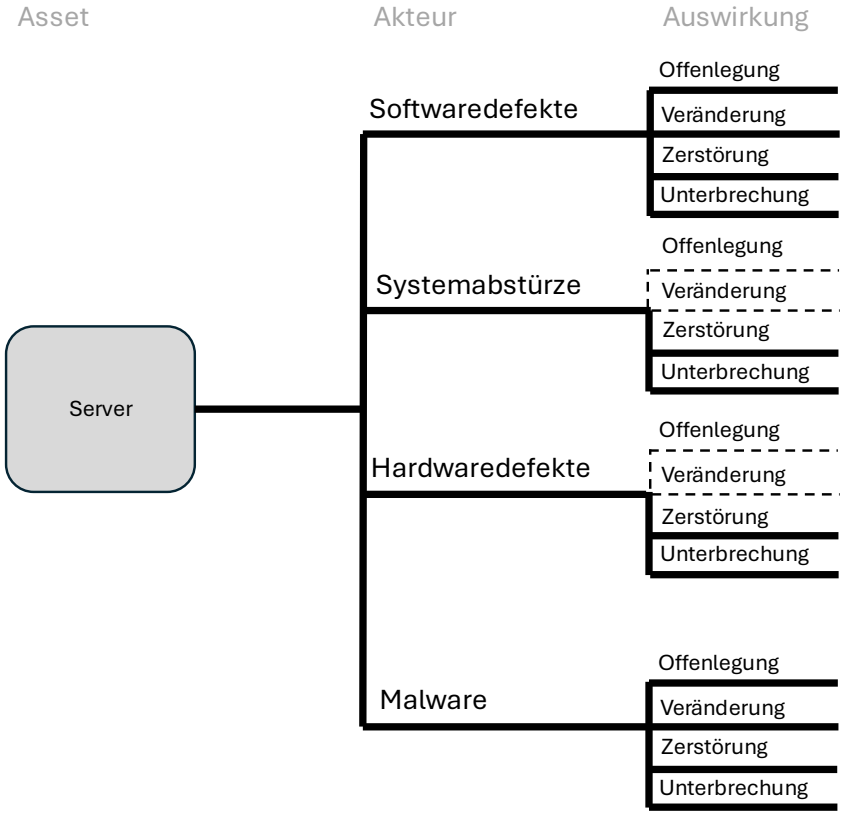

Abbildung 17: Bedrohungsprofil für Systemprobleme

Die potentiellen Täter werden nur für die Kategorien des Netzzugangs und des physischen Zugangs ermittelt. Beispiele dafür sind sowohl beim Server als auch bei DiosZX Mitarbeiter, der IT-Support, Ransomware-Gruppierungen oder Patienten. Für absichtliche Handlungen wird zusätzliche die Stärke des Motivs bestimmt. Dieses wird überwiegend als mittelstark eingeschätzt. Das bedeutet, dass der Täter auf die Organisation fokussiert ist, ohne eine außergewöhnlich hohe Intensität einzusetzen, um der Zahnarztpraxis zu schaden. Bei Außentätern kommt auch ein „geringes“ Motiv in Betracht. Bei diesem wählt der Täter die anzugreifende Organisation nicht speziell aus.

Die Einschätzung über das bisherige Eintreten der Bedrohungen für den Server zeigt für die Offenlegung und den Verlust von Daten sowie die Unterbrechung des Zugangs zum Server eine geringe Anzahl von Vorfällen beziehungsweise eine geringe Anzahl von erkannten Vorfällen. In vielen Fällen sind die Bedrohungen bisher nicht oder nur wenige Male aufgetreten. Bei der Offenlegung von Daten fällt auf, dass teilweise keine Angaben gemacht werden können. Ein Beispiel hierfür ist der Abruf von Patientendaten von Bekannten aus privaten Gründen. Hier kann nicht eingeschätzt werden, wie oft diese Handlung durchgeführt wird. Die Veränderung von Daten kommt unabsichtlich über den Netzzugang circa 20 Mal pro Jahr vor. Über andere Wege ist sie bisher nicht aufgetreten.

Da es sich bei DiosZX um eine Anwendung handelt, die vom Server bereitgestellt wird, ist zu erwarten, dass die Anzahl der aufgetretenen Bedrohungen bei DiosZX eine Teilmenge der aufgetretenen Bedrohungen des Server ist. Beim Vergleich der Daten des Server und von DiosZX kann festgestellt werden, dass diese weitestgehend übereinstimmen. Dies bedeutet, dass DiosZX für diese aufgetretenen Bedrohungen beim Server verantwortlich ist. Unterschiede gibt es beispielweise bei Hardware-Defekten. Zweimal haben Hardware-Defekte bisher zu Problemen bei der Nutzung von DiosZX in Behandlungszimmern geführt. Diese kamen jeweils bei Client-PCs vor. Bei den bisherigen Servern gab es keine Hardware-Defekte.

4.2.2 Phase 2: Schwachstellen in der Infrastruktur identifizieren

In der zweiten Phase werden für jedes Asset die Zugriffswege und die technologiebasierten Prozesse analysiert.

Prozess 3: Analyse der IT-Infrastruktur in Bezug auf kritische Assets

Auf dem „Network Access Paths Worksheet” (s. Anhang F, S. 55ff. und Anhang G, S. 55ff., jeweils „Step 17“ und „Step 18a“ bis „Step 18e“) werden die Zugriffswege auf die Assets in der Infrastruktur der Praxis ermittelt (Prozess 3.1). Hier werden die Systeme abgefragt, mit denen das kritische Asset am engsten verknüpft ist und dokumentiert, wie Daten der kritischen Assets abgefragt und gesichert werden. Ebenfalls wird ermittelt, welche Systeme auf das Asset zugreifen. [56, S. 31ff.]

Der Server besteht aus einem physischen Server, auf dem zwei virtuelle Server betrieben werden. Abgesehen von Fernwartungen werden Daten des Servers nur über das interne Netzwerk übertragen. Der Zugriff auf den Server geschieht mit den Clients. Gesichert werden seine Daten auf zwei NAS-Systemen.

DiosZX wird auf dem virtuellen Server „APP“ betrieben. Die Clients in der Anmeldung, im Büro und in den Behandlungszimmern greifen darauf zu. Übertragen werden die Daten über das interne Netzwerk. Gesichert werden die Daten der Anwendung auf zwei NAS-Systemen.

Die soeben erhobenen Informationen werden für alle Assets auf dem „Infrastructure Review Worksheet“ (s. Anhang E, S. 65ff., „Step 19a“ bis „Step 21“) zusammengefasst (Prozess 3.2). Hier werden Systeme in Klassen eingeteilt und deren Verbindung zu den kritischen Assets notiert. Darüber hinaus wird angegeben, wer für die Klassen zuständig ist und inwieweit Sicherheitsanforderungen beim Betrieb der Systeme beachtet werden. [56, S. 31ff.]

Im Falle der Zahnarztpraxis handelt es sich bei den Klassen um Server, das interne Netzwerk, Client-PCs und Speichergeräte. Für die Geräte sind der Inhaber sowie der Hardware-Dienstleister verantwortlich. Sicherheitsanforderungen werden beim Betrieb dieser bisher eher in einem geringen Maß berücksichtigt.

Die daran anschließende „Gap-Analyse“ führte zu keinen Änderungen bei den Bedrohungsprofilen und den Erkenntnissen im Bereich der Sicherheitspraktiken.

4.2.3 Phase 3: Entwicklung von Schutzstrategie und Sicherheitsplänen

In der dritten Phase werden Risiken identifiziert und analysiert sowie eine Schutzstrategie und Pläne zum Umgang mit den Risiken entwickelt.

Prozess 4: Identifizieren und Analysieren von Risiken

In diesem Schritt (Prozess 4.1) werden die zu Beginn definierten Kriterien zur Bewertung von Auswirkungen heranzogen. Für alle aktiven Äste der Bedrohungsbäume werden nun mit den Kriterien die Auswirkungen der Bedrohungen für die fünf Auswirkungsbereiche Ansehen, Gesundheit, gesetzliche Strafen, finanzielle Auswirkungen und Produktivität bewertet. Dies erfolgt mit den Kategorien Hoch, Mittel und Gering. (s. Anhang F, S. 9ff. und Anhang G, S. 9ff., jeweils „Step 22“)

Sowohl beim Server als auch bei DiosZX hat die Offenlegung von Informationen Einfluss auf das Ansehen und hat mögliche finanzielle und rechtliche Konsequenzen. Die Einschränkungen der Produktivität und der Sicherheit und Gesundheit werden hierbei als gering eingeschätzt. Im Gegensatz dazu kann die Veränderung von Daten die Gesundheit der Patienten und die Produktivität erheblich einschränken. Auch der Verlust von Daten und die Unterbrechung des Zugangs auf die Assets haben hauptsächlich einen hohen Einfluss auf

die Produktivität. Als Beispiel ist in Abbildung 18 die unabsichtliche Offenlegung von Informationen über den Netzzugang von Mitarbeitern der Praxis für DiosZX dargestellt. Diese hat nach der Bewertung einen geringen Einfluss auf die Produktivität und die Sicherheit der Patienten. Jedoch kann diese Auswirkungen auf das Ansehen haben und finanzielle und rechtliche Konsequenzen nach sich ziehen. Wie groß diese Konsequenzen sind, ist letztendlich auch vom Ausmaß des konkreten Schadensereignisses abhängig. Hier sind sie als „mittel“ bewertet.

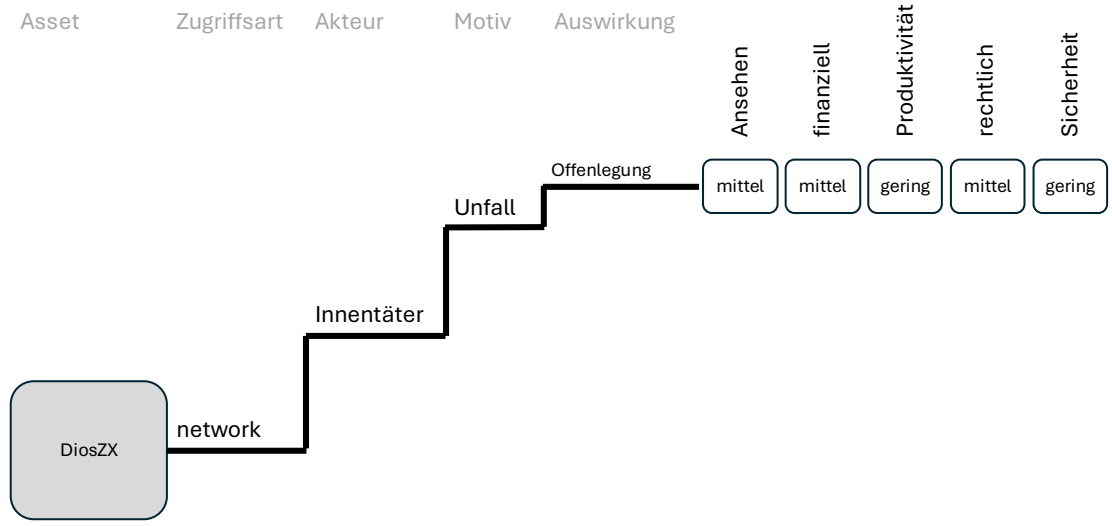

Abbildung 18: Auswirkungen einer unabsichtlichen Offenlegung von Informationen durch einen Innentäter über das Netzwerk für die Anwendung DioszX

Die Schritte zur Bestimmung der Eintrittswahrscheinlichkeit der Bedrohungen wurden wie bereits beschrieben nicht durchgeführt.

Prozess 5: Entwicklung von Schutzstrategie und Plänen zum Umgang mit Risiken

Der letzte Prozess beginnt mit der Beschreibung der aktuellen Schutzstrategie (Prozess 5.1). Hier wird auf dem „Protection Strategy Worksheet“ (s. Anhang H, S.23ff., „Step 25“) das Verhalten der Organisation in den 15 Sicherheitsbereichen noch einmal detaillierter abgefragt und diese Erkenntnisse aus Prozess 1.3 übertragen. Die Analyse der Angaben der Zahnarztpraxis ergibt, dass viele Sicherheitsbereiche bisher nicht beachtet werden oder Strategien oft nur informell und undokumentiert vorliegen. Als Beispiel kann hier das IT-Sicherheitstraining für Mitarbeiter genannt werden, welches bisher nicht durchgeführt wird.

Im anschließenden Schritt müssen Ansätze zum Umgang mit den Risiken gewählt werden (Prozess 5.2). Hier kommen die Akzeptanz, Entschärfung oder Zurückstellung in Frage. Dies passiert wieder auf den „Risk Profile Worksheets“ (s. Anhang F, S. 9ff. und Anhang G, S. 9ff., jeweils „Step 27“). Darüber hinaus werden circa drei Sicherheitsbereiche ausgewählt, auf die sich die Risikobehandlungstätigkeiten konzentrieren. Die Entscheidung erfolgt auf der Basis mehrerer Faktoren. Dazu gehören die potentiellen Auswirkungen der Risiken, die Bewertung der Praktiken der Organisation in den Sicherheitsbereichen und die für das Asset relevanten Schutzziele. [56, S. 75ff.]

Die Zahnarztpraxis hat sowohl für den Server als auch für DiosZX die Verfügbarkeit als wichtigstes Schutzziel identifiziert. Aus diesem Grund werden bevorzugt Risiken, die die Produktivität beeinträchtigen, zur Entschärfung ausgewählt. Ebenfalls sollen Risiken, die die Sicherheit der Patienten bedrohen, verstärkt behandelt werden. Diese beiden Bereiche gehen hauptsächlich mit Bedrohungen einher, die zu einer Veränderung von Daten, zu einem Datenverlust oder zu einer Unterbrechung des Asset-Zugriffs führen. Einige Risiken, die diese Bereiche betreffen werden zur Entschärfung vorgemerkt. Zusätzlich soll das Risiko, das eine Offenlegung von Informationen aufgrund der physischen Konfiguration von Geräten ermöglicht, reduziert werden. Der Einfluss dieser Bedrohung wird zwar als eher gering eingeschätzt, jedoch tritt diese mehrmals am Tag auf. Alle verbleibenden Risiken werden zurückgestellt und sollen zu einem späteren Zeitpunkt erneut analysiert werden. Zunächst soll kein Risiko akzeptiert werden.

Zur Auswahl der drei Sicherheitsbereiche, in denen die Pläne zum Umgang mit den Risiken entwickelt werden sollen, werden zunächst alle mit einem roten Status markierten Bereiche betrachtet. Aufgrund der gewählten Risiken und der Bewertung der Sicherheitsbereiche werden

- die Schaffung von Bewusstsein für Sicherheit und Schulungen,
- das Notfallmanagements und
- die Authentifizierung und Autorisierung

als Bereiche gewählt, in denen Maßnahmen getroffen werden. Sicherheitsschulungen sollen das Wissen und die Aufmerksamkeit der Mitarbeiter im Bereich der IT-Sicherheit stärken. Auch die Aufrechterhaltung des Betriebs und die Vorbereitung auf Probleme soll in den Blick genommen werden. Mit dem dritten Sicherheitsbereich sollen die Zugangskontrollmechanismen zu den IT-Systemen und Zugriffsrechte überarbeitet werden.

Für die drei gewählten Sicherheitsbereiche werden anschließend jeweils ein Plan zum Umgang mit Risiken entwickelt (Prozess 5.3). Diese werden auf dem „Mitigation Plan Worksheet“ (s. Anhang H, S. 115ff., „Step 28“) notiert. Die Pläne werden auf Basis von vorgeschlagenen (s. Anhang H, S. 83ff.) und eigenen Maßnahmen zur Entschärfung von Risiken angelegt. Dabei soll eine Maßnahme im besten Fall mehrere Risiken gleichzeitig behandeln. [56, S. 83ff.]

Im Bereich der Schaffung von Bewusstsein für Sicherheit und Schulungen soll die Teilnahme von Mitarbeiter an Fortbildungen in diesem Bereich geplant werden. Darüber hinaus soll ein formaler Prozess zur Einweisung von neuen Mitarbeitern in Bezug auf die IT-Sicherheit etabliert werden.

Der zweite gewählte Sicherheitsbereich betrifft das Notfallmanagement. Eine Kritikalitätsanalyse der Assets der Zahnarztpraxis wird in dieser Arbeit durchgeführt. Zu den geplanten Maßnahmen in diesem Bereich gehört auch das Aufstellen von Plänen zum Notfallmanagement und zur Aufrechterhaltung des Betriebes im Notfall. Um den Verlust von Daten zu

verhindern, sollen die Datensicherungspraktiken um die Offline-Sicherung außerhalb des Praxisnetzes und um die Lagerung von Backup-Datenträgern außerhalb des Hauses erweitert werden. Auch das Wiedereinspielen von Backups soll getestet werden. Damit sollen die Risiken von Bedrohungen, die zu einem Datenverlust führen, entschärft werden.

Der dritte Sicherheitsbereich beschäftigt sich mit der Authentifizierung und Autorisierung. Hier wird die Einrichtung von einem Benutzerkonto pro Mitarbeiter vorgeschlagen. Diese sollen, nach dem Prinzip der geringsten Privilegien, möglichst wenige Rechte haben und einen sicheren Authentifizierungsmechanismus besitzen. Darüber hinaus soll mit der automatischen Aktivierung der Bildschirmsperre der unautorisierte Zugriff auf Clients verhindert werden.

Anschließend wird im „Protection Strategy Worksheet“ (s. Anhang H, S. 23ff., „Step 29“) erhoben, ob die neuen Maßnahmen einen Einfluss auf die Sicherheitsbereiche der Schutzstrategie haben und diese verändern (Prozess 5.4).

So führt zum Beispiel das Einführen von IT-Sicherheitstrainings oder das Aufstellen eines Notfallmanagements in der Zahnarztpraxis dazu, dass sich die Schutzstrategie in den jeweiligen Bereichen ändert. Im Gegensatz dazu führt die Maßnahme einer automatischen Bildschirmsperre nicht zu einer Änderung der Schutzstrategie im Sicherheitsbereich der Authentifizierung und Autorisierung. Eine Änderung würde erst vorliegen, wenn die Verfahren in diesem Bereich dokumentiert werden.

Abschließend werden auf dem „Next Steps Worksheet“ (s. Anhang H, S. 129ff., „Step 30“) die weiteren Schritte festgelegt (Prozess 5.5). Hierzu gehört die Überprüfung des Fortschritts bei der Implementierung der Maßnahmen in der Zahnarztpraxis, was monatlich erfolgen soll. Eine Erweiterung der OCTAVE-S-Umsetzung um weitere Assets ist aktuell nicht geplant, soll aber nach der Implementierung der aktuellen Maßnahmen erneut geprüft werden. Auch einer erneute Durchführung von OCTAVE-S ist gegenwärtig nicht geplant.

4.3 Aspekte des B3S „Medizinische Versorgung“

Mit den Schutzzielen der Patientensicherheit und der Versorgungseffektivität sowie den Kritikalitätsklassen zur Priorisierung der Risikobewertung etabliert der B3S „Medizinische Versorgung“ Kriterien, die die Risikoanalyse des Standards für Krankenhäuser anpassen. Nachfolgend wird der Schutzbedarf in Bezug auf die Patientensicherheit und die Versorgungseffektivität für die Zahnarztpraxis erhoben. Anschließend werden die IT-Systeme in eine Kritikalitätsklasse bezüglich der medizinischen Versorgung der Patienten erhoben. Zunächst wird jedoch auf die Definitionen der Begriffe geblickt.

Die Patientensicherheit bezieht sich die physische und psychische Gesundheit von Menschen. Bei einer Beeinträchtigung dieser mit „unvertretbaren Risiken“ wird das Schutzziel verletzt. [9, S. 9]

Die Behandlungseffektivität hat das Ziel, dass die „Prozesse und Informationen zur medizinischen Behandlung“ der Patienten effektiv zusammenwirken und der Informationsaustausch sichergestellt ist. [9, S. 9]

Die Kritikalität der Schutzobjekte für die Patientensicherheit und die Behandlungseffektivität wird danach bewertet, ob eine Beeinträchtigung des Schutzziels bei Problemen mit dem Schutzobjekt wahrscheinlich ist. Dafür werden die Kategorien „geringe Gefährdung“, „mittlere Gefährdung“ und „hohe Gefährdung“ vorgeschlagen. [9, S. 9]

Die Kritikalität von Systemen wird mit einer Kategorisierung in drei Klassen bestimmt. Die Klassen geben an, ob ein Ausfall des Systems nur kurz-, mittel- oder langfristig kompensiert werden kann. Im Standard wird dies für Systeme der Informationstechnik, Medizintechnik, Kommunikationstechnik und Versorgungstechnik vorgenommen. [9, S. 50f.]

Im Standard werden auch die Anforderungen an die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit bewertet. Die beiden branchenspezifischen Schutzziele sollen bei der Bewertung der allgemeinen Schutzziele einbezogen werden. Die Kritikalitätsklassen dienen wiederum zur Priorisierung bei der Risikobewertung. [9, S. 45ff.]

In Tabelle 26 sind die in der Strukturanalyse des IT-Grundschutzes erhobenen Zielobjekte dargestellt. Für diese soll festgestellt werden, welchen Einfluss eine Beeinträchtigung des Schutzobjektes auf die Schutzziele der Patientensicherheit und die Behandlungseffektivität hat. Darüber hinaus werden die IT-Systeme und Kommunikationsverbindungen in Kritikalitätsklassen eingeteilt. Diese Ergebnisse werden mit dem Schutzbedarf der allgemeinen Schutzziele aus dem IT-Grundschutz verglichen.

Tabelle 26: Schutzbedarf an Patientensicherheit und Behandlungseffektivität und Kritikalitätsklasse für Zielobjekte der Zahnarztpraxis

Kürzel	Schutzobjekt	Patientensicherheit	Behandlungseffektivität	Kritikalitätsklasse (nur IT-Systeme)
GP001	Terminvereinbarung	mittel	hoch	
GP002	Patientenaufnahme	hoch	hoch	
GP003	Untersuchung und Behandlung	hoch	hoch	
GP004	Aufbereitung von Material/Werkzeug und Praxishygiene	hoch	hoch	
GP005	Labortätigkeiten	gering	hoch	
GP006	Personalmanagement/-verwaltung	mittel	gering	
GP007	Dokumentation	hoch	hoch	
GP008	Abrechnung	gering	mittel	
GP009	Einkauf/Materialbestellung	gering	mittel	
GP010	IT-Betrieb	mittel	hoch	
GP011	Wartung und Unterweisung	mittel	mittel	
GP012	Kommunikation mit Laboren und Kollegen	hoch	hoch	
A001	Textverarbeitung, Präsentation, Tabellenkalkulation	gering	mittel	
A002	E-Mail-Client	gering	mittel	
A003	Webbrowser	gering	gering	
A004	PDF-Reader	gering	gering	
A005	Fernwartung	gering	mittel	
A006, A006a, A006b	Backup, Veeam, Hyper Backup	gering	mittel	
A007	Voice over IP	gering	hoch	
A008	Active Directory Domain Services	mittel	hoch	
A009	Fileserver	mittel	hoch	
Am001	Praxisverwaltung	mittel	hoch	

Am002	Schnittstelle Telematikinfrastruktur	mittel	mittel	
Am003	Abrechnungshilfe	gering	gering	
Am004, Am004a, Am004b	Röntgensoftware, Sidexis, VistaScan	hoch	hoch	
Am006	Monitorprüfung	gering	gering	
Am007	Digitale Planungshilfe	gering	gering	
C001	Client Anmeldung	gering	hoch	Klasse 2
C002	Clients Behandlungszimmer	gering	hoch	Klasse 2
C003	Client Büro	mittel	hoch	Klasse 1
D001	Multifunktionsdrucker (Anmeldung)	gering	mittel	Klasse 3
D002	Drucker (Büro)	gering	gering	Klasse 3
N001	Router zum Internet	mittel	mittel	Klasse 2
N002/M001	Ti-Konnektor	mittel	mittel	Klasse 2
N003	Switch (Keller)	hoch	hoch	Klasse 1
N004	Switch (Büro)	hoch	hoch	Klasse 1
N005	Switch (Anmeldung)	mittel	hoch	Klasse 2
N007	Heizkörpersteuerung	gering	gering	Klasse 3
M002	Kartenlesegerät	gering	mittel	Klasse 2
M003	Röntgen (Orthophos SL)	hoch	hoch	Klasse 1
M004	Röntgen (Vistascan)	hoch	hoch	Klasse 1
M005	Aufbereitungsgerät MELAG Vacuclave 118	hoch	hoch	Klasse 2
S001	Server	hoch	hoch	Klasse 1
S001a	Domänen-Controller	mittel	hoch	Klasse 1
S001b	Fileserver	mittel	hoch	Klasse 1
S002	Backupspeicher	gering	mittel	Klasse 2
T001	Telefonanlage	gering	gering	Klasse 3
T002	Telefon (VoIP)	gering	hoch	Klasse 2
T003	Telefon (ISDN)	gering	gering	Klasse 3
O001	Thermostat	gering	gering	Klasse 3

O002	KZV-Abrechnungs-stick	gering	gering	Klasse 3
O003	USB-Stick (Aufbe-reitungsgerät)	gering	gering	Klasse 3
K001	Internetanschluss	mittel	mittel	Klasse 2
K002	Verbindungen zwi-schen Netzkompo-nenten innerhalb der Praxis	hoch	hoch	Klasse 1
K003	Verbindungen zwi-schen Switches und dem Server	hoch	hoch	Klasse 1
K004	Verbindungen zwi-schen Switches und Clients	mittel	hoch	Klasse 1
K005	Verbindungen zwi-schen Switches und Medizingeräten	hoch	hoch	Klasse 1
K006	Verbindung zwi-schen Router und VoIP-Telefon	gering	hoch	Klasse 2
K007	WLAN Heizkörper-steuerung	gering	gering	Klasse 3

Bei der Schutzbedarfsfeststellung des IT-Grundschutzes werden mit dem Schadensszenario „persönliche Unversehrtheit“ mögliche Gefahren für die Gesundheit von Personen berücksichtigt. Vergleichbar ist das Szenario mit dem Schutzziel Patientensicherheit des B3S „Medizinische Versorgung“, der dieses Schutzziel zusätzlich für Zielobjekte bewertet. Aspekte des speziellen Schutzziels der Behandlungseffektivität lassen sich im IT-Grundschutz im Schadensszenario „Aufgabenerfüllung“ wiederfinden. Da die Schutzziele des IT-Grundschutzes auf Basis der Schadensszenarien bewertet werden, fließen diese Aspekte in die Bewertung der allgemeinen Schutzziele ein. Jedoch können mit der gesonderten Erhebung der Patientensicherheit und Behandlungseffektivität im B3S „Medizinische Versorgung“ spezifische Anforderungen der Branche und der kritischen Dienstleistung in den Fokus gerückt und die Risikoanalyse an die Branche angepasst werden.

Beim Vergleich der Kritikalitätsklasse mit dem Schutzbedarf der Verfügbarkeit aus der Bearbeitung des IT-Grundschutzes kann eine hohe Übereinstimmung beobachtet werden. Bei 29 von 32 Zielobjekten stimmt die erste Kritikalitätsklasse mit einem sehr hohen Schutzbedarf, die zweite Kritikalitätsklasse mit einem hohen Schutzbedarf und die dritte Kritikalitätsklasse mit einem normalen Schutzbedarf überein.

Unterschiede gibt es lediglich bei der VoIP-Telefonie und dem USB-Stick des Aufbereitungsgerätes. Das VoIP-Telefon (T002) und dessen Kommunikationsverbindung (K006) werden aufgrund deren Bedeutung für die Geschäftsprozesse der Terminvereinbarung (GP001) und der Kommunikation mit Laboren und Kollegen (GP012) in die zweite Klasse eingeordnet. Der Schutzbedarf nach IT-Grundschutz wurde aufgrund möglicher Alternativen als normal eingeschätzt. Mit dieser Argumentation wäre auch eine Einordnung in die dritte Klasse denkbar.

Der Schutzbedarf der Verfügbarkeit nach IT-Grundschutz für den USB-Stick des Aufbereitungsgerätes (O003) wird nach dem Maximumprinzip als hoch eingeschätzt. Im Gegensatz dazu wird er in die dritte Kritikalitätsklasse eingeordnet, da er lediglich die Aufbereitungsvorgänge dokumentiert und einfach ersetzt werden kann.

Je nachdem wie man die kurz-, mittel- und langfristige Kompensationsmöglichkeit bei den Kritikalitätsklassen definiert, können diese also mit Verfügbarkeitskategorien übereinstimmen. Es bleibt zu beachten, dass die Bestimmung der Kritikalitätsklasse nicht im vorgesehenen Gebiet eines Krankenhauses angewendet wurde. Die Kritikalitätsklassen beziehen sich ausschließlich auf die kritische Dienstleistung, während der Schutzbedarf der Verfügbarkeit einer Institution auch weitere Geschäftsbereiche und Aspekte eines Unternehmens einbeziehen kann. Auch eine andere Definition der Anforderungen an die Verfügbarkeit kann zu anderen Ergebnissen führen oder die Vergleichbarkeit zwischen den Anforderungen an die Verfügbarkeit und den Kritikalitätsklassen erschweren.

4.4 Aspekte der ISO/IEC 27005

Im folgenden Kapitel wird der ereignisbasierte Ansatz zur Risikoidentifizierung der ISO/IEC 27005 beispielhaft dargestellt.

Als zugrundeliegendes Ereignis dient ein Ransomware-Angriff. Bei einem solchen Angriff werden mit Schadprogrammen Daten von Computersystemen verschlüsselt, der Zugriff auf diese blockiert und ein Lösegeld gefordert [90]. In der Zahnarztpraxis könnte ein solcher Angriff den Server und die Clients betreffen und damit die Verfügbarkeit und Vertraulichkeit verletzt werden.

Zu Beginn werden mögliche Risikoquellen ermittelt. Die Norm charakterisiert Risikoquellen nach Motivation und Fähigkeiten und nennt einige Beispiele. Im Szenario eines Ransomware-Angriffs auf die Zahnarztpraxis kommen besonders cyberkriminelle Gruppierungen mit einem hohen Organisationsgrad in Frage. Bei diesen besteht das Motiv meist darin, sich finanziell zu bereichern. Auch terroristisch oder staatlich organisierte Angriffe, die gezielt die Gesundheitsversorgung einschränken sollen, sind denkbar. [20, S. 62ff.]

Mögliche Angriffswege, über welche eine Ransomware in die Zahnarztpraxis eindringen könnte, sind infizierte E-Mail-Anhänge oder infizierte Webseiten [91]. Auch die Ausnutzung

von Sicherheitslücken in Programmen muss beachtet werden. Als Angriffspunkte kommen beispielsweise die Clients in der Anmeldung und im Büro in Betracht, auf welchen E-Mails empfangen und Material bestellt wird. Von diesen aus könnte sich die Ransomware im Praxisnetzwerk ausbreiten und den Server sowie die Backup-Systeme befallen. [6]

Ein erfolgreicher Angriff könnte zentrale Geschäftsprozesse wie die Behandlung von Patienten unterbrechen und zu einem erheblichen Reputationsverlust führen. Es besteht die Gefahr, dass die gespeicherten Patientendaten unwiederbringlich verloren gehen oder veröffentlicht werden. Durch die Wiederherstellung der IT-Systeme und Ausfälle könnten sehr hohe Kosten entstehen. Auch rechtliche Konsequenzen könnten beispielweise bei Datenschutzverstößen folgen. Nach den im Kapitel zur Evaluation des IT-Grundschutzes eingeführten Bewertungskategorien wird daher der mögliche Schaden als „existenzbedrohlich“ eingeschätzt.

Nach Einschätzung des BSI im Lagebericht zur IT-Sicherheit in Deutschland aus dem Jahr 2023 sind Ransomware-Angriffe gegenwärtig die größte Bedrohung aus dem Bereich der Cyberkriminalität [6]. Eine Studie des Branchenverbands Bitkom e.V. aus dem Jahr 2024 berichtet, dass 60 Prozent der befragten Unternehmen in einem Zeitraum von zwölf Monaten mit Ransomware angegriffen wurden [92]. Auf ein ähnliches Ergebnis von 59 Prozent kommt auch der „Sophos Ransomware-Report 2024“ [93]. Aufgrund dieser Studien und den gegenwärtig unzureichenden Sicherheitsmaßnahmen wird die Eintrittshäufigkeit als „hoch“ bewertet. Das daraus resultierende Risiko ist „sehr hoch“.

Zur Reduktion des Risikos kommen einige Maßnahmen in Betracht. Dazu gehören die schon in den vorhergehenden Kapiteln erwähnten Maßnahmen zum Updatemanagement, zur Einführung von IT-Sicherheitsschulungen, zur Einführung von sicheren Authentifizierungsmechanismen und zur Erweiterung des Datensicherungskonzeptes. Darüber hinaus sollte ein Virenschutzprogramm genutzt werden.

Als potentiell größte Angriffsfläche werden die Clients angesehen, auf denen E-Mails abgerufen werden. Um eine Ausbreitung von diesen ins Praxisnetz zu verhindern, könnten Clients, die E-Mails abrufen, mittels einer physischen Trennung isoliert werden. Dazu muss mindestens ein zusätzlicher Client außerhalb des Praxisnetzes zum Empfang von Mails bereitgestellt werden. In diesem Fall muss ein Verfahren zum Austausch der Daten zwischen Praxisnetz und dem Client zum Abrufen der E-Mails entwickelt werden. Alternativ kann zum Abrufen von E-Mails auch die Einrichtung einer virtuellen Umgebung geprüft werden.

Mit diesen Maßnahmen soll sowohl die Wahrscheinlichkeit reduziert werden, dass ein Angriff erfolgreich ist, als auch der resultierende Schaden reduziert werden, indem eine Ausbreitung der Ransomware erschwert wird.

4.5 STRIDE/DREAD

Zur praktischen Anwendung von STRIDE/DREAD wird die Nutzung eines Clients (zum Beispiel in einem Behandlungszimmer), der mit dem Server-Message-Block-Protokoll (SMB) auf einen freigegebenen Ordner des Fileservers zugreift, modelliert (s. Abbildung 19). Dazu wird das „Threat Modeling Tool“ von Microsoft [81] genutzt.

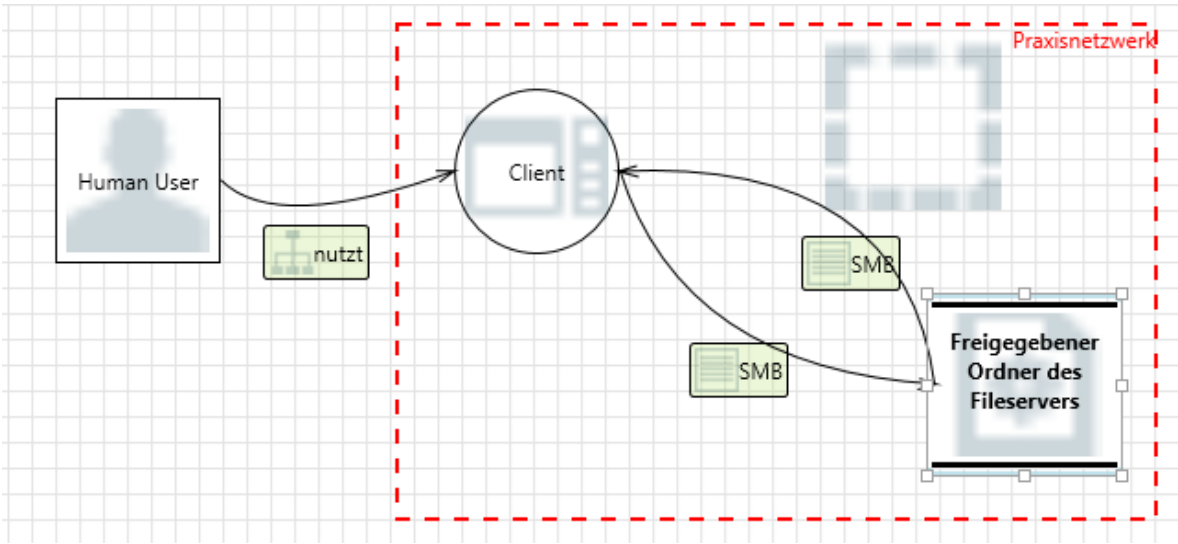

Abbildung 19: Darstellung eines Ausschnitts des Praxisnetzwerks mit dem Threat Modeling Tool

Das „Threat Modeling Tool“ generiert basierend auf den STRIDE-Kategorien automatisiert Bedrohungen. Für das oben zu sehende Modell konnten insgesamt 14 Bedrohungen ermittelt werden. Ein Beispiel für eine solche Bedrohung ist, dass dem Client vorgetäuscht wird, dass es sich bei dem Nutzer um eine der berechtigten Personen handelt. Dies könnte zu einer unbefugten Nutzung des Clients führen. Das „Threat Modeling Tool“ weist hierbei darauf hin, dass ein Authentifizierungsmechanismus angewendet werden sollte.

Nachfolgend wird die oben genannte Bedrohung mit dem DREAD-Modell bewertet. Die Bewertung findet anhand der fünf Kategorien Schaden, Reproduzierbarkeit, Ausnutzbarkeit, betroffene Nutzer und Auffindbarkeit statt. Dabei werden die in Tabelle 3 dargestellten Bewertungskriterien genutzt.

Wenn ein Angreifer Zugriff auf einen Client hat, könnte er Daten, die sich auf dem Client oder dem Server befinden, löschen. Daher wird die Kategorie „Schaden“ mit zehn Punkten bewertet.

Sofern der Client eingeschaltet ist, ist ein Angriff sehr leicht reproduzierbar, da aktuell keine Bildschirmsperre verwendet wird. Aus diesem Grund wird die Kategorie „Reproduzierbarkeit“ mit zehn Punkten bewertet.

Aufgrund fehlender Sicherheitsmaßnahmen wie einer Bildschirmsperre, kann ein Angriff bei eingeschaltetem Client ohne besondere Fähigkeiten oder Tools durchgeführt werden. Die Ausnutzbarkeit wird mit zehn Punkten bewertet.

Ein Angreifer kann Daten löschen, die alle Patienten betreffen. Daher wird die Kategorie „betroffene Nutzer“ mit zehn Punkten bewertet.

Die Bedrohung und damit zusammenhängende Schwachstellen können sehr einfach gefunden werden. Daher wird die Auffindbarkeit mit zehn Punkten bewertet.

Mit einem Gesamtergebnis von 50 Punkten wird die Bedrohung als kritisch bewertet.

Für die ermittelte Bedrohung müssen nun Gegenmaßnahmen entwickelt werden. Dabei kommen die bereits bei anderen Konzepten erwähnten Maßnahmen einer Bildschirmsperre, der zwei-Faktor-Authentifizierung und die Forderung, starke Passwörter zu nutzen, in Frage. Damit könnten die Reproduzierbarkeit und die Ausnutzbarkeit erheblich reduziert werden. Mit der Einführung eines Berechtigungskonzeptes, wonach dem Nutzer nur die nötigen Rechte gegeben werden, kann der Schaden reduziert werden.

4.6 Diskussion der Evaluation

Am Beispiel einer Zahnarztpraxis kann aufgezeigt werden, wie mit unterschiedlichen Standards Risiken identifiziert, bewertet und Maßnahmen zu deren Behandlung entwickelt werden können. Im Allgemeinen erwies sich die Zuteilung von Ressourcen in Form von Arbeitszeit für die Zahnarztpraxis als schwierig. Das Ausfüllen von Fragenkatalogen und das Einholen von Informationen zur Praxis musste zusätzlich zur eigentlichen Arbeitszeit erledigt werden.

Mit der Anwendung der Konzepte konnten einige Sicherheitsmängel festgestellt werden. Darunter kann zum Beispiel die fehlende Bildschirmsperre genannt werden. Aus Sicherheitsperspektive sind die aufgeführten Maßnahmen notwendig. Aus Sicht des Praxisbetreibers besteht die Gefahr, dass die Produktivität eingeschränkt wird und andere Richtlinien erschwert oder verletzt werden. In diesem Beispiel und auch bei den anderen Maßnahmen muss nach deren Implementierung überprüft werden, wie diese aufgenommen werden. Für den Fall, dass diese nicht angenommen werden, müssen diese angepasst oder Alternativen gefunden werden.

Gründe für den Sicherheitszustand der Praxis können darin gesehen werden, dass sich die Praxis bereits durch die Vielzahl anderer bürokratischer Aufgaben überfordert sieht. Zur Einrichtung der IT-Systeme wird die Zahnarztpraxis von einem Hardware-Dienstleister betreut. Dessen Angebote im Bereich der IT-Sicherheit waren der Praxis bisher nicht bekannt.

Zur Bearbeitung des IT-Grundschutzes des BSI wird die Standard-Vorgehensweise gewählt. Dies ist die umfassendste Variante, welche jedoch mit dem höchsten Aufwand

verbunden ist. Bei den erhobenen Maßnahmen handelt es sich um ein erstes Paket. Dieses sollte nicht zu groß sein, damit die Zahnarztpraxis nicht mit zu vielen Maßnahmen überfordert wird. Im weiteren Verlauf müssen verbleibende Anforderungen erfüllt und weitere Risiken mit Maßnahmen gemildert werden. Dies ist gerade in der Standard-Absicherung inklusive der Risikoanalyse sehr aufwändig. Eine Alternative mit einem etwas verringertem Aufwand bietet der IT-Grundschutz mit der Basis-Absicherung an.

Mögliche Anpassungen des bisherigen Vorgehens könnte die Schutzbedarfskategorien betreffen. Gegenwärtig werden finanzielle Auswirkungen von 1.000 Euro bis 30.000 Euro als „hoch“ definiert. Dieser große Bereich könnte weiter differenziert werden, um eine genauere Einordnung möglicher Schäden vornehmen zu können. Andererseits könnten zusätzliche Kategorien wiederum die Einschätzung erschweren.

OCTAVE-S ist für kleine Unternehmen mit unter 100 Mitarbeitern konzipiert. Trotzdem wirkten einige Fragen und Anforderungen, die sich daraus ergeben, für den konkreten Anwendungsfall der Zahnarztpraxis überdimensioniert. Auch der Umstand, dass es in der Zahnarztpraxis kein IT-Personal gibt, erschwerte die Bearbeitung des Standards. So erwies es sich als schwierig, Unterschiede der einzelnen strategischen Sicherheitsbereiche den Mitarbeitern zu verdeutlichen und Handlungen der Praxis in Bezug auf diese zu erheben.

Die Eintrittswahrscheinlichkeit einer Bedrohung wurde bei der Bearbeitung des OCTAVE-S-Standards nicht erhoben. Bei der Auswahl der Behandlungsansätze für die Risiken konnte beobachtet werden, dass dieser Aspekt trotzdem intuitiv abgeschätzt und in die Entscheidung einbezogen wird, ohne die Eintrittswahrscheinlichkeit formal zu bestimmen. An dieser Stelle ist auch die erhobene Anzahl der bisher aufgetretenen Bedrohungen hilfreich.

Betrachtete Aspekte des B3S „Medizinische Versorgung“ sind die beiden branchenspezifischen Schutzziele der Patientensicherheit und der Behandlungseffektivität sowie die Kritikalitätsklassen. Auch wenn Kriterien, die in die Bewertung der branchenspezifischen Schutzziele einfließen, bereits in die Bewertung der allgemeinen Schutzziele aufgenommen wurden, können branchenspezifische Schutzziele die besonderen Sicherheitsanforderungen einer Organisation in den Mittelpunkt rücken und die Risikoanalyse individualisieren. Eine Priorisierung anhand der Kritikalitätsklassen rückt den Schutz der kritischen Dienstleistung in den Vordergrund. Im Beispiel der Zahnarztpraxis konnten nur bedingt Unterschiede zwischen den Kritikalitätsklassen und dem Schutzbedarf an die Verfügbarkeit festgestellt werden. Dabei müssen die genannten Beschränkungen beachtet werden.

Im Hinblick auf die ISO/IEC-Norm 27005 wurde der darin beschriebene ereignisbasierte Ansatz zur Risikoidentifizierung angewendet. Diesem steht der wertbasierte Ansatz gegenüber, welcher von der Risikoanalyse des IT-Grundschutzes und OCTAVE-S verfolgt wird. Vorteile des Ereignisbasierten sind ein geringerer Aufwand und eine Fokussierung auf kritische Risiken. Im Gegensatz dazu kann man mit dem wertbasierte Ansatz über die Erhebung aller Assets und der Analyse der Schwachstellen und Bedrohungen Risiken systematisch erheben, gezielte Maßnahmen treffen und die Wahrscheinlichkeit verringern, dass

Risiken übersehen werden. Hierbei muss man sich nicht für einen Ansatz entscheiden, sondern kann diese kombinieren. [94]

Mit der Kombination von STRIDE und DREAD werden zwei Konzepte aus dem Bereich des Threat Modeling angewendet. Mit der Modellierung eines Ausschnitts der Praxis wird eine Bedrohung identifiziert, die bereits mit dem IT-Grundschutz des BSI und mit OCTAVE-S erkannt wurde. Dies zeigt auf, dass mit unterschiedlichen Ansätzen zum Teil ähnliche Ergebnisse erzielt werden können.

5 Diskussion und Fazit

In dieser Arbeit werden die Risikoanalysekonzepte des IT-Grundschutzes, von OCTAVE-S, des B3S „Medizinische Versorgung“, der ISO/IEC-Norm 27005 und die Threat-Modeling-Ansätze STRIDE und DREAD vorgestellt und im Hinblick auf die Eignung für KMU und der einzelnen Schritte der Risikoanalyse verglichen. Abschließend werden am Beispiel einer Zahnarztpraxis der IT-Grundschutz und OCTAVE-S angewendet sowie Aspekte des B3S „Medizinische Versorgung“ und der ISO/IEC-Norm 27005 evaluiert.

Anhaltspunkte für die Eignung der Standards für KMU liefert die von Mark Le Corre entwickelte Tauglichkeitsprüfung [74]. Hier werden Bewertungen anhand festgelegter Merkmale durchgeführt. Alle vier Standards erfüllen die Kompatibilitätskriterien überwiegend. Mit 79,7 Prozent erzielt die ISO/IEC-Norm 27005 das beste Ergebnis. Dicht dahinter folgt der BSI-Standard 200-3 mit 78,1 Prozent. Auf dem geteilten dritten Platz befinden sich der B3S „Medizinische Versorgung“ und der OCTAVE-S-Standard mit 70,3 Prozent. Damit weist die ISO/IEC-Norm 27005 die höchste KMU-Tauglichkeit auf. Bei den Kriterien „Vollständigkeit“, „Aufbau“, „Wirtschaftlichkeit“ und „Überprüfbarkeit der Anforderungen“ und damit bei vier von fünf Kategorien gehört die Norm zu den bestbewerteten Standards.

Bei der Auswahl eines Standards spielen jedoch weitere Faktoren eine Rolle. So kann ein auf die spezielle Branche zugeschnittener Standard wie der B3S „Medizinische Versorgung“ den Aufwand reduzieren und das Informationssicherheitsmanagement und die Risikoanalyse an die Branche anpassen. Dies macht der Sicherheitsstandard mit branchenspezifischen Schutzzielen und den Kritikalitätsklassen. Darüber hinaus gibt er dem Anwender hilfreiche Informationen über krankenhaustypische Systeme und spezielle Gefährdungen für die Branche.

Der IT-Grundschutz des BSI bietet mit der Möglichkeit zur Auswahl zwischen verschiedenen Vorgehensweisen KMU die Möglichkeit, das Handeln an den individuellen Bedarf anzupassen. Die Risikoanalyse des IT-Grundschutzes kommt in den Vorgehensweisen der Standard-Absicherung und Kern-Absicherung zum Einsatz. Aufgrund der bereits durch das BSI durchgeführten Risikoanalyse für Schutzobjekte mit normalen Schutzbedarf muss diese nicht für alle Schutzobjekte durchgeführt werden. Nach Angaben des BSI stellt diese Risikoanalyse einen vereinfachten Ablauf dar [3, S. 155].

Im Vergleich zum IT-Grundschutz, der das Vorgehen konkreter ausführt, ist die ISO/IEC-Norm eher allgemein gehalten. Dabei werden auf verschiedene Möglichkeiten beim Vorgehen im Risikomanagement eingegangen. So beschreibt die Norm den ereignisbasierten und den wertbasierten Ansatz und zeigt Möglichkeiten für eine quantitative Risikobeurteilung auf.

Im Hinblick auf KMU stellt OCTAVE-S einen für kleinere Unternehmen konzipierten Standard dar. Die strukturierte Form der Schritte, die in abzuarbeitenden Arbeitsblättern vorliegen, vereinfacht die Bearbeitung für den Anwender. Hier ist zu beachten, dass der Standard nur in der englischen Sprache vorliegt und zuletzt im Jahr 2005 aktualisiert wurde. Der Standard gibt einen Überblick über den aktuellen Stand in den Sicherheitsbereichen der Organisation und ermöglicht, die Sicherheit für kritische Assets zu verbessern, muss jedoch in einen Managementrahmen eingebunden werden. [62]

Die Vereinfachung, die der OCTAVE-S-Standard mit seinen Arbeitsblättern ermöglicht, könnte heutzutage für andere Standards erreicht werden, indem in ISMS-Tools für unerfahrene Benutzer oder bestimmte Branchen eine ebenso enge Begleitung durch einen Standard integriert wird.

Mit STRIDE und DREAD werden Threat-Modeling-Ansätze vorgestellt, mit denen Bedrohungen und Schwachstellen identifiziert und bewertet werden. Diese können die jeweiligen Risikoanalyseschritte der Standards ergänzen oder in einem eigenständigen Threat-Modeling-Prozess das Sicherheitsniveau verbessern.

Welcher Standard für ein KMU am besten geeignet ist, hängt letztendlich von vielen Faktoren ab. So können Partnerunternehmen bestimmte Standards und deren Zertifizierung fordern. Auch rechtliche Anforderungen, die beispielsweise mit der NIS-2-Richtlinie steigen werden, können die Einführung eines Risiko- und Informationssicherheitsmanagements notwendig machen. Je nach Branche und Unternehmensgröße können branchenspezifische oder komprimierte Standards von Vorteil sein. Dabei muss beachtet werden, dass die Informationssicherheit kein einmal zu erreichender Zustand ist, sondern ein Prozess, der ständig aufrechterhalten und weiterentwickelt werden muss.

Das Betreiben eines ISMS und die Durchführung einer Risikoanalyse sind immer mit einem gewissen Aufwand verbunden und benötigen entsprechendes IT-Fachwissen. Für KMU, die kein eigenes IT-Personal haben, stellt dies eine besondere Herausforderung dar. Für diese könnte die Unterstützung durch einen externen Informationssicherheitsbeauftragten in Frage kommen. Dieser kann beim Aufbau eines ISMS unterstützen und dem Etablieren von Sicherheitsmaßnahmen behilflich sein.

Deutlich ist dies bei der in dieser Arbeit untersuchten Zahnarztpraxis. Hier wurden Fragen der Informationssicherheit bisher nicht ausreichend beachtet. Dass es sich bei dieser Praxis um keinen Einzelfall handelt, verdeutlichen die in der Einleitung aufgeführten Studien des BSI. Danach sind die rechtlichen Anforderungen an Zahnarztpraxen, die in Form einer IT-Sicherheitsrichtlinie vorliegen, nur 58 Prozent der Befragten bekannt und etwa ein Drittel gibt an, diese vollständig umgesetzt zu haben. Auch konnten Schwachstellen festgestellt werden, die sowohl in vielen der befragten Praxen als auch in der in dieser Arbeit untersuchten Praxis bestehen. [12] [13]

Nach einer Umfrage des Zentralinstituts für die Kassenärztliche Versorgung in Zusammenarbeit mit der Kassenzahnärztlichen Bundesvereinigung (KZBV) fühlen sich knapp 97 Prozent der befragten Zahnärztinnen und Zahnärzten durch die Vielzahl an bürokratischen Aufgaben überlastet. Die Digitalisierung wird nicht als Hilfe betrachtet, sondern führt nach Angaben der Befragten bei 81 Prozent zu einer Beeinträchtigung des Praxisalltags. [95]

Dennoch ist es notwendig, dass die IT-Sicherheit ausreichend beachtet und in die Praxisabläufe integriert wird. Wichtig für Organisationen wie Zahnarztpraxen ist, dass zunächst ein Problembewusstsein geschaffen wird und mögliche Konsequenzen und Gefahren bekannt sind. Es sollten niedrigschwellige Angebote verfügbar sein und an die Unternehmen herangetragen werden, damit im Fall von Arzt- und Zahnarztpraxen die IT-Sicherheitsrichtlinie flächendeckend umgesetzt wird [12].

Für die in dieser Arbeit untersuchte Zahnarztpraxis hat die Einhaltung der Anforderungen der IT-Sicherheitsrichtlinie nach § 390 SGB V die primäre Priorität. Der mit dieser Arbeit gestartete IT-Grundschutz-Prozess wird zunächst weitergeführt. Zu einem langfristigen Betrieb eines vollwertigen ISMS nach IT-Grundschutz oder nach der ISO/IEC-Norm 27001 sieht sich die Zahnarztpraxis alleine jedoch nicht in der Lage. Damit die untersuchte und auch weitere Praxen ein ISMS betreiben, könnte ein auf die Anforderungen einer Zahn- oder Arztpraxis angepasster und komprimierter Standard etabliert werden, bei dessen Umsetzung die Praxen unterstützt werden.

Die Erstellung eines solchen Standards zum Beispiel in Form eines IT-Grundschutz-Profils stellt einen möglichen Ansatz für weitere Forschungsarbeiten dar. Die in dieser Arbeit untersuchte Zahnarztpraxis gehört zu den Kleinstunternehmen. Damit werden die Standards nur an der kleinsten Kategorie von KMU angewendet. Eine Evaluation der Standards sollte daher auch an kleinen und mittleren Unternehmen vorgenommen werden. Ebenfalls könnten Unternehmen anderer Branchen untersucht werden. Dies muss nicht nur im Hinblick auf die hier aufgeführten Standards erfolgen, sondern könnte auch weitere Standards wie das „NIST Risk Management Framework“ [96] als allgemeines Risikomanagementkonzept oder die Richtlinie „VdS 10000 – Informationssicherheits-Managementsystem für kleine und mittlere Unternehmen (KMU)“ [97] als für KMU konzipierter Standard einschließen.

Die Einrichtung eines Praxisnetzwerks übernehmen häufig externe Dienstleister, da den Betreibern Zeit und Fachkenntnisse dafür fehlen. Eine Kontrolle oder Überwachung der Arbeit des IT-Dienstleisters ist für den Praxisbetreiber im Allgemeinen nicht möglich, so dass er sich auf dessen Kompetenzen verlassen können muss.
Die Einbindung von IT-Dienstleistern in Sicherheitsvorgaben stellt einen möglichen Ansatz dar. So könnten IT-Dienstleister verpflichtet werden hinsichtlich der IT-Sicherheitsrichtlinie zu beraten und Installationen im Einklang mit dieser IT-Sicherheitsrichtlinie durchzuführen.

Trotz des hohen Aufwands, der mit dem Betrieb eines ISMS, der Durchführung einer Risikoanalyse und dem Etablieren von Maßnahmen einhergeht, müssen Sicherheitsbetrachtungen in Unternehmensabläufe integriert werden. Die enorme Bedeutung von

Informationstechnik und die damit verbundenen Gefahren erfordern eine hohe Aufmerksamkeit. Denn für die Cybersicherheit gilt dasselbe wie für die Zähne: Vorsorge ist besser als Nachsorge.

Literaturverzeichnis

[1] Bitkom e.V., „Wirtschaftsschutz 2023“. 2023. [Online]. Verfügbar unter: https://www.bitkom.org/sites/main/files/2023-09/Bitkom-Charts-Wirtschaftsschutz-Cybercrime.pdf. [Zugriff am 11.09.2024].

[2] Deutsche Industrie- und Handelskammer, „Digitalisierung weiter eher Werkzeug als Innovationsmotor - Die DIHK-Digitalisierungsumfrage 2023“. 2024. [Online]. Verfügbar unter: https://www.dihk.de/de/themen-und-positionen/wirtschaft-digital/digitalisierung/digitalisierungsumfrage-23. [Zugriff am 12.09.2024].

[3] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-3 - Risikoanalyse auf der Basis von IT-Grundschutz, V1.0“. 2017. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2. [Zugriff am 13.09.2024].

[4] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kompendium“. 2023. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf?__blob=publicationFile&v=4#download=1. [Zugriff am 13.09.2024].

[5] Statistisches Bundesamt (Destatis), „55 % in kleinen und mittleren Unternehmen tätig“. [Online]. Verfügbar unter: https://www.destatis.de/DE/Themen/Branchen-Unternehmen/Unternehmen/Kleine-Unternehmen-Mittlere-Unternehmen/aktuell-beschaeftigte.html. [Zugriff am 11.09.2024].

[6] Bundesamt für Sicherheit in der Informationstechnik, „Die Lage der IT-Sicherheit in Deutschland 2023“. 2023. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2023.html?nn=129410. [Zugriff am 11.09.2024].

[7] Deutschland sicher im Netz, „DsiN-Praxisreport 2021/22 Mittelstand@IT-Sichereit“. 2022. [Online]. Verfügbar unter: https://www.sicher-im-netz.de/dsin-praxisreport-202122-mittelstand-it-sicherheit. [Zugriff am 11.09.2024].

[8] Bundesamt für Sicherheit in der Informationstechnik, „Tätigkeitsbericht Gesundheit - Cybersicherheit im Gesundheitswesen 2023“. 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Taetigkeitsbericht_Gesundheit_2023.pdf?__blob=publicationFile&v=8. [Zugriff am 12.09.2024].

[9] Deutsche Krankenhausgesellschaft, „Branchenspezifischer Sicherheitsstandard "Medizinische Versorgung", V1.2“. 2022. [Online]. Verfügbar unter: https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/. [Zugriff am 28.08.2024].

[10] Westdeutscher Rundfunk, „Hackerangriff auf Krankenhäuser im Kreis Soest“. 2024. [Online]. Verfügbar unter: https://www1.wdr.de/nachrichten/westfalen-lippe/hacker-angriff-hospital-lippstadt-100.html. [Zugriff am 12.09.2024].

[11] J. Schieb, „Cyberangriff in Soest: Wieso Hacker immer öfter Kliniken attackieren“. 2024. [Online]. Verfügbar unter: https://www1.wdr.de/nachrichten/cyberangriffe-auf-krankenhaeuser-100.html. [Zugriff am 12.09.2024].

[12] Bundesamt für Sicherheit in der Informationstechnik, „Evaluierung der IT-Sicherheitsrichtlinie in Arztpraxen“. 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/SiRiPrax/SiRiPrax_2024.html. [Zugriff am 12.09.2024].

[13] Bundesamt für Sicherheit in der Informationstechnik, „Abschlussbericht Projekt CyberPraxMed - Sicherheit in Arztpraxen“. 2023. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/DigitaleGesellschaft/CyberPraxMed_Abschlussbericht.html. [Zugriff am 12.09.2024].

[14] S. Klipper, Information Security Risk Management - Risikomanagement mit ISO/IEC 27001, 27005 und 31010, Wiesbaden: Vieweg+Teubner GmbH, 2011.

[15] H.-P. Königs, IT-Risikomanagement mit System - Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken, Wiesbaden: Springer Vieweg, 2017.

[16] M. Durst et al., „Was ist ein PDCA_Zyklus? Plan-Do-Check-Act einfach erklärt“. 2021. [Online]. Verfügbar unter: https://der-prozessmanager.de/aktuell/wissensdatenbank/pdca-zyklus. [Zugriff am 31.07.2024].

[17] K.-R. Müller, IT-Sicherheit mit System, Wiesbaden: Springer Vieweg, 2018.

[18] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-2 - IT-Grundschutz-Methodik, V1.0“. 2017. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_2.pdf?__blob=publicationFile&v=2. [Zugriff am 13.09.2024].

[19] DIN EN ISO/IEC 27000:2020-06, Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Überblick und Terminologie (ISO/IEC 27000:2018).

[20] DIN EN ISO/IEC 27005:2024-05 - Entwurf, Informationssicherheit, Cybersicherheit und Datenschutz - Leitfaden zur Handhabung von Informationssicherheitsrisiken (ISO/IEC 27005:2022).

[21] Bundesministerium der Justiz, „§ 267a HGB - Einzelnorm“. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/hgb/__267a.html. [Zugriff am 06.06.2024].

[22] Bundesministerium der Justiz, „§ 267 HGB - Einzelnorm“. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/hgb/__267.html. [Zugriff am 26.04.2024].

[23] Amtsblatt der Europäischen Union, „Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (2003/361/EG)“. 2003. [Online]. Verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361&from=EN. [Zugriff am 06.06.2024].

[24] Prof. Dr. O. Schneck, „Rechtsgrundlagen des Risikomanagements / 1.1 Gesetz zur Kontrolle und Transparenz von Unternehmen (KonTraG)“. [Online]. Verfügbar unter: https://www.haufe.de/finance/haufe-finance-office-premium/rechtsgrundlagen-des-risikomanagements-11-gesetz-zur-kontrolle-und-transparenz-von-unternehmen-kontrag_idesk_PI20354_HI2711385.html. [Zugriff am 03.08.2024].

[25] Bundesministerium der Justiz, „§ 91 AktG - Einzelnorm“. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/aktg/__91.html. [Zugriff am 03.08.2024].

[26] Bundesministerium der Justiz, „§ 289 HGB - Einzelnorm“. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/hgb/__289.html. [Zugriff am 03.08.2024].

[27] TÜV Nord, „Risikomanagement im Unternehmen: Tipps | TÜV NORD“. 2022. [Online]. Verfügbar unter: https://www.tuev-nord.de/de/unternehmen/bildung/wissen-kompakt/unternehmensfuehrung/risikomanagement-in-unternehmen/. [Zugriff am 03.08.2024].

[28] Bundesamt für Sicherheit in der Informationstechnik, „BSI - BSI-Gesetz“. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/BSI-Gesetz/bsi-gesetz_node.html. [Zugriff am 01.08.2024].

[29] Bundesministerium der Justiz, „§ 2 BSIG - Einzelnorm“. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/bsig_2009/__2.html. [Zugriff am 01.08.2024].

[30] Bundesministerium der Justiz, „§ 8a BSIG - Einzelnorm“. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/bsig_2009/__8a.html. [Zugriff am 28.05.2024].

[31] Bundesministerium der Justiz, „BSI-KritisV - Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz“. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/bsi-kritisv/BJNR095800016.html. [Zugriff am 01.08.2024].

[32] M. Rohrlich, „NIS2: Alles, was Sie wissen müssen | Lexware“. 2024. [Online]. Verfügbar unter: https://www.lexware.de/wissen/unternehmensfuehrung/nis2-richtlinie/. [Zugriff am 02.08.2024].

[33] Europäisches Parlament und Rat, „Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)“. 2022. [Online]. Verfügbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:02022L2555-20221227. [Zugriff am 02.08.2024].

[34] TÜV Nord, „IT-Sicherheitsgesetz, KRITIS-Verordnung und Normen | TÜV NORD“. 2024. [Online]. Verfügbar unter: https://www.tuev-nord.de/de/unternehmen/bildung/wissen-kompakt/informationssicherheit/gesetze-und-normen-zur-it-sicherheit/. [Zugriff am 02.08.2024].

[35] Europäisches Parlament und Rat, „Datenschutz-Grundverordnung (DSGVO)“. 2022. [Online]. Verfügbar unter: https://eur-lex.europa.eu/DE/legal-content/summary/general-data-protection-regulation-gdpr.html. [Zugriff am 02.08.2024].

[36] intersoft consulting, „Art. 32 DSGVO - Sicherheit der Verarbeitung“. [Online]. Verfügbar unter: https://dsgvo-gesetz.de/art-32-dsgvo/. [Zugriff am 02.08.2024].

[37] intersoft consulting, „Art. 35 DSGVO - Datenschutz-Folgenabschätzung“. [Online]. Verfügbar unter: https://dsgvo-gesetz.de/art-35-dsgvo/. [Zugriff am 02.08.2024].

[38] intersoft consulting, „Erwägungsgrund 35 DSGVO - Gesundheitsdaten“. [Online]. Verfügbar unter: https://dsgvo-gesetz.de/erwaegungsgruende/nr-35/. [Zugriff am 15.09.2024].

[39] intersoft consulting, „Art. 9 DSGVO - Verarbeitung besonderer Kategorien personenbezogener Daten“. [Online]. Verfügbar unter: https://dsgvo-gesetz.de/art-9-dsgvo/. [Zugriff am 15.09.2024].

[40] intersoft consulting, „§ 22 BDSG - Verarbeitung besonderer Kategorien personenbezogener Daten“. [Online]. Verfügbar unter: https://dsgvo-gesetz.de/bdsg/22-bdsg/. [Zugriff am 15.09.2024].

[41] Bundesministerium der Justiz, „§ 391 SGB 5 - Einzelnorm“. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/sgb_5/__391.html. [Zugriff am 01.08.2024].

[42] Bundesministerium für Justiz, „§ 390 SGB 5 - Einzelnorm“. [Online]. Verfügbar unter: https://www.gesetze-im-internet.de/sgb_5/__390.html. [Zugriff am 01.08.2024].

[43] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-1 Managementsysteme für Informationssicherheit (ISMS), V1.0“. 2017. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_1.pdf?__blob=publicationFile&v=2. [Zugriff am 13.09.2024].

[44] Bundesamt für Sicherheit in der Informationstechnik, „Unser Leitbild“. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Das-BSI/Leitbild/leitbild_node.html. [Zugriff am 06.05.2024].

[45] Bundesamt für Sicherheit in der Informationstechnik, „Auftrag“. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/auftrag_node.html. [Zugriff am 06.05.2024].

[46] Bundesamt für Sicherheit in der Informationstechnik, „Kurzprofil des BSI“. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Das-BSI/Auftrag/BSI-Kurzprofil/kurzprofil_node.html. [Zugriff am 06.05.2024].

[47] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz“. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html. [Zugriff am 03.05.2024].

[48] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Kompendium - Werkzeug für Informationssicherheit“. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html. [Zugriff am 21.05.2024].

[49] Bundesamt für Sicherheit in der Informationstechnik, „BSI - Lerneinheit 2.9: Wahl der Vorgehensweise“. [Online]. Verfügbar unter: https://www.bsi.bund.de/dok/10990410. [Zugriff am 24.05.2024].

[50] Bundesamt für Sicherheit in der Informationstechnik, „Lerneinheit 7.7: Risiken bewerten“. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_7_Risikoanalyse/Lektion_7_07/Lektion_7_07_node.html. [Zugriff am 24.05.2024].

[51] Bundesamt für Sicherheit in der Informationstechnik, „Business Continuity Management - BSI-Standard 200-4, V1.0“. 2023. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8. [Zugriff am 13.09.2024].

[52] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Profile - Strukturbeschreibung - Version 1.0“. 2018. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Profile/Strukturbeschreibung.pdf?__blob=publicationFile&v=1. [Zugriff am 13.09.2024].

[53] Bundesamt für Sicherheit in der Informationstechnik, „IT-Grundschutz-Profile“. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Profile/Profile/itgrundschutzProfile_Profile_node.html. [Zugriff am 22.05.2024].

[54] Bundesamt für Sicherheit in der Informationstechnik, „BSI - Allgemeine Informationen zu KRITIS“. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/Allgemeine-Infos-zu-KRITIS/allgemeine-infos-zu-kritis_node.html. [Zugriff am 20.07.2024].

[55] Bundesamt für Sicherheit in der Informationstechnik, „Orientierungshilfe zu Inhalten und Anforderungen an branchenspezifische Sicherheitsstandards (B3S) gemäß § 8a Absatz 2 BSIG“. 2024. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-b3s.pdf?__blob=publicationFile&v=12. [Zugriff am 07.06.2024].

[56] C. Alberts et al., „Volume 3: Method Guidelines in OCTAVE(R)-S Implementation Guide, Version 1.0“. 2005. [Online]. Verfügbar unter: https://insights.sei.cmu.edu/documents/1608/2005_002_001_14273.pdf. [Zugriff am 13.09.2024].

[57] C. Alberts et al., „Introduction to the OCTAVE(R) Approach“. 2003. [Online]. Verfügbar unter: https://insights.sei.cmu.edu/documents/16/2003_012_001_51556.pdf. [Zugriff am 13.09.2024].

[58] C. Alberts und A. Dorofee, „OCTAVE(SM) CRITERIA, Version 2.0“. 2001. [Online]. Verfügbar unter: https://insights.sei.cmu.edu/documents/655/2001_005_001_13871.pdf. [Zugriff am 13.09.2024].

[59] E. Lachapelle und F. Rama, „Risk Assessment with OCTAVE“. 2015. [Online]. Verfügbar unter: https://pecb.com/whitepaper/risk-assessment-with-octave. [Zugriff am 17.06.2024].

[60] B. A. Tucker, „Advancing Risk Management Capability Using the OCTAVE FORTE Process“. 2020. [Online]. Verfügbar unter: https://insights.sei.cmu.edu/documents/2312/2020_004_001_644641.pdf. [Zugriff am 26.09.2024].

[61] C. Alberts et al., „Volume 1: Introduction to OCTAVE-S in OCTAVE(R)-S Implementation Guide, Version 1.0“. 2005. [Online]. Verfügbar unter: https://insights.sei.cmu.edu/documents/1608/2005_002_001_14273.pdf. [Zugriff am 13.09.2024].

[62] C. Alberts et al., „OCTAVE-S Implementation Guide, Version 1.0“. 2005. [Online]. Verfügbar unter: https://insights.sei.cmu.edu/documents/1608/2005_002_001_14273.pdf. [Zugriff am 13.09.2024].

[63] C. Alberts et al., „Volume 2: Preparation Guidelines in OCTAVE(R)-S Implementation Guide, Version 1.0“. 2005. [Online]. Verfügbar unter: https://insights.sei.cmu.edu/documents/1608/2005_002_001_14273.pdf. [Zugriff am 13.09.2024].

[64] C. Alberts et al., „Volume 6: Ciritical Asset Workbook for Systems in OCTAVE(R)-S Implementation Guide, Version 1.0“. 2005. [Online]. Verfügbar unter: https://insights.sei.cmu.edu/documents/1608/2005_002_001_14273.pdf. [Zugriff am 13.09.2024].

[65] DIN EN 45020:2007-03, Normung und damit zusammenhängende Tätigkeiten - Allgemeine Begriffe (ISO/IEC Guide 2:2004).

[66] DIN EN ISO/IEC 27001:2024-01, Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementssysteme - Anforderungen (ISO/IEC 27001:2022).

[67] DIN EN ISO/IEC 27002:2024-01, Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre - Informationssicherheitsmaßnahmen (ISO/IEC 27002:2022).

[68] N. Kirtley, „Threat Modeling“. 2023. [Online]. Verfügbar unter: https://threat-modeling.com/threat-modeling/. [Zugriff am 17.09.2024].

[69] The OWASP Foundation, „OWASP Threat Modeling Project“. [Online]. Verfügbar unter: https://owasp.org/www-project-threat-model/. [Zugriff am 17.09.2024].

[70] M. Cobb, „Risk assessment vs. threat modeling: What's the difference?“. 2023. [Online]. Verfügbar unter: https://www.techtarget.com/searchsecurity/tip/Risk-assessment-vs-threat-modeling-Whats-the-difference. [Zugriff am 26.09.2024].

[71] M. Howard und Lipner Steve, The Security Development Lifecycle, Redmond, Washington: Microsoft Press, 2006.

[72] N. Shevchenko, „Threat Modeling: 12 Available Methods“. 2018. [Online]. Verfügbar unter: https://insights.sei.cmu.edu/blog/threat-modeling-12-available-methods/. [Zugriff am 17.09.2024].

[73] N. Kirtley, „DREAD Threat Modeling“. 2023. [Online]. Verfügbar unter: https://threat-modeling.com/dread-threat-modeling/. [Zugriff am 17.09.2024].

[74] M. Le Corre, „Bachelorbareit - Analyse von IT-Notfallmanagement-Standards und -Normen im Kontext von KMU“. 2020. [Online]. Verfügbar unter: https://monami.hs-mittweida.de/frontdoor/index/index/year/2022/docId/13303. [Zugriff am 13.09.2024].

[75] R. Flesch, „How to write Plain Englisch“. [Online]. Verfügbar unter: https://web.archive.org/web/20160712094308/http://www.mang.canterbury.ac.nz/writing_guide/writing/flesch.shtml. [Zugriff am 14.08.2024].

[76] F. Merges, Assistenzsystem zur Testung und Verbesserung der Lesbarkeit von Gebrauchsinformationen, Siegen: Universität Siegen, 2014.

[77] Ahrefs, „Silbenzähler - Zeichen zählen & Sprechzeit“. [Online]. Verfügbar unter: https://wordcount.com/de/syllable-counter. [Zugriff am 25.09.2024].

[78] Bundesamt für Sicherheit in der Informationstechnik, „BSI-Standard 200-3: Risikomanagement“. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-3-Risikomanagement/bsi-standard-200-3-risikomanagement_node.html. [Zugriff am 13.08.2024].

[79] Deutsche Krankenhausgesellschaft, „Informationssicherheit im Krankenhauser - Branchenspezifischer Sicherheitsstandard (B3S)“. [Online]. Verfügbar unter: https://www.dkgev.de/themen/digitalisierung-daten/informationssicherheit-und-technischer-datenschutz/informationssicherheit-im-krankenhaus/. [Zugriff am 13.08.2024].

[80] DIN Media, „DIN EN ISO/IEC 27005 - 2024-05 - DIN Media“. 2024, [Online]. Verfügbar unter: https://www.dinmedia.de/de/norm-entwurf/din-en-iso-iec-27005/379085196. [Zugriff am 13.08.2024].

[81] Microsoft Corporation, „Microsoft Threat Modeling Tool“. 2023. [Online]. Verfügbar unter: https://learn.microsoft.com/de-de/azure/security/develop/threat-modeling-tool. [Zugriff am 17.09.2024].

[82] Bundesamt für Sicherheit in der Informationstechnik, „Beschreibung des Beispielunternehmens RECPLAST GmbH“. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Recplast/Beschreibung_Recplast.pdf?__blob=publicationFile&v=1. [Zugriff am 01.09.2024].

[83] Compliance Essentials GmbH, „DSGVO Bußgeld Datenbank - immer aktuell und vollständig | dsgvo-portal.de“. [Online]. Verfügbar unter: https://www.dsgvo-portal.de/dsgvo-bussgeld-datenbank/. [Zugriff am 01.09.2024].

[84] dios, „Wichtige Informationen für easyTI Kunden - dios.de“. 2021. [Online]. Verfügbar unter: https://www.dios.de/aktuelles/wichtige-information-fuer-easyti-kunden/. [Zugriff am 28.08.2024].

[85] eHealth Experts GmbH, „easyTI - Dokumentation“. 2021. [Online]. Verfügbar unter: https://hasomed.de/wp-content/uploads/2021/08/easyti_Benutzerhandbuch.pdf. [Zugriff am 31.08.2024].

[86] Kassenzahnärztliche Bundesvereinigung und Bundeszahnärztekammer, „Datenschutz & IT-Sicherheit in der Zahnarztpraxis - Leitfaden + Empfehlungen zur Umsetzung der IT-Sicherheitsrichtlinie“. 2021. [Online]. Verfügbar unter: https://www.kzbv.de/datenschutz-und-it-sicherheit-in-der.91.de.html. [Zugriff am 02.09.2024].

[87] gematik, „Informationsblatt - Anschluss einer medizinischen Einrichtung“. 2017. [Online]. Verfügbar unter: https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Erste_Schritte/gem_OPB_Infoblatt_Anschluss_2017-10-BR-DGDV1_web.pdf. [Zugriff am 01.09.2024].

[88] Kassenzahnärztliche Bundesvereinigung, „Telematikinfrastruktur - Ein Überblick“. 2024. [Online]. Verfügbar unter: https://www.kzbv.de/ti-das-gesundheitsnetz.1163.de.html. [Zugriff am 01.09.2024].

[89] gematik, „Anschluss medizinischer Einrichtungen an die Telematikinfrastruktur - Ein Überblick für Dienstleister vor Ort (DVO)“. 2019. [Online]. Verfügbar unter:

https://fachportal.gematik.de/fileadmin/user_upload/fachportal/files/Service/Anschluss_medizinischer_Einrichtungen_an_die_Telematikinfrastruktur__DVO_/gemInfo_Anschluss_TI_DVO_V2.2.1_Anh.pdf. [Zugriff am 01.09.2024].

[90] Bundesamt für Sicherheit in der Informationstechnik, „Ransomware - Vorsicht vor Erpressersoftware“. [Online]. Verfügbar unter: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Schadprogramme/Ransomware/ransomware_node.html. [Zugriff am 10.09.2024].

[91] M. Zoltan, „Wie verbreitet sich Ransomware in einem Netzwerk?“. 2024. [Online]. Verfügbar unter: https://www.privacyaffairs.com/de/how-ransomware-spread-network/. [Zugriff am 09.10.2024].

[92] Bitkom e.V., „Mehr als die Hälfte der Unternehmen werden Opfer von Ransomware-Attacken“. 2024. [Online]. Verfügbar unter: https://www.bitkom.org/Presse/Presseinformation/Mehr-als-Haelfte-Unternehmen-Opfer-Ransomware. [Zugriff am 10.09.2024].

[93] Sophos, „Ransomware-Report“. 2024. [Online]. Verfügbar unter: https://www.sophos.com/de-de/content/state-of-ransomware. [Zugriff am 10.09.2024].

[94] K. M. Decker, „Informationssicherheit - ohne methodische Risikoidentifizierung ist alles Nichts“. 2017. [Online]. Verfügbar unter: https://mit-solutions.com/downloads/Artikel_Risikoidentifizierung.pdf. [Zugriff am 12.09.2024].

[95] Kassenzahnärztliche Bundesvereinigung, „Pressemitteilung vom 17.6.2024“. 2024. [Online]. Verfügbar unter: https://www.kzbv.de/pressemitteilung-vom-17-6-2024.1868.de.html. [Zugriff am 19.09.2024].

[96] NIST Computer Security Resource Center, „NIST Risk Management Framework“. 2024. [Online]. Verfügbar unter: https://csrc.nist.gov/Projects/risk-management. [Zugriff am 01.10.2024].

[97] VdS Schadensverhütung GmbH, „VdS 10000 - Das ISMS für kleine und mittlere Unternehmen (KMU)“. [Online]. Verfügbar unter: https://vds.de/kompetenzen/cyber-security/zertifizierungen/informationssicherheits-und-datenschutzmanagement/vds-10000-informationssicherheit-fuer-kmu. [Zugriff am 01.10.2024].

Anhang

Anhang A, IT-Grundschutz: Leitlinie zur Informationssicherheit (elektronisch beigelegt, Datei: BSI_1_Sicherheitsleitlinie.pdf)

Anhang B, IT-Grundschutz: Strukturanalyse (elektronisch beigelegt, Datei: BSI_2_Strukturanalyse.xlsx)

Anhang C, IT-Grundschutz: Abhängigkeiten (elektronisch beigelegt, Datei: BSI_3_AbhängigkeitenStrukturanalyse.xlsx)

Anhang D, IT-Grundschutz: Schutzbedarfsfeststellung (elektronisch beigelegt, Datei: BSI_4_Schutzbedarfsfeststellung.xlsx)

Anhang E, OCTAVE-S: Volume 4: Organizational Worksheet (elektronisch beigelegt, Datei: OCTAVE_1_Volume4.pdf)

Anhang F, OCTAVE-S: Volume 6: Critical Asset Worksheets for Systems (Server) (elektronisch beigelegt, Datei: OCTAVE_2_Volume6.pdf)

Anhang G, OCTAVE-S: Volume 7: Critical Asset Worksheets for Applications (DiosZX) (elektronisch beigelegt, Datei: OCTAVE_3_Volume7.pdf)

Anhang H, OCTAVE-S: Volume 9: Strategy an Plan Worksheets (elektronisch beigelegt, Datei: OCTAVE_4_Volume9.pdf)

Eidesstattliche Erklärung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Quellen und Hilfsmittel angefertigt habe. Sämtliche Stellen der Arbeit, die im Wortlaut oder dem Sinn nach Publikationen oder Vorträgen anderer Autoren entnommen sind, habe ich als solche kenntlich gemacht. Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt oder anderweitig veröffentlicht.

Ort, Datum	Vollständiger Name	Unterschrift

Nutzungs- und Verwertungsrechte

Ich übertrage zusätzliche Nutzungs- und Verwertungsrechte für die vorliegende Arbeit und allen damit in Zusammenhang stehenden Daten auf Grundlage *der Creative Commons Lizenz* "*CC0*" an alle genannten Betreuer dieser Arbeit.

Ort, Datum	Unterschrift