Alfried Krupp Krankenhaus

HOCHSCHULE RUHR WEST
UNIVERSITY OF APPLIED SCIENCES

Bachelorarbeit

Implementierung und Risikobewertung der Integration von Sonografie-Geräten in die Krankenhauslandschaft im Rahmen einer Industriepartnerschaft

Bachelorarbeit zur Erlangung des akademischen Grades
Bachelor of Science

vorgelegt von:

Selime Yilmaz

Matrikelnummer: 10009374

Studiengang: Gesundheits- und Medizintechnologien

Partnerunternehmen:
Alfried Krupp Krankenhaus
Alfried-Krupp-Straße 21
45131 Essen

Betreuer im Partnerunternehmen:
Dr. rer. medic. Mark Oehmigen
Betreuer an der HRW:
Prof. Dr.-Ing. Carole Leguy

Essen, den 20. November 2023

Eidesstattliche Erklärung

Hiermit erkläre ich, dass die vorliegende Bachelorarbeit selbstständig angefertigt wurde. Es wurden nur die in der Arbeit ausdrücklich benannten Quellen und Hilfsmittel benutzt. Wörtlich oder sinngemäß übernommenes Gedankengut habe ich als solches kenntlich gemacht. Die vorgelegte Arbeit hat weder in der gegenwärtigen noch in einer anderen Fassung schon einem anderen Fachbereich der Hochschule Ruhr West oder einer anderen wissenschaftlichen Hochschule vorgelegen.

Essen, den 20. November 2023

Selime Yilmaz

Danksagung

Die vorliegende Arbeit wurde unter der Aufsicht von Dr. rer. medic. Mark Oehmigen im Alfried Krupp Krankenhaus in Essen Rüttenscheid erstellt.

Ich möchte mich ganz besonders beim Alfried Krupp Krankenhaus bedanken, insbesondere meinem Betreuer Dr. Mark Oehmigen. Seine fachliche Kompetenz und seine wertvollen Ratschläge haben maßgeblich zum Gelingen meiner Arbeit beigetragen. Ein weiterer Dank gebührt meinen Professoren Frau Prof. Dr. Leguy und Herrn Knecht. Ihre wertvollen Ratschläge und ihr konstruktives Feedback haben mir geholfen, meine Arbeit stetig zu verbessern und neue Erkenntnisse zu gewinnen.

Ein herzliches Dankeschön geht auch an meine Familie und Freunde, die mich stets ermutigt und motiviert haben. Abschließend möchte ich betonen, dass diese Bachelorarbeit nicht nur mein persönlicher Erfolg ist, sondern das Ergebnis einer gemeinsamen Anstrengung vieler Menschen. Ich bin dankbar für die wertvolle Unterstützung, die ich von Ihnen allen erhalten habe.

Inhaltsverzeichnis

1. Abkürzungsverzeichnis

Abkürzung	Bedeutung
DICOM	Digital Imaging and Communications in Medicine
IT	Informationstechnik
WLAN	Wireless local Network
BfArM	Bundesinstitut für Arzneimittel und Medizinprodukte
EDV	Elektronische Datenverarbeitung
CT	Computer-Tomographie
MRT	Magnetresonanztomographie
MHz	Mega Hertz
PACS	Picture Archiving and Communication Systems
HL7	Health Level 7
LAN	Local Network
GSM	Global System for Mobile Communications
UMTS	Universal Mobile Telecommunication System
LTE	Long Term Evolution
WAN	Wide Area Network
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
DoD	Department-of-Defense
WPA2	Wi-Fi Protected Access 2
WPS	Wi-Fi Protected Setup
DoS	Danial of Service

IP	Internet Protocol
TCP	Transmission Control Protocol
ARP	Address Resolution Protocol
MAC	Media Access Control
IDS	Intrusion Detection System
QMS	Qualitätsring Medizinische Software
GDT	Geräte-Daten-Träger
USV	Unterbrechungsfreie Stromversorgung
WAP	Wireless Access Point
AP	Access Point
IKT	Informations- und Kommunikationstechnologie
AKK	Alfried Krupp Krankenhaus
IMC	Intermediate Care
MB	Megabyte
GB	Gigabyte
DHCP	Dynamic Host Configuration Protocol
VLAN	Virtual local area network
KIS	Krankenhausinformationssystem
EPA	Elektronische Patientenakte
EAP-TLS-Protokoll	Extensible Authentication Protocol
SS-Point	Service Access Point
RA	Registrierungsstelle
CA	Zertifizierungsstelle
BSI	Bundesamtes für Sicherheit in der Informationstechnik
MPBetreibV	Medizinprodukte-Betreiberverordnung
IPsec	Internet Protocol secure

TLS	Transport Layer Security
SSL	Secure Sockets Layer
WEP	Wired Equivalent Privacy
PSK	Pre-Shared Key
VPN	Virtual Private Network
PRNG	pseudo random number generator
DGUV	Deutsche Gesetzliche Unfallversicherung

1 Einleitung

Die Digitalisierung der Medizintechnik wurde in den 1990er Jahren durch die Entwicklung des DICOM-Standards vorangetrieben, der als Reaktion auf die Fortschritte in der Computer- und Softwaretechnologie im Bereich der Radiologie entstand. Die Integration von aktiven Medizingeräten und Netzwerkkomponenten in medizinische Netzwerke hat zur Folge, dass IT-Netzwerke in Krankenhäusern und anderen Gesundheitseinrichtungen eine stetig wachsende Rolle in der medizinischen Diagnostik und Behandlung einnehmen. Insbesondere im Bereich der bildgebenden Systeme in der Ultraschall- und Radiologie-Technik sind Betriebssysteme, Software und Vernetzung heute nicht unumgänglich. (Armin, 2012)

Der Hardware-Anteil moderner Medizintechnik wird immer geringer. Gleichzeitig steigt die Bedeutung von IT-Anwendungen wie Software und Netzwerkanbindungen wie Hardware und Infrastruktur. Funktionalitäten und Prozesse der Diagnostik und Therapie wandern vermehrt vom autonomen Medizinprodukt in das IT-Netzwerk des Krankenhauses. Dabei übertragen zunehmend mehr aktive Medizingeräte ihre Daten über das IT-Netzwerk eines Krankenhauses, tauschen sie aus und archivieren sie auf Servern. (Armin, 2012)

Um die Vernetzung und Risikominderung der IT-Infrastruktur in einer Gesundheitseinrichtung zu verbessern, sind spezifische Normen und Richtlinien erforderlich. Eine hierfür entwickelte Norm ist die DIN EN 80001-1:2011. Die internationale IEC-Norm DIN EN 80001-1:2011 stellt ein Normenwerk zur Verfügung, das einen Risikomanagementprozess gemäß dem aktuellen Stand der Technik definiert. Dieses Normenwerk ermöglicht die effektive Kontrolle fundamentaler Risiken, die durch den Einsatz eines medizinischen IT-Netzwerks entstehen können. (DKG, 2011)

1.1 Aufgabenstellung und Zielsetzung

Die Integration von Sonografie-Geräten in die Krankenhauslandschaft eröffnet neue Perspektiven für die medizinische Bildgebung und Diagnostik. Im Rahmen einer Industriepartnerschaft zwischen dem Alfried Krupp Krankenhaus und GE HealthCare wird angestrebt, diese Technologie erfolgreich in die bestehende Infrastruktur zu implementieren. Die Identifizierung und Bewertung potenzieller Risiken sind dabei von entscheidender Bedeutung, um einen sicheren und effizienten Einsatz der Geräte zu gewährleisten. Die Arbeit befasst sich mit der Durchführung einer Risikoanalyse im Rahmen der Integration von Ultraschallgeräten im AKK unter Berücksichtigung der DIN EN 80001-1:2011 „Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten“, welche

Anforderungen an das Risikomanagement beim Einsatz von IT-Netzwerken in medizinischen Einrichtungen definiert. Zusätzlich werden ergänzende Methoden aus dem BSI IT-Grundschutz und der ISO/IEC 27005 herangezogen.

Ziel dieser Arbeit besteht darin, potenzielle Risiken zwischen den einzelnen Schnittstellen zu identifizieren und zu bewerten, um geeignete Maßnahmen zur Risikominderung abzuleiten. Die Geräte werden über eine Silex-Box (Bridge) mit dem IT-Netzwerk verbunden und dienen als WLAN-Schnittstelle, um die Mobilität der Geräte im gesamten Krankenhaus zu ermöglichen.

1.2 Aufbau der Arbeit

Die vorliegende Arbeit ist in sechs Abschnitte strukturiert. Nach einer Einleitung, die die Thematik und Zielsetzung erläutert, folgt im zweiten Kapitel eine umfassende Darstellung des Hintergrunds. Dabei werden Informationen über die beteiligten Partner, das Sonografie-Gerät und die Grundlagen der Bildverarbeitung präsentiert. Der abschließende Teil dieses Kapitels befasst sich mit dem Thema Netzwerke. Die Differenzierung der verschiedenen Netzwerkarten ist von entscheidender Wichtigkeit, um ein Verständnis für den Aufbau von Netzwerken und den Datenaustausch zu entwickeln sowie die Unterschiede zwischen medizinischen IT-Netzwerken und konventionellen IT-Netzwerken zu erkennen.

Das dritte Kapitel ist eine Übersicht der Norm DIN EN 80001-1 mit einer Erläuterung der einzelnen Schutzziele der Norm und der Informationssicherheit. Zudem werden die Verantwortlichkeiten der beteiligten Parteien gemäß den Vorgaben der DIN EN 80001-1 beschrieben. Des Weiteren wird im vierten Kapitel das Risikomanagementsystem detailliert beschrieben und die einzelnen Prozessschritte, die zur Erfüllung der Norm eingeführt werden müssen, aufgeführt. Die Arbeit schließt in Kapitel fünf mit einer Zusammenfassung der Ergebnisse und einem Ausblick, welche Maßnahmen das Alfried Krupp Krankenhaus ergreifen könnte.

2 Hintergrund

2.1 Alfried Krupp Krankenhaus

Das Alfried Krupp Krankenhaus ist ein Stiftungskrankenhaus, welches der Alfried-Krupp von Bohlen und Halbach-Stiftung gehört. Die Gründung des Alfried Krupp Krankenhauses geht auf ein Militärhospital zurück, welches vor 150 Jahren gegründet wurde, um verletzte Soldaten im Krieg von 1870-1871 zu verarzten. Die Nutzung des Krankenhauses war in der Zeit von 1872 bis 1920 auf die Mitarbeiter und deren Familien beschränkt. Seit 1920 steht das Krankenhaus nicht nur den Mitarbeitern, sondern der gesamten Essener Bevölkerung zur Verfügung. Im Jahr 1980 erfolgte die Neugründung des Krankenhauses im Essener Stadtteil Rüttenscheid und 2007 die Übernahme des Lutherhauses in Steele. Des Weiteren wurde ein Ärztehaus gegenüber dem Rüttenscheider Krankenhaus erbaut. Neben den internistischen, chirurgischen und HNO-Abteilungen wurde eine geburtshilflich-gynäkologische Abteilung und eine ophthalmologische Abteilung errichtet. (Brusis, 2011)

An beiden Standorten sind insgesamt 21 medizinische Kliniken angesiedelt. Über 575 Betten mit 13 Kliniken stehen am Standort Rüttenscheid zur Verfügung. In Steele werden 320 Betten in 8 Kliniken vorgehalten. Darüber hinaus sind beide Häuser akademisches Lehrkrankenhaus der Universität Duisburg-Essen. (Alfried Krupp Krankenhaus, 2023)

2.1.1 Medizintechnik

Ein Rückblick auf die Vergangenheit verdeutlicht die wechselseitige Beziehung zwischen medizinischem Fortschritt und technologischem Erfolg. Faszination des Menschen für Medizin und Technik reicht bereits Tausende von Jahren zurück. Einer der ersten medizinischen Geräte war das Proktoskop, welches zur Darmuntersuchung genutzt wurde. Es werden auch Werkzeuge zur Heilung von gebrochenen Armen im antiken Rom und die visuelle Sehhilfe im 13. Jahrhundert erwähnt. (Kramme, Medizintechnik Verfahren - Systeme - Informationsverarbeitung, 2017)

Ein Wendepunkt in der neuzeitlichen Medizin war die Entdeckung der Röntgenstrahlen im Jahr 1895. Im Laufe des 20. Jahrhunderts wurden immer mehr technische Instrumente und Apparate entwickelt, um die medizinische Versorgung zu verbessern. Beispiele dafür sind das Elektrokardiogramm, das 1903 für die klinische Behandlung zugelassen wurde, und die nichtinvasive Messung des Blutdrucks am Oberarm. Weitere wichtige Entwicklungen waren die Erfindung der künstlichen Niere im Jahr 1942 und das erste Patientenüberwachungsgerät im Jahr 1965.

(Kramme, Medizintechnik Verfahren - Systeme - Informationsverarbeitung, 2017)

Die Medizintechnik hat die moderne Medizin und Technik maßgeblich geprägt und mitentwickelt. Ohne diese technologischen Methoden wäre es nicht möglich, eine Vielzahl von Behandlungen durchzuführen und Krankheitsbilder zu diagnostizieren. (Kramme, 2017)

Der Medizintechniker überprüft die Funktion und die ordnungsgemäße Verwendung medizinischer Geräte im Hinblick auf Messung und Sicherheit. Die Verwaltung und Dokumentation umfassen eine wichtige organisatorische Rolle, da tausende von medizinischen Geräten erfasst werden müssen. Zur Unterstützung dieser Aufgaben wird oft eine computergestützte Facility-Management-Software eingesetzt, die mit einem Ticketsystem kombiniert wird, um Ausfälle und Störungen zu protokollieren und kurzfristig Ersatz bereitzustellen. Des Weiteren sind Störungen von Medizinprodukten, die eine Gefährdung für Patienten darstellen können, dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) umgehend zu melden. (Kruber, 2015)

Im AKK wird die Software HSD NOVA-fm genutzt, die für die Bereiche der Medizintechnik, Instandhaltung und Facility-Management geeignet ist. Bei einem Problem wird das Gerät von einem Medizintechniker bewertet und je nach Möglichkeiten repariert oder ausgemustert. Die Reparatur wird entweder von der Medizintechnik oder von einem externen Dienstleister vorgenommen. Bei einer Ausmusterung wird eine Ersatzbeschaffung in die Wege geleitet. (AKK, 2023)

2.1.2 EDV

Seit etwa drei Jahrzehnten werden im Gesundheitswesen IT-Systeme eingeführt. Ursprünglich waren diese Systeme spezialisierte Bereichssysteme, die nur bestimmte Prozesse unterstützten. Sie waren isoliert und ermöglichten keinen Datenaustausch mit anderen Abteilungssystemen innerhalb des Krankenhauses. Diese Systeme waren durch mangelnde Vollständigkeit, Redundanz und Asynchronität charakterisiert. (P.Gocke & Debatin, 2011)

Die fortschreitende Digitalisierung eröffnet eine Vielzahl von Möglichkeiten zur Steigerung der Effizienz und Qualität der Patientenversorgung. Allerdings sind auch potenzielle Risiken zu berücksichtigen, die mit der zunehmenden Integration von Informationstechnologie in die Arbeitsabläufe und Geschäftsprozesse im Gesundheitswesen verbunden werden. Ohne die Anwendung komplexer IT-Systeme wäre die moderne Medizin nicht realisierbar, da diese eine grundlegende Voraussetzung für einen effizienten Klinikbetrieb darstellt. Dies hat zur Folge, dass die potenziellen Auswirkungen eines Versagens oder einer Einschränkung dieser Systeme

zunehmen. In der heutigen Zeit trägt die Informationstechnologie maßgeblich zur effizienten Durchführung zahlreicher Abläufe im klinischen Umfeld bei. Dabei ist der Einsatz von IT-Systemen nicht nur im medizinischen Bereich von großer Bedeutung. Von der Kontrolle der Gebäudetechnik über die Organisation von Wäschereidiensten bis hin zur Gewährleistung einer angemessenen Speiseversorgung der Patienten spielt die Informationstechnologie eine entscheidende Rolle bei der Steuerung, Unterstützung und Überwachung wichtiger Prozesse. (Deutsche Krankenhausgesellschaft e.V., kein Datum)

Die Implementierung von EDV-Systemen im Gesundheitswesen begann zunächst in den administrativen und medizinischen Bereichen von Krankenhäusern. (Hollberg, Pleuss, & Rittersbacher, 1973) In medizinischen Einrichtungen bieten sie Unterstützung für das Personal in den Bereichen Verwaltung, Medizin und Pflege an, um ihre Arbeitsabläufe effizient auszurichten. Dies beinhaltet die Durchführung kurzfristiger Planungen, die Erstellung umfassender Dokumentationen und die Abwicklung von Abrechnungen. (Miller, Katharina, 2023)

Das EDV-System trägt zur Optimierung des fortlaufenden Arbeitsprozesses bei. Es ist von großer Bedeutung, dass sowohl die technischen als auch die wirtschaftlichen Aspekte bei der Implementierung oder Erweiterung von EDV-Systemen berücksichtigt werden. Anhand von medizinischen und informationstechnischen Standards wird gezeigt, dass es heutzutage möglich ist, integrierte Systeme aufzubauen. (Dittel & Kopacek, 1995)

2.2 GE HealthCare

GE HealthCare ist ein weltweit tätiges Unternehmen aus den USA, dass sich auf die Bereiche Medizintechnik, pharmazeutische Diagnostik und digitale Technologien spezialisiert hat. Der Fokus des Unternehmens liegt darauf, Krankenhäuser effizienter zu machen, Ärzte in ihrer Arbeit zu unterstützen, Therapien präziser zu gestalten und die Gesundheit sowie Zufriedenheit der Patienten durch integrierte Lösungen, Dienstleistungen und Datenanalysen zu verbessern. Das Unternehmen hat seinen Firmensitz in Großbritannien und stellt seinen Kunden in über 100 Ländern weltweit mehr als 43.000 Mitarbeiterinnen und Mitarbeiter zur Verfügung. (Herrmann, Kleinbeck, & Ritterskamp, 2009)

GE HealthCare ist Hersteller einer breiten Vielfalt innovativer Technologien, darunter Ultraschall, Magnetresonanztomografie (MRT) und chirurgische Navigation. Diese fortschrittlichen Technologien bieten medizinischem Fachpersonal unter anderem die Möglichkeit, einen detaillierten Einblick in den menschlichen Organismus zu erhalten. Die Integration von medizinischen IT-Systemen optimiert die medizinische Versorgung, indem sie

eine reibungslose Kommunikation und Zusammenarbeit zwischen verschiedenen Akteuren im Gesundheitswesen ermöglicht. (Herrmann, Kleinbeck, & Ritterskamp, 2009)

2.3 Sonografie-Gerät

Die Verwendung von Ultraschallwellen, die zur Ortung von Gegenständen dienten, ist militärischer Abstammung. Erst 1942 wurde der Ultraschall erstmals in der Medizin eingesetzt, als der Nervenarzt Karl Dussik einen Seitenventrikel im Gehirn abbildete. In den Folgejahren wurde das Verfahren in diversen Disziplinen weiterentwickelt. Die zerstörungsfreien Werkstoffprüfungstechniken, die aus dem Bereich der Physik stammen und während des Zweiten Weltkriegs entwickelt wurden, fanden in der Medizin eine umfangreiche Anwendung durch enge Forschungszusammenarbeit zwischen Physikern und Medizinern. (Birnbaum & Albrecht, 2007)

1954 wurden die ersten zweidimensionalen Darstellungen entwickelt, bei denen der Patient in einem mit Wasser gefüllten Behälter platziert wurde und von einer synchron vertikal oszillierenden Ultraschallquelle umgeben war. Donald und Brown entwickelten 1957 den ersten Kontakt-Compound-Scanner in Glasgow, der es ermöglichte, den Patienten ohne die Notwendigkeit eines Wasserbads zu untersuchen. Seitdem wird die Sonde auf die Hautoberfläche positioniert und manuell bewegt. Die Einführung der ersten Echtzeitgeräte erfolgte 1965. Erst in den achtziger Jahren wurde die Ultraschalldiagnostik weit verbreitet und eingesetzt. (Birnbaum & Albrecht, 2007)

Die bildgebende Diagnostik mit Ultraschall gewann in den vergangenen Jahren zunehmend an Relevanz. Dies ist auf verschiedene Faktoren zurückzuführen: Die Methode ist anpassungsfähig, transportabel, kosteneffektiv und bei fachgerechter Durchführung nicht schädlich für den Patienten. (Dössel, 2016) Die daraus resultierende Konsequenz ist, dass die Ultraschalldiagnostik ohne ionisierende Strahlung auskommt und heutzutage nicht mehr wegzudenken ist. (Kramme, 2017) Zudem wurde die Aufnahmequalität kontinuierlich verbessert, sodass die erzeugten Aufnahmen heute eine wichtige therapeutische Indikation haben. Auch ermöglicht der Doppler-Ultraschall die Darstellung des zirkulierenden Blutes in den Gefäßen. (Dössel, 2016)

Die Sonografie ist in einigen Fällen dazu übergegangen, andere Methoden wie CT, MRT oder die konventionelle Röntgendiagnostik teilweise zu ersetzen oder zu komplettieren. Im Vergleich zu diesen Techniken ermöglicht der Ultraschall eine Echtzeitdarstellung der durchstrahlten Organe auf einem Bildschirm im Schnittbildverfahren, ähnlich einer tomografischen Schnittbilddarstellung. (Kramme, 2017)

2.3.1 Funktionsweise

Die Bildentstehung in der Sonographie ist ein komplizierter Vorgang, der durch das Prinzip der Streuung erschwert wird. Streuung bezieht sich auf die Tatsache, dass Schallwellen in verschiedenen Geweben unterschiedliche Geschwindigkeiten haben. Dies führt dazu, dass die Schallwellen auf ihrem Weg durch den Körper gestreut und abgelenkt werden. Es sei darauf hingewiesen, dass dies nur eine grobe Erklärung für das Prinzip der Streuung ist. (Kramme, 2017)

Ultraschallgeräte in der Medizin nutzen Longitudinalwellen im Frequenzbereich von 1 bis 16 MHz und werden mittels des reversiblen Piezo-Effekts generiert. In diesem Verfahren dienen die Wandler sowohl als Sender als auch Empfänger. Sie senden Schallimpulse aus und empfangen die reflektierten Signale im Impuls-Echo-Verfahren. Im Vergleich zu niederfrequentem Ultraschall dringt hochfrequenter Ultraschall weniger tief in das Körpergewebe ein, liefert jedoch eine bessere Auflösung der Aufnahmen. Das Eindringen in das Körpergewebe und das höchste Auflösungsvermögen des Bildes sind daher unmittelbar von der Schallfrequenz abhängig. Die Qualität der Bilder kann signifikant durch die Auswahl des passenden Schallkopfs sowie die Anpassung bestimmter Parameter am Sonografie-Gerät wie Verstärkung, Eindringtiefe, Fokus und Presets bestimmt werden. (Birnbaum & Albrecht, 2007)

2.4 Standards für Schnittstellen

Eine standardisierte Schnittstelle wird durch eine festgelegte Zusammenstellung von Vorschriften definiert. Durch die Verwendung standardisierter Schnittstellen können Bauteile oder Module, die dieselbe Schnittstelle verwenden, interoperabel sein und Daten gemäß den definierten Standards ausführen. Im Gesundheitssektor werden verschiedene Normen angewandt. (Kramme, Medizintechnik, Verfahren - Systeme - Informationsverarbeitung, 2011)

2.4.1 HL7

Health Level 7 ist ein globaler Standard zum Datenaustausch im Gesundheitssystem. Der Einsatz von HL7-Kommunikationsservern ermöglicht eine Optimierung der Schnittstellen zwischen Subsystemen in Krankenhäusern. Diese Server reduzieren die Menge der notwendigen Schnittstellen, da nicht jedes System direkt an das Krankenhausinformationssystem angebunden werden muss. Das Resultat ist ein einheitlicher und vereinfachter Kommunikationsablauf sowie eine Kostenreduktion, da getrennte Schnittstellen Kosten verursachen. Der HL7-Server wandelt Datenformate selbstständig in das vom Empfängersystem benötigte Format um. Die Einrichtung und Pflege der Schnittstellen

wird zentral auf dem Kommunikationsserver vorgenommen. Die Vernetzung von Medizingeräten kann ebenfalls über HL7-Server stattfinden, was zu einer spezifischen Systemlandschaft führt. (Kramme, Medizintechnik, Verfahren - Systeme - Informationsverarbeitung, 2011)

2.4.2 DICOM

Digital Imaging and Communications in Medicine ist ein offizieller Standard, der den Datenaustausch von digitalen Bilddaten und zugehörigen Informationen ermöglicht. In Bezug darauf definiert der DICOM-Standard das Speicherungsformat und das Kommunikationsprotokoll für den Datenaustausch. Eine wachsende Anzahl von Systemherstellern in der medizinischen Bildgebung implementiert den DICOM-Standard in ihren Geräten, beispielsweise in der digitalen Radiographie, Magnetresonanztomographie, Computertomographie, Endoskopie oder Sonographie. Dadurch entsteht eine hohe Austauschbarkeit zwischen den Bildgebungssystemen und den Bildbearbeitungs- und digitalen Bildarchivierungssystemen. (Kramme, Medizintechnik, Verfahren - Systeme - Informationsverarbeitung, 2011)

2.4.3 PACS

Das Picture Archiving and Communication System ist ein umfassendes bildgebendes System, das darauf abzielt, den Workflow innerhalb des Behandlungsprozesses zu optimieren. Ein wichtiger Bestandteil dieses Systems ist die Bilddistribution, die als autonomes System digitale Bilder und damit verbundene Informationen an die Leistungserbringer im Gesundheitswesen bereitstellt und so die zeitgerechte Versorgung der Patienten sicherstellt. Ursprünglich für die Radiologie entwickelt, wird PACS inzwischen auch in anderen klinischen Bereichen wie Kardiologie und Pathologie eingesetzt. Die Nutzung des Systems kann die Diagnose beschleunigen und die Effektivität des Behandlungsprozesses erhöhen. (Huang, 2003)

2.5 Netzwerke

In einem Netzwerk sind alle technischen Kommunikationskomponenten zusammengefasst, die der Übermittlung und Weiterleitung von Informationen zwischen den angeschlossenen Endsystemen dienen. Die Übertragung und der Zugriff auf freigegebene Ressourcen finden über spezifische Kommunikationswege statt. Die Endgeräte, wie beispielsweise Telefone, Computer, Server oder Terminals, sowie die Netzwerkknoten, wie Switches und Router, können sich entweder in einem lokalen Netzwerk (LAN) oder in einem Weitverkehrsnetzwerk (WAN) an verschiedenen räumlichen Orten befinden. Die Verbindung zwischen ihnen kann drahtlos beispielsweise über WLAN, GSM, UMTS oder LTE sowie auch alternativ drahtgebunden mittels Kabel oder Glasfaser erfolgen. (Dehn, 2017)

Ein Netzwerk setzt sich prinzipiell aus passiven und aktiven Komponenten zusammen. Passive Komponenten sind Geräte ohne eigene Stromversorgung, die nicht direkt am Datenverkehr eines Netzes beteiligt sind. Aktive Komponenten übernehmen direkt den Transport der Daten zwischen den Endgeräten und verfügen meist über eine eigene Stromversorgung, wenn sie nicht über Power over Ethernet (PoE) arbeiten. Sie sind für die Kontrolle und Anpassung des Datentransports zwischen den verschiedenen Segmenten eines lokalen oder Weitverkehrsnetzes verantwortlich. Aktive Komponenten strukturieren Netzwerke, regeln den Verkehr und optimieren die Routen. (Dehn, 2017)

Um Daten zwischen verschiedenen Computersystemen zu übertragen, werden verschiedene Komponenten benötigt: Netzwerkkarten, die die Kommunikation zwischen Rechnern und externen Systemen in einem Netzwerk ermöglichen. Sie dienen als Schnittstelle zwischen einem Endgerät und dem Datenträger und ermöglichen so den Datenaustausch. (Dehn, 2017) Switches agieren als Kopplungselemente, die die Funktion eines Verteilers übernehmen und für die Übertragung von Datenpaketen dienen. Router, ermöglichen die Verbindung von lokalen Netzwerken zu Weitverkehrsnetzwerken, Gateways dienen als Protokollumsetzer. Daten werden empfangen und entsprechend den Bedingungen des Zielgeräts umformatiert. Außerdem können weitere Komponenten wie Bridges, Repeater und Hubs Teil des Netzes sein. (Schnabel Patrick, 2023)

Die Firewall ist eine Sicherheitsvorrichtung, die unerlaubte und unbefugte Zugriffsversuche des öffentlichen Internets auf ein lokales Netzwerk verhindern soll. Dabei ermöglicht sie die Überwachung, Protokollierung, Blockierung und Freigabe des ein- und ausgehenden Datenverkehrs. Sie befindet sich üblicherweise an der Schnittstelle zwischen dem öffentlichen und dem lokalen Netzwerk und ist häufig in einen Router integriert. (Schnabel Patrick, 2023)

2.5.1 Drahtgebundenen Netzwerke

Um Daten mit drahtgebundenen Netzwerken übertragen zu können, ist es notwendig, einen Sender und einen Empfänger zu haben. Die Datenquelle, auch als Sender bezeichnet, übermittelt Informationen in Form von Datenframes an das Datenziel, den Empfänger. Dabei wird eine eindeutige Adresse verwendet, um den Empfänger zu identifizieren. Diese Informationen werden über ein Transportmedium wie Kabel oder Glasfaser weitergeleitet. (Dehn, 2017)

In einem Netzwerk regeln Protokolle den Kommunikationsprozess zwischen den Systemen. (Schnabel Patrick, 2023) Dies führt dazu, dass in der Regel mehrere Protokolle innerhalb einer Übertragung verwendet werden. (Dehn, 2017) Die Gliederung erfolgt gemäß einem ISO/OSI-7-Schichtenmodell, in dem jedes Protokoll eine spezifische Ebene zugeordnet ist. Die Datenübertragung in solchen Netzwerken erfolgt mittels der Ethernet-Technologie. Bei Ethernet handelt es sich um eine Familie von Netzwerktechnologien, die vorwiegend in LANs, aber auch zur Verknüpfung umfangreicher Netzwerke (WAN) eingesetzt werden. Unter der Verantwortung IEEE gibt es zahlreiche Standards für Ethernet. (Schnabel Patrick, 2023)

Referenzmodell des 7 Schichten OSI-Schichtmodells:

Um Prozesse in einzelne Arbeitsschritte zu unterteilen, wurden in der Computer- und Netzwerktechnik Schichtenmodelle entwickelt. Dabei wird jeder Prozessschritt bzw. jeder Task als eine Ebene in einem Schichtenmodell abgebildet. (Schnabel Patrick, 2023)

Tabelle 1: Referenzmodell ISO/ OSI-Modell (Eigene Darstellung nach Anlehnung (Schnabel Patrick, 2023))

	ISO/ OSI-Schicht	Protokoll Schicht	DoD- Schicht
7	Anwenderschicht	DNS HTTP SMTP IMAP	Applikation Layer
6	Darstellungsschicht		
5	Kommunikationsschicht		
4	Transportschicht	TCP UDP	Transport Layer
3	Vermittlungsschicht	IPv4 IPv6	Internet Layer
2	Sicherungsschicht	Ethernet, WLAN, Token Ring, FDDI, Frame Relay	Network Access Layer
1	Bitübetragungsschicht		

2.5.2 Kabellose Netzwerke

Im Bereich der lokalen Netzwerke haben sich vor allem zwei Standards durchgesetzt: Ethernet und WLAN. Ethernet basiert auf einer kabelgebundenen Übertragungstechnologie, während WLAN eine drahtlose Modifikation des Ethernet-Protokolls darstellt, bei der elektromagnetische Wellen zur Datenübertragung genutzt werden. WLAN wird überwiegend in Situationen genutzt, in denen eine Verkabelung unpraktisch oder nicht durchführbar ist. (Dehn, 2017)

Die Integration der WLAN-Technologie nimmt in Gesundheitseinrichtungen immer mehr an Wichtigkeit zu. Die Digitalisierung durch WLAN-Standards ist mittlerweile in den meisten Stationen üblich. Mobile Visitenwagen ermöglichen dem Fachpersonal sowie den Ärzten jederzeit den Zugriff auf die Patientendaten und das Hinzufügen von Verordnungen und neuen Befunden. Diese Informationen werden in der elektronischen Patientenakte gespeichert, die alle relevanten Daten des Patienten enthält. (Gärtner, 2010)

Einen wesentlichen Vorteil stellen mobile Geräte dar, die in den jeweiligen Stationen ortsunabhängig eingesetzt werden können. Abgesehen von den positiven Aspekten der ortsunabhängigen Kommunikation zwischen den Anwendern weisen die drahtlosen LAN-Standards auch einige Einschränkungen auf. (Gärtner, 2010) Das Anzapfen von Funkwellen ist im Vergleich zu kabelgebundenen Netzen wesentlich einfacher, da eine konventionelle Antenne genügt, um den Datenaustausch auch von externen Lauschern außerhalb des mit WLAN vernetzten Gebäudes zu erfassen. Die Reichweite der WLAN-Funkwellen beträgt bei normaler Nutzung je nach Gelände und Signalstärke etwa 150 Meter.

Sicherheitslücken: WLAN

Auch das WLAN zeigt Sicherheitslücken auf, da eine Datenübertragung durch die Ausbreitung von Funksignalen erfolgt. Der Übertragungsradius ist durch die Signalintensität begrenzt. Ein potenzieller Angreifer kann Daten abgreifen, indem er ein Empfängermedium in Reichweite der Funksignale positioniert. Es besteht auch das Risiko, dass Unbefugte die Funkinfrastruktur nutzen oder sich Netzzugang verschaffen. Es existieren diverse Angriffsszenarien, darunter Denial-of-Service, Man-in-the-Middle und IP-Spoofing. (Schnabel Patrick, 2023)

1. **Denial of Service (DoS)**

Bei einem Denial of Service (DoS) handelt es sich um einen gezielten Angriff auf die Verfügbarkeit bzw. Erreichbarkeit eines Dienstes, eines Servers oder eines ganzen Netzwerkes. Hierbei erfolgt typischerweise eine hohe Anzahl von Zugriffsversuchen auf den Dienst, den Server oder das Netzwerk, was dazu führt, dass diese überlastet werden und nicht mehr

erreichbar sind. In diesem Fall handelt sich es entweder um einen gezielten Anschlag oder um eine Fehlfunktion in der Software. (Schnabel Patrick, 2023)

2. **Man-in-the-Middle**

Beim Man-in-the-Middle-Angriff interveniert ein Hacker in die Verbindung zwischen zwei vertrauenswürdigen Teilnehmern. Der Täter gibt vor, dass seine Pakete von einem Computer gesendet werden, dem das angegriffene Ziel vertraut. Durch diese vorgetäuschte Identität kann der Eindringling das Ziel dazu verleiten, sämtliche Pakete an ihn zu übermitteln. Anschließend analysiert der Hacker die gesendeten Datenpakete und verfälscht sie bei Bedarf. (Schnabel Patrick, 2023)

3. **IP-Spoofing**

IP-Spoofing ist eine gängige Angriffsmethode, mit der ein potenzieller Täter die Schwachstellen des TCP/IP-Protokolls ausnutzt, um sich in die Position eines Man-in-the-Middle zu versetzen. Erreicht wird dies durch das Verschicken von IP-Datenpaketen mit einer vorgetäuschten Quell-IP-Adresse. Bei ARP-Spoofing handelt es sich um eine Methode des IP-Spoofings, bei der ein Hacker sich die Schwachstellen des Ethernet-Protokolls zunutze macht. Dafür werden vorgetäuschte ARP-Anfragen erstellt und die MAC-Adresse verändert, um den Datenverkehr umzulenken und abzufangen. (Schnabel Patrick, 2023)

Sicherheitsmaßnahmen für WLAN (Schnabel Patrick, 2023)**:**

- Separierung der WLANs von anderen Netzwerkabschnitten (Gast-WLAN),
- Eigenes Admin-Passwort für Zugangspunkt zuweisen,
- Installation eines IDS (Intrusion Detection System) im WLAN
- Verschlüsselung nach dem neuesten Stand der Technik (WPA 2 /IEEE 802.1x)

2.5.3 Medizinisches Netzwerk

Nach der DIN EN 80001-1:2011 umfasst ein medizinisches Netzwerk ein IT-Netz, in das aktive medizinische Geräte eingebunden sind. Die Fähigkeit zum Austausch von Daten und zur gemeinsamen Nutzung zwischen verschiedenen medizinischen Systemen, die Netzwerke impliziert, bedeutet, dass Netzwerke einen essenziellen Bestandteil der Patientenversorgung darstellen. In Gesundheitseinrichtungen werden medizinische Daten über IT-Netzwerke transportiert. (Gärtner, 2010)

Diese Daten umfassen administrative Informationen, Bilder und Befunde sowie kritische Vitaldaten und Alarmmeldungen von Überwachungsmonitoren. Auf diese Weise entstehen

medizinische Netzwerke, die eine große Anzahl angeschlossener medizinischer Systeme umfassen. Diese Systeme bestehen aus einer Konfiguration von medizinischen Geräten, Netzwerkkomponenten (Hardware, Software) und Servern. In medizinischen Netzwerken befinden sich aktive Medizinprodukte wie Modalitäten und programmierbare medizinische elektrische Systeme (PEMS) als Netzwerkkomponenten. (Gärtner, 2010)

Wie in Abschnitt 2.4 erläutert, ermöglicht die Kompatibilität standardisierter Schnittstellen den Datenaustausch zwischen Komponenten oder Modulen, die dieselbe Schnittstelle unterstützen. Im Gesundheitswesen werden spezifische Standards verwendet, um sicherzustellen, dass diese Interoperabilität gewährleistet ist. (Kramme, Medizintechnik, Verfahren - Systeme - Informationsverarbeitung, 2011)

Bei einer fortschreitenden Vernetzung und Übertragung medizinischer Daten über medizinische Netzwerke, insbesondere bei zeitsensiblen Daten können die folgenden Herausforderungen auftreten (Gärtner, 2010):

- Computer- und Kernspintomographen können keine Aufnahmen mehr aufzeichnen
- IP-Adresskonflikte verursachen, dass Alarmmeldungen auf einer Intensivstation nicht übermittelt werden und Patienten zu Schaden kommen oder verunglücken, weil das Personal nicht benachrichtigt wird.
- Netzüberlastung durch Live-Übertragung von Bildern aus einem Schlafanalyselabor
- Fehlerhafte Konfiguration eines Routers im Kernnetz, Versagen
- Hersteller installiert Firmware auf einem Switch, eine Anwendung fällt aus.
- Ausfall der USV für eine abgesetzte Anlage, Fehlfunktion oder Versagen der USV während des periodischen Funktionstests der Notstromversorgung.
- Fehlererkennung von Netzwerkkarten
- Schadsoftware im Netzbetrieb

2.5.5 Wireless-Bridge-Gerät

Eine Netzwerkbrücke (Bridge) fungiert als ein Gerät, das die Aufgabe hat, ein lokales Netzwerk in zwei getrennte Segmente aufzuteilen. Hierbei werden die negativen Aspekte von Ethernet, die vor allem in größeren Netzwerken auftreten, kompensiert. Die Nutzung von Bridges als Verbindungselement ist heute eher selten, da die Limitierungen von Ethernet eher durch den Einsatz von Switches umgangen werden. Grundsätzlich enthält eine WLAN-Topologie drahtlose Netzwerkteilnehmer, die als WLAN-Clients betrachtet werden, und mindestens eine WLAN-Basisstation, die als Wireless Access Point (WAP) oder als Access Point (AP) dargestellt wird. (Schnabel Patrick, 2023)

Innerhalb eines WLAN ist der Access Point das einzige aktive Element der Schicht 2. Ähnlich wie eine Bridge stellt der Access Point die Verbindung zwischen zwei Netzwerken verschiedener physikalischer Ebenen her, z. B. zwischen drahtlosem LAN und kabelgebundenem Ethernet. Die Bildung eines Extended Service Sets (ESS/IEEE 802.11c) erfolgt, wenn mehrere Access Points in Form von zwei oder mehreren Basic-Service-Sets eine drahtlose Verbindung zueinander herstellen. Die Nutzung der Bridging-Technologie zwischen zwei Access Points ermöglicht eine Ausdehnung der Reichweite eines lokalen Netzwerks ohne den Einsatz von physischen Verbindungen. Dadurch können Bereiche miteinander verbunden werden, die mit konventionellen Kabeln nicht möglich wären. Der Standard IEEE 802.11c ermöglicht die drahtlose Verbindung zweier Netzwerktopologien mittels WLAN. Dies wird durch den Einsatz von zwei Access Points erreicht, die eine spezielle Funkstrecke aufbauen. Die Erkennung der Gegenstation wird anhand der MAC-Adresse realisiert, wodurch Verbindungsversuche von herkömmlichen drahtlosen Geräten abgelehnt werden. (Schnabel Patrick, 2023)

3 Risikomanagement nach DIN EN 80001-1:2011

Risikomanagement ist ein Instrument der Unternehmensführung, das darauf abzielt, Fehler oder Risiken, die auf eine Organisation Einfluss nehmen, zu identifizieren, zu bewerten, vermeiden oder in ihren Auswirkungen zu begrenzen. Es beinhaltet auch die Bewertung der Effektivität der ergriffenen Vorkehrungen. Das Ziel des Risikomanagements besteht darin, Risiken zu erfassen, zu bewerten und steuerbar zu machen. Alle externen und internen Gefahren, die auf eine Einrichtung zukommen, werden im Rahmen eines umfangreichen Risikomanagements berücksichtigt. Dabei werden auch Risiken auf strategischer Ebene untersucht, wie beispielsweise Corporate Governance, Änderungen im organisatorischen Umfeld, Kundensegmente und Märkte, Produkte und Dienstleistungen sowie Finanzen. (Wolfgang & Ehrenbaum, 2011)

Das Risikomanagement in Krankenhäusern birgt heutzutage bereits eine Fülle von Forderungen und Regularien, um die Unternehmensziele zu gewährleisten. Darüber hinaus sind Krankenhäuser aufgefordert, effiziente Lösungen für wachsende Anforderungen durch den Gebrauch moderner Informations- und Kommunikationstechnologien (IKT) zu entwickeln. Um die Maßnahmen in diesem Bereich zu systematisieren und die Wirksamkeit des Risikomanagements zu verbessern, wurde die internationale Norm IEC 80001-1:2010 „Application of risk management for IT-networks incorporating medical devices“ erarbeitet. Die Nutzung moderner Informations- und Kommunikationstechnologien bietet bedeutende Möglichkeiten, die Qualität der Versorgung zu verbessern und die Sicherheit der Patienten zu steigern. (DKG, 2011)

Die Integration verschiedener Systeme und Komponenten in medizinischen IT-Netzwerken ist eine grundlegende Anforderung. Dies gilt insbesondere für vielfältige Anwendungen, darunter die Erfassung von Patientendaten in elektronischer Form, die Speicherung und Dokumentation von Befunden, die elektronische Unterstützung der Medikamententherapie, intensivmedizinische Alarmmeldungen oder telemedizinische Anwendungen. Bei der Einbindung vernetzbarer Medizingeräte in existierende IT-Netzwerke ergeben sich spezifische Fragestellungen. Diese müssen eine Bandbreite von verwaltungstechnischen und klinischen Anforderungen unterstützen. (DKG, 2011)

Beispielsweise müssen Lösungen gefunden werden, um mit den Auswirkungen eines Netzwerkausfalls oder einer Unterbrechung der Netzwerkkommunikation während des Gebrauchs dieser Medizingeräte umzugehen. Diese Aspekte erfordern eine systematische Analyse und Beantwortung durch das Risikomanagement, um adäquat auf mögliche

Gefahrensituationen reagieren zu können. Die Bereitstellung von Informationen ist für zahlreiche Anwendungsbereiche von wesentlicher Bedeutung. Sollte ein Dienst nicht verfügbar sein oder können beispielsweise Alarmmeldungen nicht übermittelt werden, resultieren daraus Gefahrensituationen, für die das Risikomanagement entsprechende Gegenmaßnahmen vorsehen muss. (DKG, 2011)

Der vorliegende Standard ist primär für Betreiber medizinischer IT-Netzwerke, aber auch für Anbieter von Medizinprodukten und Netzwerkprodukten relevant. Die in der Norm festgelegten Schutzziele sind die Sicherheit (Sicherheit der Patienten), die Sicherheit der Daten- und Systemsicherheit und Effektivität (Wirksamkeit der Vorkehrungen). Um die DIN EN 80001-1:2011 umzusetzen, sind die Benennung der Risikomanagementziele, die Zuweisung von Verantwortlichkeiten innerhalb des Betriebes und die Ernennung eines Risikomanagers erforderlich. Der Risikomanager ist für die Steuerung, Koordination und Dokumentation aller relevanten Abläufe und Informationsflüsse zwischen den beteiligten Akteuren verantwortlich. (DKG, 2011)

Der folgende Implementierungsleitfaden unterstützt die Krankenhausleitung sowie die Verantwortlichen in den Bereichen Informationstechnologie und Medizintechnik bei der Implementierung der Prozesse des Risikomanagements. Dabei wird auch die Integration in das übergeordnete Risikomanagement des Krankenhauses berücksichtigt. (DKG, 2011)

3.1 Verantwortliche Organisation

Einrichtungen, die medizinische Produkte wie Geräte oder Software in medizinischen IT-Netzwerken anwenden, müssen eindeutige Zuständigkeiten für die Integration dieser Medizingeräte in solche Netzwerke definieren. Die übergeordnete Verantwortung für das Risikomanagement von medizinischen IT-Netzwerken trägt die verantwortliche Organisation, die je nach Unternehmensform und Struktur der Konzern, der Klinikverbund oder das Einzelkrankenhaus als Anwender der Medizinprodukte in medizinischen IT-Netzwerken sein kann. Die verantwortliche Organisation ist dafür verpflichtet, einen Prozess zu implementieren, der alle Tätigkeiten des Risikomanagements im Verlauf des gesamten Lebenszyklus des medizinischen IT-Netzwerks abdeckt. Dieser beinhaltet die Planung, Entwicklung, Installation, Geräteverbindung, Konfiguration, Anwendung, Wartung und das außer Betrieb nehmen von Geräten. (siehe Abbildung 1) (DKG, 2011) Es liegt in der Verantwortung der obersten Führungsebene, die Strategie, Richtlinien und Maßnahmenkataloge zu genehmigen und somit verbindlich zu machen. Die Führung trägt die Verantwortung für sämtliche Aspekte und nicht

nur für die Genehmigung einzelner Elemente. Diese müssen anschließend in der Organisationsstruktur konsequent umgesetzt werden. (Gärtner, 2010)

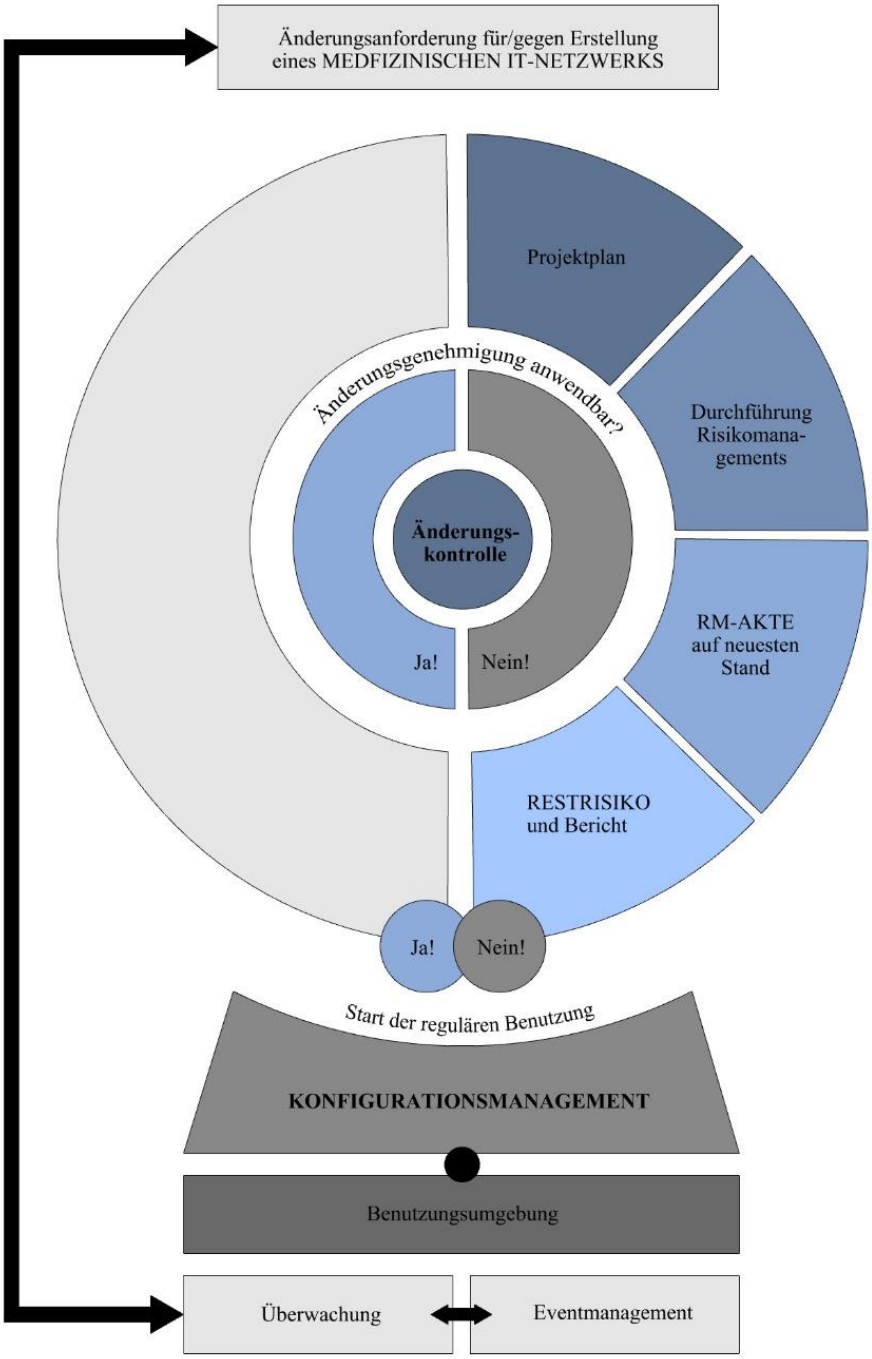

Abbildung 1: Lebenszyklus (Eigene Darstellung nach Anlehnung (DKG, 2011))

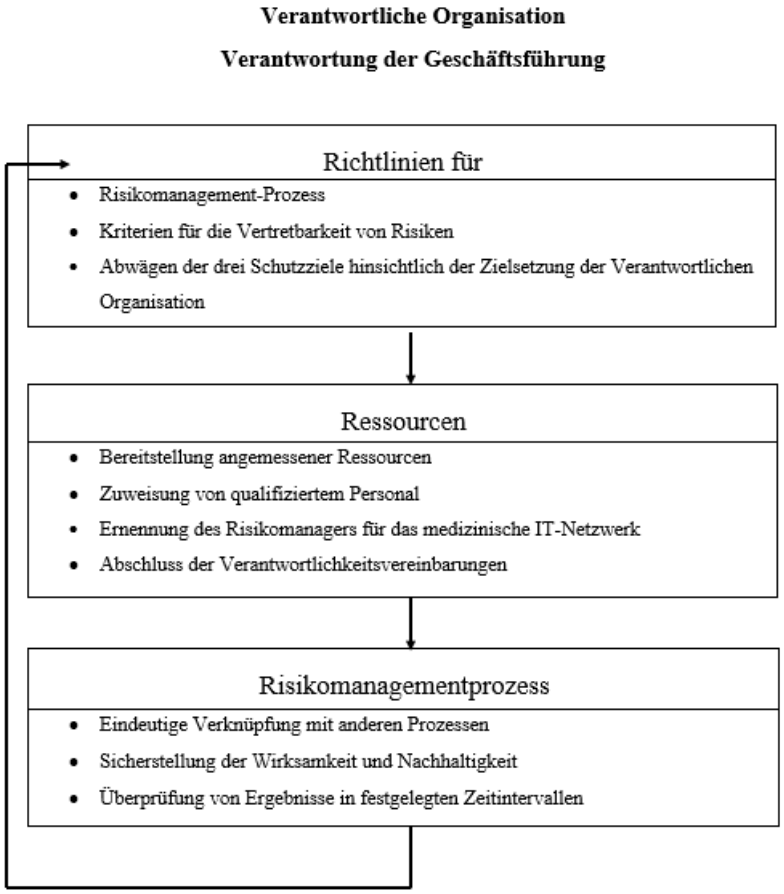

Abbildung 2: Verantwortliche Geschäftsebene (Eigene Darstellung nach Anlehnung (DKG, 2011))

Wie in der Abbildung 2 ersichtlich, ist die oberste Führungsebene verantwortlich für die Initiierung eines Risikomanagementprozesses durch die Schaffung der Stelle eines Risikomanagers und die Bereitstellung der erforderlichen Ressourcen. Dazu gehört die Entwicklung einer Unternehmensstrategie für den Einsatz und die Handhabung von medizinischen Netzwerken sowie die Erstellung von Richtlinien und Maßnahmenkatalogen, die festlegen, wie das medizinische Netzwerk genutzt werden soll, welche Vorkehrungen bei Ausfällen, Unterbrechungen oder Malware-Angriffen zu treffen sind. (Gärtner, 2010)

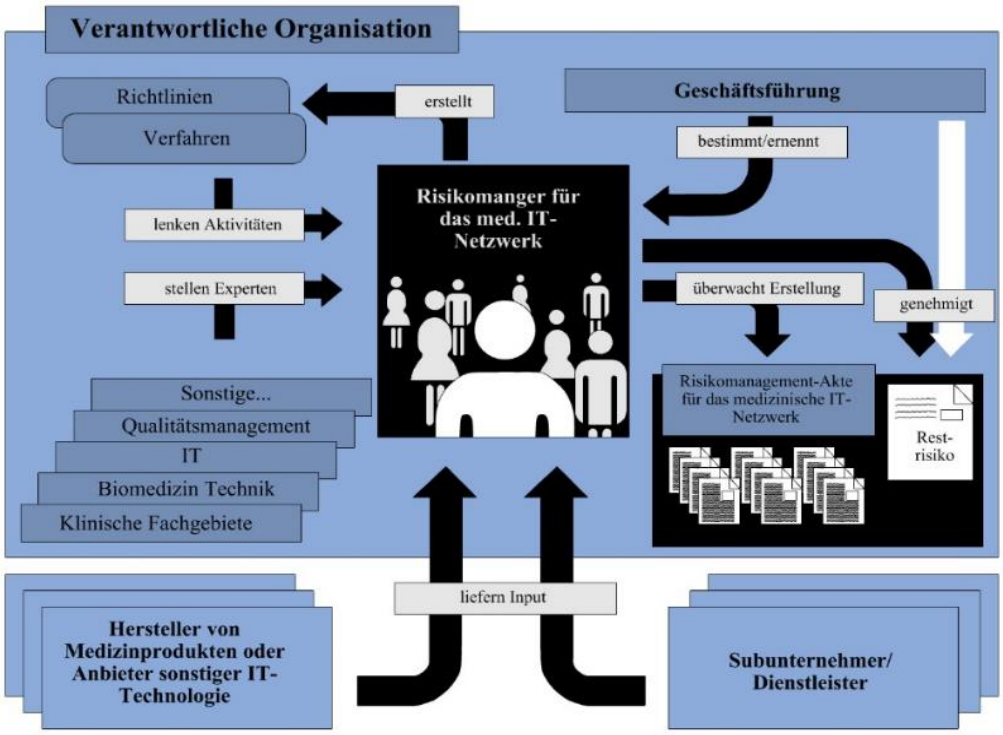

Abbildung 3: Verantwortliche Organisation (Eigene Darstellung nach Anlehnung (DKG, 2011))

Die Abbildung 3 veranschaulicht, dass der Risikomanager eine Schlüsselfigur im ganzen Prozess ist. Er agiert als Schnittstelle zwischen, der Medizintechnik, der IT-Abteilung, dem Einkauf und der Unternehmensleitung. Damit der IT-Risk-Manager einen Risikomanagement-Prozess einleiten kann, benötigt er verschiedene Informationen, die er durch effektive Kommunikation mit MP-Herstellen aufbaut und aufrecht haltet. Die zur Verfügung gestellten Unterlagen sollen in der Risikomanagement-Akte dokumentiert werden. Gemäß den Richtlinien der DIN EN ISO 14971 gibt es keine spezifische Vorgabe für das Format einer Risikomanagement-Akte. Es ist daher offen, ob sie in schriftlicher oder elektronischer Weise geführt wird. (DKG, 2011)

3.2 Schutzziele

Die DIN-EN 80001-1 definiert drei grundlegende Schutzziele: Sicherheit, Datenschutz und Systemsicherheit sowie Effektivität. Diese Ziele haben das Ziel, potenzielle Gefahren zu verhindern und die daraus resultierenden Schäden zu minimieren. (DKG, 2011) Die Informationssicherheit beinhaltet weitere grundlegende Schutzziele und Werte. Dieses wären die Verfügbarkeit, Integrität und Vertraulichkeit. (Darms, Haßfeld, & Fedtke, 2019) Diese

Risiken können durch Störungen, Manipulationen, Ausfälle, Malware und andere Faktoren verursacht werden. (Gärtner, 2010)

Sicherheit (Patientensicherheit)

Der Definitionsbegriff Sicherheit bezieht sich in diesem Kontext auf die Sicherheit von Patienten, Betreibern und Dritten. (DKG, 2011) Es ist äußerst wichtig, dass die Gesundheit eines Patienten nicht durch Störungen oder Fehler in der Informationstechnologie im Krankenhaus beeinträchtigt wird, da dies zu einer unzureichenden oder beeinträchtigten Behandlung führen kann. (BSI, 2023)

Daten- und Systemsicherheit

Um die Sicherheit von Daten und Systemen zu gewährleisten, ist es unerlässlich, geeignete Sicherheitsmaßnahmen zu implementieren, um mögliche oder potenzielle Bedrohungen auszuschließen. (DKG, 2011)

Effektivität

Das Schutzziel der Effektivität konzentriert sich auf die Realisierung der angestrebten Prozesse. Dazu gehört beispielsweise die verlässliche Übermittlung von Informationen zur Patientenversorgung oder die Durchführung medizinischer Abläufe. (DKG, 2011)

Verfügbarkeit (Datenzugriff)

Die Nutzbarkeit von IT-Komponenten ist gewährleistet, wenn diese von den Betreibern kontinuierlich und ohne Einschränkungen genutzt werden können. Ein Mangel an grundlegenden Informationen oder Systemen wird in der Regel schnell bemerkt, insbesondere, wenn Tätigkeiten ohne sie nicht fortgesetzt werden können. Bei einem Ausfall eines IT-Systems sind der Zugriff auf Patientendaten, die Erstellung neuer Patientenakten und medizinische Eingriffe nicht möglich. (Darms, Haßfeld, & Fedtke, 2019)

Vertraulichkeit (Datenschutz)

Vertraulichkeit umfasst den Schutz vor unberechtigter Weitergabe von Informationen. Der Zugang zu vertraulichen Daten und Informationen sollte nur autorisierten Personen in entsprechender Form erlaubt sein. (Darms, Haßfeld, & Fedtke, 2019) Die daraus resultierenden Risiken bezeichnen potenzielle Bedrohungen, bei denen Daten von unbefugten Personen eingesehen oder sogar manipuliert werden können, ohne dass dies von den autorisierten Nutzern beabsichtigt ist. (Seilbold, 2006) Vertrauliche Unternehmensdaten lassen sich an verschiedenen Schnittstellen ausspähen, beispielsweise durch das Eindringen in

Sicherheitslücken oder gezielt installierte Backdoors in der Applikationssoftware oder in Betriebssystemen. (Darms, Haßfeld, & Fedtke, 2019)

Integrität (Datensicherheit)

Integrität bezieht sich auf die Gewährleistung der Richtigkeit von Daten und der ordnungsgemäßen Funktionalität von Systemen. Der Verlust oder die Manipulation von Daten kann zu schwerwiegenden Konsequenzen führen, wie fehlerhaften Behandlungen oder falschen Medikationen. Ein Beispiel hierfür ist die Verwendung falscher Datensätze bei der Strahlentherapie, was zu schweren Schäden oder sogar zum Tod des Patienten führen kann. Wenn Daten aufgrund von Manipulation, Eingabefehlern oder Softwarefehlern versehentlich einer falschen Person zugewiesen werden, können unerwünschte Konsequenzen auftreten. (Darms, Haßfeld, & Fedtke, 2019)

3.3 Prozesse des Risikomanagements

Die Norm 80001-1 legt den Prozess des Risikomanagements für medizinische IT-Netzwerke fest und gliedert ihn in mehrere Schritte. Diese werden im Folgenden näher erläutert.

3.3.1 Risikopolitik

Die Risikomanagement-Politik ist ein integraler Bestandteil der Unternehmenspolitik und beinhaltet wesentliche Informationen für das unternehmensweite Risikomanagement-Framework. Das Rahmenwerk muss sicherstellen, dass die Geschäftsleitung eine adäquate und aktualisierte Risikomanagementpolitik unterstützt und diese an alle relevanten Stakeholder kommuniziert wird. Die Unternehmenspolitik kann verschiedene Inhalte zur Einbindung des Risikomanagements in das Unternehmensmanagementsystem enthalten. (Königs, 2017)

Grundsätze für das Risikomanagement (Königs, 2017)**:**

- Aufgabe und Engagement der Unternehmensleitung
- Externer und interner Zusammenhang
- Zweck und Zielsetzung des Risikomanagements
- Leitlinien für die Risikoklassifizierung und die Akzeptanz- und Toleranzkriterien
- Spezifikation des Frameworks mit seiner Grundstruktur und den wichtigsten Anweisungen für die Durchführung, darin eingeschlossen die Zuständigkeiten und die Zuweisung von Ressourcen.
- Überwachung, Revision und Maßnahmen zur stetigen Optimierung des Risikomanagements

- Anforderungen des definierten Risikomanagements-Frameworks
- Sensibilisierungs- und Kommunikationsanforderungen

3.3.2 Risikomanagementplanung

Der Risikomanagementprozess nach DIN EN 80001-1 sollte Bestandteil des bestehenden umfassenden Risikomanagements im Krankenhaus sein. Gemäß den Normanforderungen sind alle Bearbeitungsschritte und die erzielten Ergebnisse in der Risikomanagement-Akte zu protokollieren. Ausgangspunkt für die Risikomanagementplanung sollte die Definition des fachlichen Projektumfangs (Scope-Definition) unter Beachtung der allgemein gültigen Grundlagen des Projektmanagements sein. (DKG, 2011)

Erfasst werden dabei im Wesentlichen die Ziele des Projektes, die relevanten Workflows und Konfigurationselemente sowie signifikante, beispielsweise entscheidende Rahmenbedingungen. Zunächst erfolgt eine Planung der zeitlichen und finanziellen Aspekte, welche die Basis für den Risikomanagement-Plan bilden. Weiterhin wird im Rahmen der Scope-Definition eine offizielle Festlegung der zu inspizierenden Systeme durchgeführt. Es ist wichtig, während der Scope-Definition explizit bestimmte Risiken einzuschließen oder auszuschließen, da diese Festlegung die Basis für alle nachfolgenden Inspektionen darstellt. (DKG, 2011)

3.3.3 Ressourcenplanung

Die Benennung eines Risikomanagers durch die Geschäftsführung, der als Projektleiter und Vermittler des Risikomanagements agiert, ist der primäre Schritt der Ressourcenplanung. Wie auch im Punkt 3.1 beschrieben. Bevor weitere Schritte unternommen werden, sollte eine Verantwortlichkeitsvereinbarung zwischen den beteiligten Akteuren abgeschlossen werden. Darin wird eine Person beauftragt, die für das Risikomanagement verantwortlich ist. Der Projektrahmen wird skizziert und die betroffenen Medizinprodukte werden aufgelistet. Die Zusammenarbeit wird detailliert beschrieben, einschließlich der Initiierung, der Kontaktpersonen und der Prüfkriterien für die Erfüllung der Verantwortlichkeiten durch die Partner. (Ahlbrandt, et al., 2013)

3.3.4 Betroffene Systeme

Die zu analysierenden Systeme müssen vor der Durchführung der Risikoanalyse identifiziert werden. Dies kann beispielsweise durch vorhandene Grundrisspläne im System erfolgen, in

denen die Standorte der Medizinprodukte verzeichnet sind, oder durch Inventarlisten. (DKG, 2011)

3.4 Begleitpapiere

Um potenzielle Risiken bei der Konnektivität von medizinischen Geräten zu identifizieren und beurteilen zu können, ist die Verfügbarkeit der herstellerseitigen Unterlagen unabdingbar. Diese Dokumentation stellt eine wesentliche Grundlage für ein effizientes Risikomanagement nach den Vorgaben der DIN EN 80001-1 dar. Der Hersteller ist verpflichtet, relevante Funktionsparameter, Leistungseigenschaften und Konfigurationsmöglichkeiten zu berücksichtigen, die für eine sichere Anwendung der betreffenden Produkte zu berücksichtigen sind. Risiken können nur dann erkannt und verhindert werden, wenn alle Informationen vom Gerätehersteller veröffentlicht werden.

Der Hersteller eines Medizinproduktes, das vernetzt werden soll, ist verpflichtet, die damit verbundenen Gefährdungen für den Anwender des Gerätes in der Dokumentation erkennbar zu machen. Dazu gehören Informationen zu Leistungseigenschaften wie Datenrate und Geschwindigkeit der Datenübermittlung sowie zur Konfigurationsmöglichkeit des IT-Netzwerkes, in das das Gerät integriert werden soll. Darüber hinaus sind technische Eigenschaften der Netzwerkanbindung und Sicherheitsaspekte wie Verschlüsselung bei WLAN-Anschlüssen anzugeben. Gemäß der dritten Ausgabe der DIN EN 60601-1 müssen Informationen zu vernetzbaren Medizinprodukten zum Zeitpunkt des Inverkehrbringens bereits in den Begleitpapieren enthalten sein. Diese Begleitdokumente müssen vorliegen, um eine Konformitätsbewertung zu ermöglichen. Für bereits vorhandene gleichartige Geräte, die nach einer älteren Version der DIN EN 60601-1 in Verkehr gebracht wurden, wird zur Sicherstellung eines einheitlichen Informations- und Schutzniveaus empfohlen, dass der Hersteller auch für diese Geräte die entsprechenden Informationen zur Verfügung stellt. Die DIN EN 80001-1:2011 definiert Mindestanforderungen an die Begleitdokumentation und sonstige Hinweise für vernetzbare Medizinprodukte, die zur Integration in ein IT-Netzwerk bestimmt sind. (DKG, 2011)

Diese Anleitungen nach der Norm müssen mindestens folgende Angaben enthalten (DKG, 2011)**:**

- Der Verwendungszweck der Integration des Medizingerätes in ein IT-Netz
- Die erforderlichen Leistungseigenschaften des IT-Netzes, in das das Medizingerät integriert wird

- Die notwendige Konfiguration des IT-Netzwerks, in das das Medizingerät eingebunden wird.
- Die technischen Eigenschaften und Sicherheitsvorgaben für den Netzanschluss des Medizingeräts.
- Den geplanten Datenfluss zwischen dem Medizingerät, dem medizinischen IT-Netzwerk und anderen Teilnehmern des Netzes. Gegebenenfalls ist auch der geplante Streckenverlauf durch das medizinische IT-Netz vorzulegen.
- Eine Aufstellung der potenziellen Risikosituationen, die auftreten können, wenn das IT-Netzwerk nicht die notwendigen Leistungseigenschaften aufweist, um den Integrationszweck des Medizingeräts zu erzielen.

3.5 Risikoanalyse „10-Punkte-Plan“

„Der Technical Report TR 719 Step by step risk management of medical IT networks - Practical applications and examples“ dient als ergänzende Richtlinie zur Grundnorm und vermittelt praktische Anwendungshinweise. Die Risikobetrachtung basiert auf der Analyse potenzieller Gefahren im Zusammenhang mit der beabsichtigten Nutzung. Eine Bedrohung kann durch spezifische Vorfälle (ereignisbezogen) als auch unabhängig davon (ereignisunabhängig) verursacht werden. Die Identifizierung möglicher Gefahrenquellen ist ein entscheidender Faktor bei der Risikoanalyse. (DKG, 2011)

Der Ablauf nach DIN EN 80001-1 wurde in zehn Schritte unterteilt, Im Folgenden werden die Arbeitsschritte dargestellt und den entsprechenden Abschnitten, die jeweils in Risikoanalyse, Risikobewertung und Risikokontrolle unterteilt werden, der Norm zugewiesen (DKG, 2011):

Risikoanalyse:

Schritt 1: Identifikation der Gefährdungen

Schritt 2: Ermittlung der Ursachen und Gefährdungssituationen

Schritt 3: Ermittlung sämtlicher nicht beobachteter Folgen und ihres Schweregrads

Schritt 4: Abschätzung der Eintrittswahrscheinlichkeit

Risikobewertung:

Schritt 5: Bewertung der Gefahren anhand definierter Akzeptanzkriterien

Risikokontrolle:

Schritt 6: Festlegung und Protokollierung der Maßnahmen

Schritt 7: Umsetzung der Maßnahmen

Schritt 8: Überprüfung der Maßnahmen

Schritt 9: Bewertung aller Risiken durch entstehen der Maßnahmen

Schritt 10: Bewertung und Berichterstattung des Restrisikos

3.6 Risiko ermitteln

Nach Festlegung der Grundlagen für das Risikomanagement können die möglichen Risiken identifiziert werden. Risiken werden durch Gefahren hervorgerufen, die mit einer bestimmten Häufigkeit zum Schadenseintritt in einer bestimmten Schadenshöhe beitragen. Eine Gefährdung kann unterschiedliche Risiken mit verschiedenen Eintrittswahrscheinlichkeiten und Schadenshöhen zur Folge haben. Die Bewertung der Bedrohungen und der entsprechenden Risiken für ein vernetztes Medizingerät beruht hauptsächlich auf verfügbaren Informationen. (DKG, 2011)

Die Informationen, die dem Risikomanagement beigefügt sind, oder die Auswertung relevanter Fragebögen können auch als Anhaltspunkt für die Ermittlung und Dokumentation von Risiken in medizinischen IT-Netzen dienen. Eine zielgerichtete Vorgehensweise unter Einbindung aller verfügbaren Informationen ist erforderlich und stellt den größten Part des Risikomanagements dar. Gleichzeitig ist es ein entscheidender Erfolgsfaktor für das gesamte Projekt, dass die möglichen Risiken vollständig erfasst werden. Die systematische Risikoerfassung sollte stets durch den Einsatz geeigneter Hilfsmittel wie Checklisten, Brainstorming, Auswertung von Wissensdatenbanken und SWOT-Analyse begleitet werden. (DKG, 2011)

3.7 Risikoanalyse

Nachdem die Risiken im vorherigen Prozess der Risiko-Identifikation erkannt und ihre Merkmale ermittelt wurden, zielt der nachfolgende Prozess der Risiko-Analyse darauf ab, ein umfassenderes Risikoverständnis zu erreichen und das Ausmaß der Risiken abzuschätzen. Dabei werden Eintrittswahrscheinlichkeiten und Schadensausmaß analysiert, um die Höhe des Risikos zu bestimmen. Dieser Prozess liefert wichtige Informationen für Entscheidungen, die zu einem angemessenen Umgang mit den Risiken führen sollen. Die Risikoanalyse führt zu einer Bewertung der Risikohöhe, die entweder qualitativ, quantitativ oder semiquantitativ erfolgen kann. Neben der Bestimmung der Risikohöhe werden von der Risikoanalyse weitere Outputs gefordert, wie beispielsweise die Identifikation der Risikoursachen oder Vorgaben für die Priorität der Risikobearbeitung. (Königs, 2017) Gemäß den vorgegebenen Anforderungen kann die Risiko-Analyse entweder quantitativ oder qualitativ erfolgen. (DKG, 2011)

Qualitative Risikoanalyse:

Durch die Risikoanalyse werden die ermittelten Risiken anhand ihrer Wahrscheinlichkeit und qualitativen Auswirkungen auf das Unternehmen eingestuft. Die Risiken werden dann in einer übersichtlichen Aufstellung gruppiert und priorisiert. Die Risikodarstellung erfolgt in einer Matrix, die die Konsequenzen der Risiken in Abhängigkeit von ihrer Eintrittswahrscheinlichkeit abbildet. (DKG, 2011)

Quantitative Risikoanalyse:

Die in der qualitativen Risikoanalyse eingestuften Gefährdungen werden nun hinsichtlich ihrer Einflüsse auf die festgelegten Schutzziele und Vorgaben des Risikomanagements untersucht. Im Gegensatz zur qualitativen Risikoanalyse erfolgt hier eine möglichst genaue quantitative Beurteilung, beispielsweise Vermögensschaden oder Beeinträchtigung der Patientenbetreuung der erhobenen Risiken vorzunehmen. Geeignete Vorkehrungen zur Reduzierung des Schadensausmaßes oder der Eintrittshäufigkeit können auf Grundlage dieser Analyse getroffen werden. Die zuvor festgelegten Anforderungen an das Risikomanagement bilden den Handlungsrahmen für die weiteren Entscheidungen der verantwortlichen Organisation. (DKG, 2011)

Risikoanalyse: Vorgehensweise (DKG, 2011)

1. Ermittlung aller Gefährdungen und ggf. Hinzufügung von Einzelheiten/Erläuterungen.
2. Für sämtliche Gefahren aus Schritt 1 gilt es, mögliche Ursachen und potenzielle Gefährdungssituationen zu identifizieren. (siehe Tabelle 2)
3. Die Eintrittswahrscheinlichkeiten der unbeabsichtigten Auswirkungen in Bezug auf die jeweilige Gefährdungssituation werden bestimmt. (siehe Tabelle 3)
4. Bewertung der Risiken anhand definierter Akzeptanzkriterien (siehe Tabelle 4)

Tabelle 2: Schweregrad von Risiken (Eigene Darstellung nach Anlehnung (DKG, 2011))

	Patientensicherheit	**Daten- und Systemsicherheit (Vertraulichkeit & Integrität)**	**Effektivität**
Katastrophal	Schwere Verletzung, Tod	Kann zu vollständiger Offenlegung sensibler Informationen führen.	Geplante Operationen/ Prozeduren nicht mehr durchführbar
Hoch	Dauerhafte Beeinträchtigung physischer Funktionen oder dauerhafte Schädigung physischer Strukturen	Kann zu signifikanter Offenlegung sensibler Informationen führen.	Geplante Operationen/ Prozeduren unterbrochen oder verzögert
Moderat	Zeitlich begrenzte und geringere Verletzungen, medizinische Intervention erforderlich	Offenlegung sensibler Informationen könnte negative (finanzielle) Folgen haben und möglicherweise einigen Ressourcenaufwand zur Beseitigung bedingen.	Belästigender bis unterbrechender Effekt auf Operationen/ Maßnahmen
Gering	Zeitlich begrenzte Unannehmlichkeiten, reversibel ohne medizinische Intervention	Offenlegung sensibler Informationen wird nur geringe Auswirkungen auf die Organisation oder einzelne Personen haben. Bedingt geringen Ressourcenaufwand zur Beseitigung.	Sehr begrenzter oder belästigender Effekt auf Operationen/ Maßnahmen
Vernachlässigbar	Geringe und kurzzeitige Unannehmlichkeiten	Bekanntwerden einer entsprechenden Bedrohung oder Schwachstelle hat vernachlässigbaren Einfluss.	Kein oder sehr begrenzter Einfluss auf Operationen/ Prozeduren

Tabelle 3: Eintrittswahrscheinlichkeit von Risiken (Eigene Darstellung nach Anlehnung (DKG, 2011))

Häufig	Unbeabsichtigte Auswirkungen treten häufig oder immer auf.
Wahrscheinlich	Es ist sehr wahrscheinlich, dass unbeabsichtigte Auswirkungen auftreten.
Selten	Es können hin und wieder unbeabsichtigte Auswirkungen auftreten.
Fernliegend	Es ist nicht wahrscheinlich, dass unbeabsichtigte Auswirkungen auftreten.
Unwahrscheinlich	Es ist sehr unwahrscheinlich, dass unbeabsichtigte Auswirkungen auftreten.

Tabelle 4: Risiko-Level-Matrix (Eigene Darstellung nach Anlehnung (DKG, 2011))

	Unbeabsichtigte Auswirkungen für Patientensicherheit, Daten- und Systemsicherheit und Effektivität	**Eintrittswahrscheinlichkeit** →				
Schweregrad ↑		**Unwahr-scheinlich**	**Fernliegend**	**Gelegentlich**	**Wahr-scheinlich**	**Häufig**
	Katastrophal					
	Kritisch					**Hoch**
	Ernst			**Moderat**		
	Gering	**Gering**				
	Vernachlässigbar					
Gering	Risiko ist akzeptabel, es sind keine weiteren Maßnahmen zur Risikobeherrschung erforderlich.					
Moderat	Die Akzeptanz des Risikos muss abgewogen werden. Auswirkungen auf die Kernziele sind vorhanden, die Praktikabilität möglicher Maßnahmen der Risikobeherrschung muss jedoch berücksichtigt werden. In Abhängigkeit davon kann das Risiko möglicherweise akzeptiert werden. Der Betreiber sollte Richtlinien für Risiken dieser Stufe definieren, die bspw. spezielle Team-Reviews oder die Abnahme durch die Geschäftsführung verlangen, grundlegende Prinzipien definieren oder den Nachweis der Reduktion auf das „vernünftigerweise Praktikable“ vorschreiben.					
Hoch	Risiko ist nicht akzeptabel, Eintrittswahrscheinlichkeit oder Schweregrad der Auswirkungen müssen zunächst reduziert werden, bevor das Medizinische IT-Netzwerk/ vernetzte Medizinprodukt eingesetzt werden kann.					

3.8 Risikobewertung

Das Ziel der Risikobewertung besteht darin, festzustellen, ob ein Risiko für die Einrichtung tolerierbar ist bzw. nicht akzeptabel ist. Hierbei wird die Höhe des Risikos, welches sich aus der Kombination von Eintrittswahrscheinlichkeit und Konsequenzen zusammensetzt, mit vordefinierten Risikokriterien verglichen. Diese Kriterien legen fest, welche Risikoarten das Klinikum bereit ist zu verantworten (Risikoakzeptanz) sowie Maßnahmen zur Risikobeherrschung zu ergriffen. Wenn das Ausmaß des Risikos die definierten Kriterien für Risiken überschreitet, müssen Risikominderungsmaßnahmen vorgenommen werden. Andernfalls ist eine Begründung der Geschäftsführung oder des Risikomanagement-Teams für die weitere Akzeptanz des Risikos erforderlich. (Wolfgang & Ehrenbaum, 2011)

3.9 Risikobewältigung

Nach Abschluss der Risikoanalyse erfolgt die Risikobewältigung, welche darauf abzielt, angemessene Maßnahmen zur Bewältigung des Risikos zu entwickeln. Hierbei werden die Maßnahmen in Risikovermeidung, Risikoreduzierung, Risikotransfer und schließlich

Risikoakzeptanz unterteilt. Hierbei ist es erforderlich, die ermittelten Risiken bezüglich ihrer Wahrscheinlichkeit des Eintretens zu bewerten und das erwartete Ausmaß des Schadens abzuschätzen. Im Rahmen der Risikobewältigung sind die Analyseergebnisse der Ausgangspunkt für die Festlegung der Strategien, die zur Bewältigung der Risiken eingesetzt werden sollen. (DKG, 2011)

1. **Risikovermeidung**

Die primäre Strategie zur Verringerung von Risiken besteht darin, geeignete Maßnahmen zu ergreifen, um die Wahrscheinlichkeit des Auftretens eines Risikos nahezu auf null zu reduzieren. Hierzu gehört die Einhaltung gesetzlicher Vorgaben und die Umsetzung von festgelegten Richtlinien. Dies kann beispielsweise durch den Verzicht auf Tätigkeiten oder Bauteile erfolgen, die mit einem hohen Risiko verbunden sind. (DKG, 2011)

2. **Risikoreduzierung**

Die zweite Strategie zur Risikobewältigung ist die Reduzierung von Risiken, bei der aktiv das Risiko angegangen wird. Hierbei handelt es sich um Risiken, die weder akzeptabel noch transferierbar sind und deren Schadensausmaß und Eintrittswahrscheinlichkeit kein Vermeiden rechtfertigen. Eine Möglichkeit, das Risiko zu mindern, besteht im Einsatz von Netzwerkredundanz oder Backup-Systemen für kritische Anlagen und Ressourcen, um eine Diversifizierung zu erreichen. (DKG, 2011)

3. **Risikotransfer**

Eine weitere Strategie besteht in der Übertragung des Risikos auf eine andere Organisation. Diese Methode wird in der Regel bei Risiken eingesetzt, die einen beträchtlichen Schaden verursachen können, aber eine vergleichsweise geringe Eintrittswahrscheinlichkeit haben. Eine häufige Vorgehensweise hierfür besteht darin, Vermögensschäden auf Versicherungsgesellschaften zu übertragen. (DKG, 2011)

4. **Risikoakzeptanz**

Die vierte Strategie ist die Akzeptanz der Risiken, bei der das Risiko bewusst in Betracht gezogen wird. Es verbleiben immer gewisse Restrisiken, deren Eintrittswahrscheinlichkeit und/oder Schadensausmaß verhältnismäßig gering sind. Für diese Risiken kann auf eine Kontrollmaßnahme verzichtet werden, gemäß den Richtlinien des Risikomanagements durch die verantwortliche Organisation. (DKG, 2011)

3.10 Risikoüberwachung

Um das Risikomanagement effektiv umzusetzen, ist es erforderlich, die ermittelten Risiken zyklisch erneut zu beurteilen und auf das Vorhandensein neuer Risiken zu überprüfen, die sich aus dem täglichen Betriebsablauf und sich wandelnden Bedingungen oder Prozessabläufen ableiten lassen. Dazu gehört auch die Beurteilung der Effektivität der ergriffenen Schutzmaßnahmen. Es ist wichtig, die Risiken und Maßnahmen angemessen zu dokumentieren und diese Dokumentation in periodischen Abständen zu überprüfen. Zur dauerhaften Überwachung und gegebenenfalls Neubeurteilung der identifizierten Risiken sollte der Risikomanager für medizinische IT-Netze geeignete Verfahren einführen. (DKG, 2011)

3.11 Risikomanagement-Akte

Die Risikomanagement-Akte fungiert als zentraler Speicherort aller Dokumente und Nachweise, die im Verlauf des Risikomanagementverfahrens erstellt oder verwendet werden. (DKG, 2011) Angestrebt wird, für jede identifizierte Schwachstelle einen Maßnahmenkatalog zu definieren, der dazu dient, einem Schadensereignis vorzubeugen, es zu vermeiden oder sein Ausmaß zu reduzieren. Abschließend ist eine Dokumentation erforderlich, aus der hervorgeht, ob das verbleibende Restrisiko unter den gegebenen Bedingungen und nach Durchführung der getroffenen Schutzmaßnahmen akzeptabel ist. Durch das Führen einer Risikomanagement-Akte kann verifiziert werden, ob eine Einrichtung die Anforderungen der IEC 80001-1 erfüllt und gegebenenfalls eine Zertifizierung erhalten kann. (Ahlbrandt, et al., 2013)

4 Praktische Ausführung der DIN EN 80001-1:2011

4.1 Hintergrund

In diesem Abschnitt erfolgt eine Durchführung der Risikoanalyse und -bewertung, welche auf den zuvor im Kapitel 3.1 detailliert beschriebenen Schutzzielen basiert.

Abbildung 4: Raumplan AKK- Intensivstation und IMC (AKK, 2023)

Intensivstation: Blau**; IMC:** Blau; **Geräteraum:** Gelb

Die vorliegende Abbildung 4 veranschaulicht den Raumplan der Intensivstation im AKK. Die linke Seite des Plans umfasst die gesamte Intensivstation, wobei die blau markierten Räume für die Verwendung von Sonografie-Geräten vorgesehen sind. Im gelb markierten Raum befinden sich sämtliche medizinische Geräte, die auf der Station benötigt werden. Die Intensivstation ist mit der Intermediate Care (IMC)-Station verbunden, wobei beide Stationen auf die Nutzung der Geräte aus dem Geräteraum zugreifen können.

4.1.1 Vorbereitung

Die Industriepartnerschaft zwischen dem Alfried Krupp Krankenhaus und GE HealthCare wird abgeschlossen, um den Altbestand an Sonografie-Geräten im gesamten Krankenhaus zu erneuern. Zunächst wurde eine Liste aller in Betrieb befindlichen Ultraschallgeräte erstellt, die

Informationen zu Fachbereich, Standort und Baujahr enthielt. Die Leitung der Medizintechnik übernimmt nach Absprache mit der Geschäftsführung den Auftrag zur Ersatzbeschaffung der Geräte. Alle Ärzte, die Ultraschallgeräte verwenden, wurden in zahlreichen Einzelinterviews gebeten, ihre Präferenzen hinsichtlich der Modelle und Sonden zu äußern. (siehe Abbildung 5) Im Rahmen einer koordinierten Zusammenarbeit zwischen der IT-Abteilung und anderen relevanten Akteuren werden die sicherheitstechnischen Anforderungen an die Geräte ermittelt und in den Beschaffungsprozess eingebunden. (AKK, 2023)

Einige der betroffenen Abteilungen sind Radiologie, Intensivmedizin, Hals-Nasen-Ohren-Abteilung, Neurologie und Innere Medizin. Nach Absprache mit dem Unternehmen wurden feste Termine für die Lieferung und Erstinbetriebnahme der Geräte vereinbart. Die Dokumentation der gelieferten Geräte obliegt einem internen Medizintechniker, der diese in das Inventar aufnimmt. Alle relevanten Informationen, die vom Hersteller zur Verfügung gestellt werden, werden in der Akte des jeweiligen Gerätes erfasst und separat digitalisiert. (AKK, 2023)

Die zu untersuchenden Ultraschallgeräte werden mittels einer Silex-Box angeschlossen, welche die Funktion besitzt, ein kabelgebundenes LAN-Gerät in ein WLAN-kompatibles Gerät umzuwandeln. (siehe Abbildung 6) (Silex Technologie, 2023) Da jedem Gerät eine individuelle Silex-Box zugewiesen wird, werden auch die entsprechenden Informationen in die Akte integriert. Zusätzlich werden alle Geräte mit eindeutigen Identifikationsnummern versehen. Vor der Nutzung müssen die Geräte mit Hilfe der Silex-Box an das hauseigene Medizintechnik Netzwerk angebunden werden. Die Box wird anhand der MAC-Adressen der Ultraschallgeräte ins Netz integriert. Da sie nicht standortgebunden genutzt werden sollen, ist eine Verbindung über LAN-Kabel nicht erforderlich. Dadurch können sie an das interne PACS angeschlossen werden und Untersuchungen über den Client durchgeführt werden. Nach einer Inspektion des Geräts durch einen Mitarbeiter von GE wurden die gewünschten Betriebseinstellungen der Ärzte eingestellt und das Gerät zur Untersuchung freigegeben. Im Jahr 2023 wurden schon acht Geräte ausgetauscht. (AKK, 2023)

Abbildung 5: Anbindung Sonografie-Gerät mit Silex-Box (AKK, 2023)

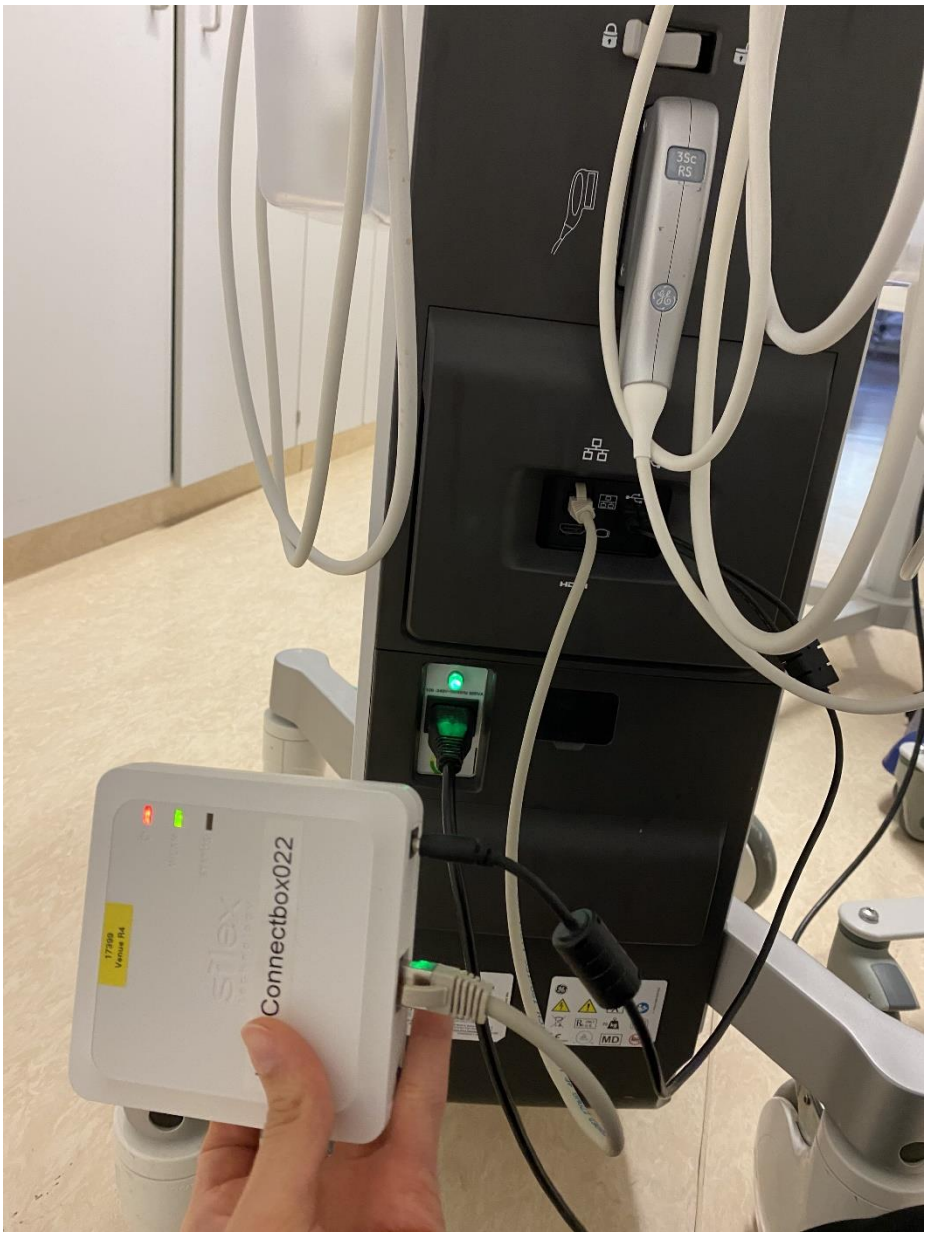

Abbildung 6: Sonden (AKK, 2023)

Auf der Grundlage der Sonografie-Geräte können nun die ersten Schritte zur Erfüllung der Norm EN 80001-1 unternommen werden. Im Rahmen dieser Arbeit wird eine umfassende Risikoanalyse des Workflows der mit Ultraschalltechnik aufgenommenen Bilddateien durchgeführt, um potenzielle Gefährdungen und Ursachen zu identifizieren. Basierend auf den Ergebnissen werden entsprechende Maßnahmen empfohlen. Die primäre Fokussierung liegt auf der Intensivstation, wo die ersten Schritte zur Umsetzung des Risikomanagements unternommen werden. Dies beinhaltet insbesondere die Erstellung eines Risikomanagement-Plans sowie die Durchführung einer Risikoanalyse.

Beschreibung des zu analysierenden Netzwerkes

Das Krankenhausnetzwerk basiert auf Ethernet und erstreckt sich über das komplette Krankenhaus. Es unterstützt Übertragungsraten von 100 MB/s und 1 GB/s. Zur automatischen IP-Konfiguration steht ein DHCP-Server zur Verfügung. Das Ultraschallgerät wird als portables medizinisches Gerät verwendet und regelmäßig zwischen verschiedenen klinischen Abteilungen innerhalb des gesamten Krankenhauses transportiert. Durch die Implementierung der VLAN-Technologie werden separate Netzwerkabschnitte erstellt, um gesicherte Netzwerke zu etablieren. Dies ermöglicht beispielsweise die Isolierung der medizinischen Netzwerke von administrativen Netzwerken. (DKG, 2011)

Die Abbildung 7 veranschaulicht einen Ausschnitt der Stern-Topologie, die im Alfried Krupp Krankenhaus verwendet wird. In der Mitte befindet sich eine Netzwerk-Komponente (Switch oder Hub), die physisch mit allen Hosts verbunden ist. Diese Komponente sorgt für die Verteilung der Datenpakete. Sie empfängt die Pakete und leitet sie an ihre Zieladresse weiter. (Schnabel Patrick, 2023)

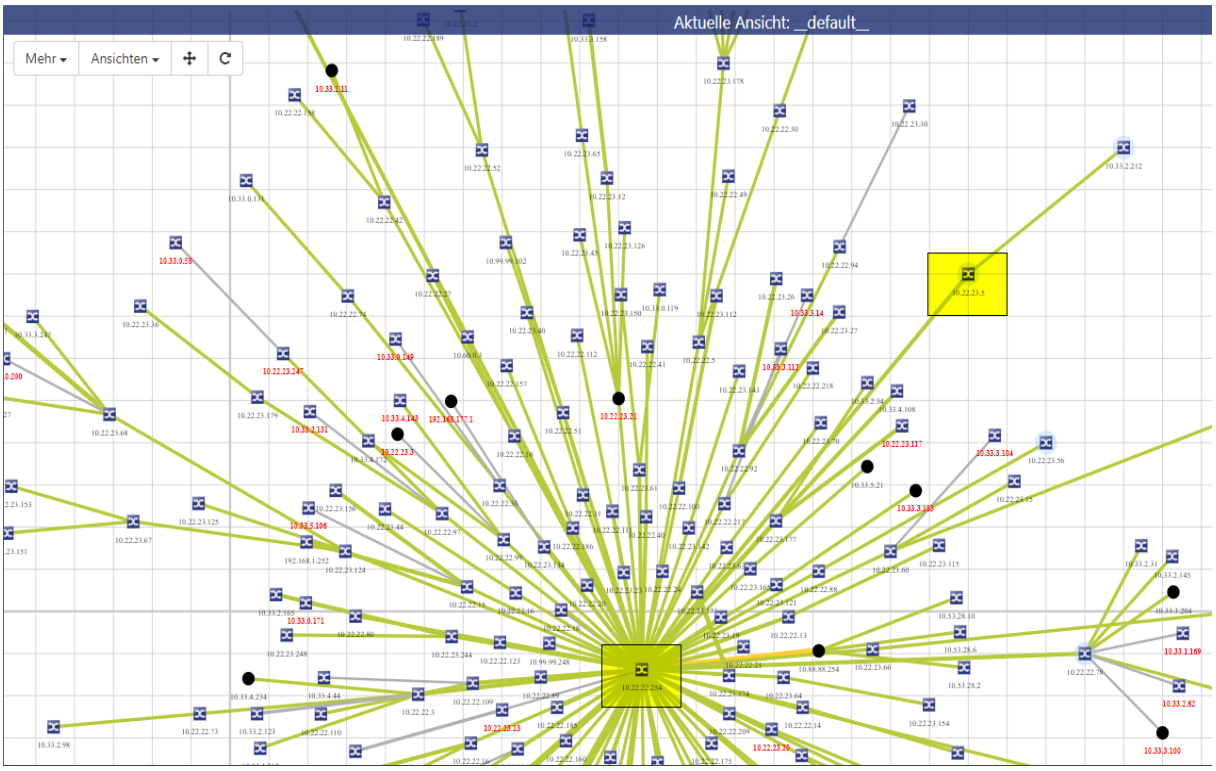

Abbildung 7: Netzwerktopologie AKK (AKK, 2023)

Beispiel anhand der Intensivstation:

Die Intensivstation ist durch einen gelben Kasten in der oberen rechten Ecke markiert.

Abbildung 8: Datentransfer am Beispiel der Intensivstation (AKK, 2023)

Die Netzwerkverbindung ermöglicht den Transfer von Daten von dem Switch zur Intensivstation und zu den Clients. Durch diese Verbindung können wichtige Informationen in Echtzeit ausgetauscht werden. Zusätzlich ist der Drucker mit dem Switch verbunden, sodass relevante Dokumente und Berichte direkt von den Clients aus gedruckt werden können. Die SS-Points stellen eine drahtlose Verbindung zum WLAN her, was die Mobilität der Mitarbeiter erhöht. Dadurch haben Sie die Möglichkeit, während Sie sich frei in der Einrichtung bewegen, auf wichtige Daten und Informationen zuzugreifen. Schließlich wird die Netzwerkverbindung genutzt, um die Daten vom WLAN auf das Ultraschallgerät zu übertragen. Dies ermöglicht es den Ärzten, Ultraschallbilder in Echtzeit zu betrachten und sofortige Diagnosen zu stellen. (AKK, 2023)

4.2 Risikomanagement-Akte

In diesem Abschnitt werden sämtliche Dokumente, die für die Durchführung einer Risikoanalyse erforderlich sind, zusammengetragen und schriftlich festgehalten. Zuerst wird der klinische Arbeitsablauf nähert erläutert. Anschließend werden alle relevanten Informationen zur Genauigkeit der Netzwerkstruktur sowie eine detaillierte Beschreibung des Serverraums. Abschließend wird eine exemplarische Darstellung des Daten-Workflows auf einer Intensivstation präsentiert.

4.2.1 Klinischer Arbeitsablauf

Das Sonografie-Gerät wird rund um die Uhr auf der Intensivstation eingesetzt. Abhängig vom Schichtwechsel arbeiten sechs bis neun Ärzte auf der Intensivstation und führen Ultraschalluntersuchungen durch. Die Untersuchung wird grundsätzlich am Patienten in Rückenlage durchgeführt. Acht Ultraschallgeräte des Herstellers GE HealthCare mit einer diversifizierten Auswahl an Schallköpfen für eine breite Palette von Untersuchungsgebieten stehen auf der Station zur Verfügung. (AKK, 2023)

Wie bereits im vorangegangenen Kapitel 4.1.1 beschrieben, werden alle Ultraschallgeräte mit LAN-Anbindung in mobile Geräte umgerüstet. Durch die Implementierung dieser Strategie wird es möglich, die Geräte nicht nur auf der Intensivstation, sondern auch auf der Intermediate Care (IMC) einzusetzen, welche eine direkte Verbindung zur Intensiv aufweist. Die erfassten

Bildaufnahmen werden zunächst auf der internen Festplatte zwischengespeichert und in bestimmten Zeitabständen automatisch gelöscht. Aufgrund der bestehenden Netzwerkverbindung über die Silex-Box werden die Daten direkt an das PACS übertragen und langfristig archiviert. Alle erfassten Ultraschallbefunde werden an das PACS übermittelt und in der elektronischen Patientenakte im KIS gespeichert, wodurch sie den medizinischen Fachkräften zur Verfügung stehen. Im Falle von Netzwerkproblemen ist es erforderlich, dass alle patientenspezifischen Daten erneut auf dem Gerät erstellt werden. Dies verzögert den Arbeitsablauf auf der Station. (AKK, 2023)

4.2.2 Netzwerkstruktur im AKK

Das IT-Netzwerk des Alfried Krupp Krankenhauses in Rüttenscheid wurde durch die Implementierung von Virtuellen-LANs (VLANs) in verschiedene Bereiche segmentiert, um eine logische Separierung zwischen dem medizinischen IT-Netzwerk vom Restnetzwerk zu gewährleisten. Das eingesetzte Transportprotokoll ist TCP/IP (Transmission Control Protocol/Internet Protocol), Version IPv4. Die in Verbindung genutzten IP-Adressen umfassen die Bereiche unter anderem das Medizintechnik-Netzwerk 10.99.116.0 und den Terminalserver 10.23.0.0. Das Netzwerk des Krankenhauses ist durch Firewalls physisch getrennt. (AKK, 2023)

Diese fungieren als Sicherheitsvorkehrungen, um unerlaubte und unbefugte Verbindungsversuche aus dem öffentlichen Internet in das lokale Netzwerk abzuwehren. Zusätzlich wird ein Proxy-Server eingesetzt, der als Speicher dient und den Zugriff auf häufig angeforderte Datensätze und Dateien aus dem Arbeitsspeicher ermöglicht. (Schnabel Patrick, 2023)

4.2.3 Physikalische Struktur Serverraum

Die physische Netzwerkstruktur ist folgendermaßen aufgebaut: Der Zugang zum Rechenzentrum erfolgt über eine Tür, die mit einem Zugangscode gesichert ist. Im Vorraum befinden sich eine unterbrechungsfreie Stromversorgung (USV), die verwendet wird, um die Funktionalität des Netzwerks auch bei einem Stromausfall aufrechtzuerhalten, sowie weitere Netzwerkschränke. Der Serverraum ist durch Hochgeschwindigkeitsleitungen in einer Sterntopologie miteinander verbunden. Ein spezieller Schlüssel wird benötigt, um die dicke Stahltür zu öffnen, die den eigentlichen Serverraum abschirmt. Innerhalb dieses Raums befinden sich Hypervisor-Server, Datenbanken, Festplatten und Speicherserver, die einen störungsfreien Betrieb der IT-Infrastruktur gewährleisten. Das Rechenzentrum folgt einem Kalt-/Warmgangkonzept, das als Planungsstandard gilt. (AKK, 2023)

Die Netzwerkschränke werden so platziert, dass ihre Fronten zueinander zeigen und kalte Luft über den Doppelboden in den Raum geleitet wird, der als Kaltluftraum dient. In der Norm ANSI/TIA/EIA-942-A (Rechenzentren) wird ein Kaltgang mit einer Breite von 1,2 m (entspricht zwei Bodenplatten) vorgeschrieben, sodass vor jedem Schrank eine perforierte Bodenplatte zur Führung der Kaltluft an die Vorderseite des Schrankes angebracht werden kann. Die Schränke stehen mit den Fronten zueinander und die Kaltluftzufuhr erfolgt über den Doppelboden. Aufgrund der Kaltluftzufuhr über den Doppelboden ist es notwendig, dass alle Bodenöffnungen, wie z. B. Kabeldurchführungen, sorgfältig mit Doppelbürstenplatten abgedichtet werden, um den statischen Druck im Boden konstant zu halten und das Risiko eines ungeordneten Luftaustritts aus dem Boden zu reduzieren. (Conteg, 2023)

In allen Netzen befinden sich Verteiler, um die notwendige Portanzahl für die angeschlossenen Geräte zur Verfügung zu stellen. Insgesamt besteht das Krankenhausnetzwerk aus ungefähr 400 Netzwerkkomponenten und 2000 netzwerknutzenden Komponenten wie Server oder Clients. Die verwendeten Netzwerkkomponenten, darunter Switches und Router, werden von Unternehmen wie HP und Arobar bereitgestellt. Diese Komponenten sind mit einer nicht blockierenden Weiterleitungs- bzw. Vermittlungsarchitektur ausgestattet, um einen sicheren Datenverkehr zu gewährleisten. Die vorgeschalteten Module sind für 1 Gigabit Ethernet und die Clients für 100 MBit konfiguriert. Zur Überbrückung längerer Hausstrecken zwischen den Schaltern (Switches) werden grundsätzlich Lichtwellenleiter eingesetzt. Der Anschluss der Clients an die Switches erfolgt über Kupferkabeln. Jeder Port bietet 1-Gigabit-Ethernet. (AKK, 2023)

Zudem wird ein Container als Backup-Rechenzentrum eingesetzt. Das Tape-Backup, auch als Bandsicherung bezeichnet, beinhaltet das periodische Kopieren von Daten von einem Primärspeichergerät auf eine Bandkassette, um die Wiederherstellung von Daten zu ermöglichen, falls eine Festplatte abstürzt oder ausfällt. Die Datensicherung auf Datenträger kann entweder händisch erfolgen oder durch geeignete Software einprogrammiert werden. (Crocetti, 2023)

4.2.4 Workflow Datenfluss

Der Arbeitsablauf auf einer Intensivstation mit einem Ultraschallgerät umfasst den Informations- und Datenfluss zwischen verschiedenen Systemen und Anwendungen. Im Folgenden wird ein typischer Workflow beschrieben:

Mit der Aufnahme des Patienten und der Eingabe seiner relevanten Informationen in das Krankenhausinformationssystem (KIS) beginnt der Informations- und Datenaustausch

zwischen den Systemen der Intensivstation. Diese Informationen umfassen sowohl administrative als auch klinische Daten des Patienten. Eine Ultraschallanforderung wird über das KIS durch den behandelnden Arzt oder qualifiziertes medizinisches Personal eingeleitet. Die Anforderung wird mittels des HL7 - Protokolls an das Ultraschallgerät übertragen. (AKK, 2023)

Der Mediziner führt eine Echographie des Patienten durch und generiert Echtzeitbilder und -videos, die auf dem Sonographie-Gerät dargestellt werden. Das Ultraschallsystem kann die generierten Bild- und Videodaten entweder intern speichern oder über das DICOM-Protokoll an ein PAC-System übertragen. DICOM definiert das medizinische Bildformat und ermöglicht den interoperablen Austausch zwischen verschiedenen Bildgebungssystemen. So kann das medizinische Personal die Aufnahmen mit den dazugehörigen Patienteninformationen verifizieren. Befunde werden von Radiologen oder anderen Fachärzten erstellt und können im KIS den behandelnden Ärzten zur Verfügung gestellt werden. (AKK, 2023)

Das Intensivpflegepersonal kann über das KIS auf die Befunde zugreifen. Die Befunde lassen sich in die elektronische Patientenakte (EPA) einpflegen. Dies erleichtert die Kontrolle und die Einbindung in die Entscheidungsprozesse. Um den Workflow im PACS zu steuern, wird die DICOM-Worklist verwendet. Um sicherzustellen, dass die richtigen Untersuchungen durchgeführt werden, enthält sie Informationen wie Patientenangaben, Art der Untersuchung und Dringlichkeit. (AKK, 2023)

Abbildung 9: Workflow Datenfluss Eigene Darstellung nach Anlehnung (AKK, 2023) (Piktogramme (STARC medical, 2023) (Vecteezy, 2023))

4.3 Risikoanalyse: Sonografie-Gerät

In diesem Abschnitt werden außer den genannten drei Schutzzielen (Patientensicherheit, Daten- und Systemsicherheit, Effektivität) der Norm 80001-1 zusätzlich die Schutzziele der Informationssicherheit (Verfügbarkeit, Vertraulichkeit, Integrität) behandelt. Hierzu wird der Gefährdungskatalog der BSI zur Hilfe genutzt. (DKG, 2011)

Die Risikoanalyse beginnt am Sonografie-Gerät und erstreckt sich bis zum PAC-System, wie in Abbildung 8 veranschaulicht. Dabei werden die Schnittstellen der Netzwerkpunkte betrachtet und auf mögliche Gefährdungen analysiert. Anschließend werden für jede identifizierte Gefährdung entsprechende Maßnahmen betrachtet.

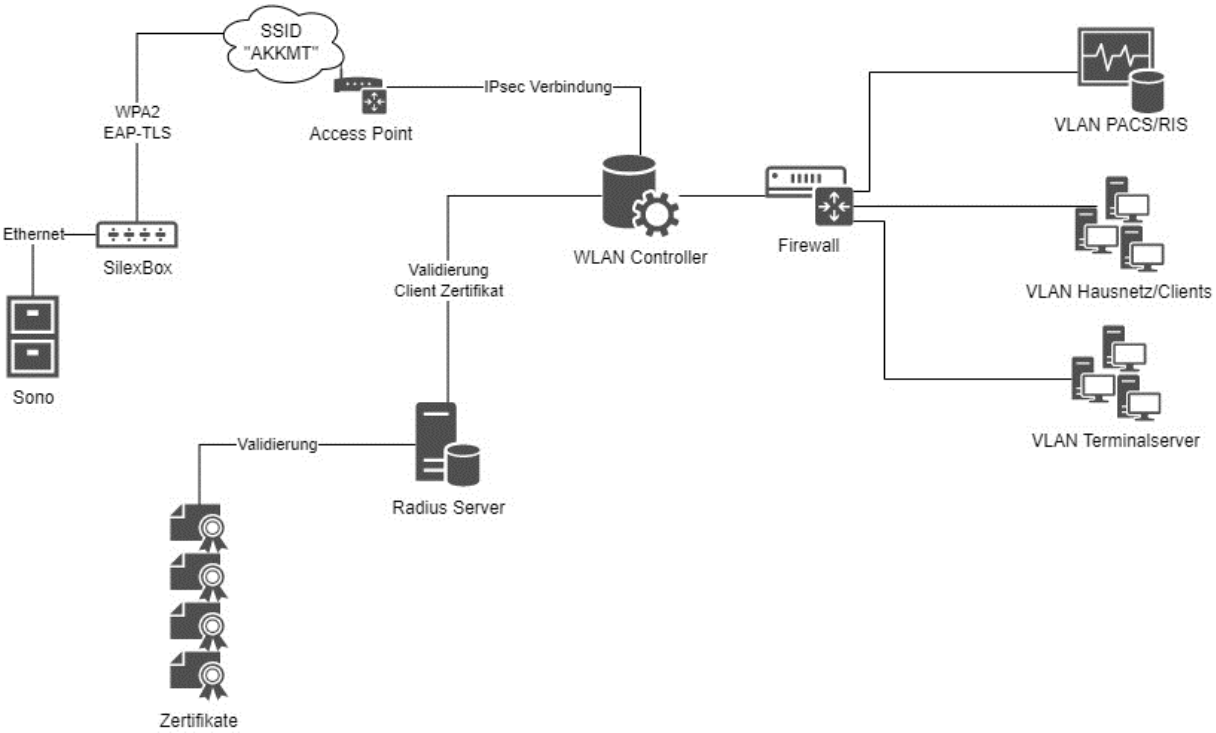

Abbildung 10: Workflow Datenübertragung (AKK, 2023)

<u>Übertragung:</u>

Nachdem die Silex-Box an das Gerät angeschlossen wird, nutzt sie spezifische Zertifikate, um über das EAP-TLS-Protokoll zu kommunizieren. Das EAP-Protokoll (Extensible Authentication Protocol) wird in lokalen Netzwerken mit IEEE 802.1x/RADIUS zur Durchführung von Authentifizierungsverfahren eingesetzt. Die primäre Funktion von EAP besteht darin, sicherzustellen, dass der Zugriff auf ein Netzwerk erst nach einer erfolgreichen Authentifizierung gestattet wird. (Schnabel Patrick, 2023)

Das Zertifikat wird zur Authentifizierung beim WLAN-Controller verwendet. Der WLAN-Controller akzeptiert nur Verbindungen von Zertifikaten, die über den Radius-Server authentifiziert wurden. Die Silex-Box nutzt WLAN und Clientzertifikate, um eine kabellose Verbindung zum WLAN-Controller herzustellen. Hierbei erfolgt eine Identitätsüberprüfung der Silex-Box mittels des Clientzertifikats, um eine sichere Kommunikation mit dem Controller zu gewährleisten. Allgemein: Der Nutzer interveniert hauptsächlich mit der Registrierungsstelle (RA), die die Zertifizierungsanträge untersucht, erfasst und an die Zertifizierungsstelle (CA)

zur Zertifizierung weitersendet. Das Zertifikat wird dem Anwender durch die RAs ausgestellt und parallel dazu über den Verzeichnisdienst veröffentlicht. Die Sperrung kann entweder vom Nutzer oder von der RA veranlasst werden und wird dann von der CA durch eine Signatur beglaubigt, überprüfbar gemacht und über den Verzeichnisdienst veröffentlicht. (Bless, et al., 2005)

Die Kommunikation zwischen dem Controller und der Box erfolgt im Rahmen des EAP-TLS-Protokolls. Innerhalb der Box befindet sich der Schlüssel des Zertifikats, der eine Anfrage an den Controller sendet. Nachfolgend sendet der Controller einen zufälligen Zahlencode an die Silex-Box, der von dieser mit dem passenden Schlüssel verschlüsselt wird, sofern das Zertifikat übereinstimmt. Die Box kann mithilfe ihres öffentlichen Schlüssels überprüfen, ob die durchgeführte Verschlüsselung gültig ist. Der WLAN-Controller fungiert als Gateway, das als aktiver Netzwerkknoten agiert und somit der Silex-Box ermöglicht, eine Verbindung zum WLAN herzustellen. (AKK, 2023)

Die Kommunikation zwischen dem Controller und der Silex-Box erfolgt mittels kryptografischer Verschlüsselung. Anschließend wird das System durch eine Firewall erweitert, die als Schutzmechanismus gegen unautorisierte Zugriffe vom öffentlichen Internet auf das lokale Netzwerk eingesetzt wird. Die Firewall implementiert einen Paketfilter auf der Grundlage des TCP/IP-Protokolls, der die Quell- und Ziel-IP-Adressen sowie die zugehörigen Portnummern (TCP) überprüft. (Schnabel Patrick, 2023)

Die Firewall im Krankenhaus implementiert eine Filterung, die auf VLANs basiert. Die Silex Box wird einem spezifischen VLAN zugewiesen, das von der Firewall als erlaubtes VLAN identifiziert wird. Die genehmigten Inhalte werden schließlich an das PACS/Radiology Information System (RIS), das Hausnetzwerk/Clients und den Terminalserver weitergeleitet. (AKK, 2023)

Potenzielle Gefährdungen nach BSI-Gefährdungskatalog:

Als Grundlage für die Analyse wurde der Gefährdungskatalog des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verwendet. Zur Veranschaulichung der grundsätzlichen Vorgehensweise wurde die Risikoanalyse anhand exemplarisch ausgewählter Gefährdungen dargestellt. Die für die Verfügbarkeit relevanten Risiken sind in Abbildung 8 gelb markiert. Die grünen Markierungen beschreiben die Risiken, die für die Integrität und Vertraulichkeit der Daten entscheidend sind. (siehe Abbildung 11)

	Gefährdung	Grundwert
G 0.1	Feuer	A
G 0.2	Ungünstige klimatische Bedingungen	I, A
G 0.3	Wasser	I, A
G 0.4	Verschmutzung, Staub, Korrosion	I, A
G 0.5	Naturkatastrophen	A
G 0.6	Katastrophen im Umfeld	A
G 0.7	Großereignisse im Umfeld	C, I, A
G 0.8	Ausfall oder Störung der Stromversorgung	I, A
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	I, A
G 0.10	Ausfall oder Störung von Versorgungsnetzen	A
G 0.11	Ausfall oder Störung von Dienstleistern	C, I, A
G 0.12	Elektromagnetische Störstrahlung	I, A
G 0.13	Abfangen kompromittierender Strahlung	C
G 0.14	Ausspähen von Informationen/Spionage	C
G 0.15	Abhören	C
G 0.16	Diebstahl von Geräten, Datenträgern und Dokumenten	C, A
G 0.17	Verlust von Geräten, Datenträgern und Dokumenten	C, A
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A
G 0.19	Offenlegung schützenswerter Informationen	C
G 0.20	Informationen aus unzuverlässiger Quelle	C, I, A
G 0.21	Manipulation von Hard- und Software	C, I, A
G 0.22	Manipulation von Informationen	I
G 0.23	Unbefugtes Eindringen in IT-Systeme	C, I
G 0.24	Zerstörung von Geräten oder Datenträgern	A
G 0.25	Ausfall von Geräten oder Systemen	A
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A
G 0.27	Ressourcenmangel	A
G 0.28	Softwareschwachstellen oder -fehler	C, I, A
G 0.29	Verstoß gegen Gesetze oder Regelungen	C, I, A
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	C, I, A
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C, I, A
G 0.32	Missbrauch von Berechtigungen	C, I, A
G 0.33	Personalausfall	A
G 0.34	Anschlag	C, I, A
G 0.35	Nötigung, Erpressung oder Korruption	C, I, A
G 0.36	Identitätsdiebstahl	C, I, A
G 0.37	Abstreiten von Handlungen	C, I
G 0.38	Missbrauch personenbezogener Daten	C
G 0.39	Schadprogramme	C, I, A
G 0.40	Verhinderung von Diensten (Denial of Service)	A
G 0.41	Sabotage	A
G 0.42	Social Engineering	C, I
G 0.43	Einspielen von Nachrichten	C, I
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I, A
G 0.45	Datenverlust	A
G 0.46	Integritätsverlust schützenswerter Informationen	I
G 0.47	Schädliche Seiteneffekte IT-gestützter Angriffe	C, I, A

Abbildung 11: BSI-Gefährdungskatalog 200-3 (BSI, 2023)

Relevante Informationen:

Es wurden die relevanten Informationen, die für die Durchführung dieser Analyse von Bedeutung sind, in einer Liste aufgeführt. Diese Informationen beziehen sich auf das untersuchte Ultraschallgerät.

Standort (AKK, 2023):

Intensivstation; Sonografie-Gerät

Clinic PC (AKK, 2023):

Hardware: Monitor, Tastatur, Maus, Desktop-PC

Software: Windows 10, über Citrix wird das Krankenhausinformationssystem IS-M Med, Virenscanner ESET; Deadalus Deep Unity (PACS); Clinic Windata

Medizingerät (AKK, 2023):

Sonografie-Gerät Venue R4 von GE HealthCare

Abkürzungen:

G: Gefährdung

U: Potenzielle Ursachen

GS: Gefährdungssituation

FO: Folgen

RB: Risikobeherrschung

ST: Schnittstelle

Anwender Risikoanalyse:

Das Sonografie-Gerät auf der Intensivstation des Krankenhauses wird drahtlos über WLAN anhand der Silex-Box verbunden und kann mobil auf der Station bedient werden. Das Gerät befindet sich im Geräteraum und wird über ein Netzwerkkabel mit einer Netzwerkdose verbunden.

Schritt 1: Identifikation der Gefährdungen

G1: Datenschutzverletzung (Patienten- oder Organisationsinformation) (AKK, 2023)

G2: Funktionseinschränkung (Ausfall der Systemfunktion) (AKK, 2023)

G3: Verbindungsverlust (Der Zugriff auf die Daten, die von den Systemfunktionen benötigt werden, ist entweder eingeschränkt oder der Zugriff wird verweigert) (AKK, 2023)

G4: Gefährdung durch Reinigungs- oder Fremdpersonal (BSI, 2023)

G5: Fehlerhafte Administration von Zugangs- und Zugriffsrechten (Isselhorst, Dr. Hartmut, 2016)

G6: Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten (Isselhorst, Dr. Hartmut, 2016)

Schritt 2: Ermittlung der Ursachen und Gefährdungssituationen

Potenzielle Ursachen:

U1: Durch die Übertragung von Schadsoftware über USB-Sticks kann es zu einer Infektion der Modalität kommen. Diese Schadsoftware ist darauf programmiert, gezielt nach persönlichen Daten zu suchen, die zur Identifikation von Patienten verwendet werden könnten, wie beispielsweise Versichertennummern oder Geburtsdaten. Sobald diese Daten gefunden werden, exportiert die Schadsoftware sie aus dem System und ermöglicht somit einen unerwünschten Informationsabfluss. (DKG, 2011)

U2: Bei der Übertragung und Installation von Malware und anderen Programmen auf der Modalität wird die Systemleistung in signifikanter Weise beeinträchtigt. Dies führt dazu, dass

Hardwareressourcen für andere Funktionen verwendet werden, wie z. B. Angriffe auf Kennwörter, Scannen oder Überlasten des Netzwerks und Peer-to-Peer-Aktivitäten (DKG, 2011).

U3: Es besteht die Möglichkeit, dass aufgrund einer fehlerhaften Konfiguration die HL7-Schnittstelle nicht ordnungsgemäß am Sonografie-Gerät eingerichtet wird, was zu einem Ausbleiben des Datenaustauschs führt. (AKK, 2023)

U4: Durch das Reinigungspersonal besteht die Möglichkeit, dass versehentlich eine Steckverbindung gelöst wird. Infolgedessen kann Wasser in die Geräte eindringen, was zu einem Verlust der Systemfunktionen führen kann. (BSI, 2023)

U5: Durch eine mangelhafte Administration der Zugriffsrechte besteht das Risiko, dass befugtes Fachpersonal auf Protokolldaten zugreifen kann. Durch gezieltes Entfernen spezifischer Einträge kann diese Person ihre Manipulationsversuche am Gerät verbergen, da diese nicht mehr in der Protokolldatei ersichtlich sind. (BSI, 2023)

U6: Bei der Demontage, der Ausleihe, der Einsendung zur Reparatur oder der Ausmusterung von Laufwerken besteht die Gefahr, dass Daten auf teilweise noch unversehrten Dateisystemen in unautorisierte Hände geraten, sofern sie nicht zuvor unwiderruflich gelöscht wurden. (BSI, 2023)

Potenzielle Gefährdungssituationen:

GS1: Datensicherheit

Bei einem Tastatur- oder USB-Keylogger handelt es sich um ein kompaktes Gerät, das zwischen die Tastatur und den Computer angeschlossen wird. Der Logger protokolliert alle Tastaturbefehle, einschließlich medizinischer Befunde, Benutzer-IDs und Passwörter. Der Keylogger wird programmiert, dass er seine Aufzeichnungen regelmäßig und automatisch über WLAN überträgt. Das unbefugte Durchführen solcher Aktivitäten ist illegal, und Angreifer übertragen die Daten oft ins Ausland, um ihre Identität zu verschleiern. Die Verwendung eines solchen Geräts ist nur legal, wenn es zur Erstellung einer zusätzlichen Sicherungskopie für den persönlichen Gebrauch verwendet wird. Im gegenteiligen Fall können USB-Keylogger zu Spionagezwecken missbraucht werden. (Darms, Haßfeld, & Fedtke, 2019)

GS2: Patientensicherheit

Bei einer medizinischen Behandlung, z. B. in der Geburtshilfe, Kardiologie oder Gastroenterologie, kann eine auf dem System installierte Malware die Ressourcen der Hardware in Anspruch nehmen und dadurch die Systemleistung beeinträchtigen. Dadurch kann

die Bilderfassung fehlschlagen oder die Durchführung der Behandlung gestört werden, beispielweise durch Schwierigkeiten bei der präzisen Navigation einer Punktionskanüle während einer Amniozentese. Darüber hinaus besteht die Möglichkeit, dass notwendige Software-Bibliotheken, die für mathematische Funktionen verwendet werden, durch möglicherweise fehlerhafte Bibliotheken ersetzt werden. Daraus ergibt sich ein Risiko für das Versagen der Bildaufnahme oder eine Störung der Behandlung. (DKG, 2011)

GS3: Effektivität

Eine inkorrekte Konfiguration kann zu Beeinträchtigungen der Verbindung zwischen dem Ultraschallgerät und der HL7-Schnittstelle führen. Dies kann dazu führen, dass keine Übertragung von Daten erfolgt oder dass die Verbindung häufig unterbrochen wird. (Darms, Haßfeld, & Fedtke, 2019)

GS4: Vertraulichkeit

Ein nicht autorisierter Besucher erlangt Zugriff auf Dokumente, Speichermedien oder Geräte und verursacht Schäden oder erhält unerlaubten Zugriff auf vertrauliche Informationen. Das Reinigungspersonal löst versehentlich eine Steckverbindung, was zu einem Kabelbruch führen kann. Darüber hinaus gelangt Wasser in das Gerät während des Reinigungsvorgangs, was zu einer Beeinträchtigung der Funktionalität führt. (BSI, 2023)

GS5: Integrität/Effektivität

Ein befugtes Fachpersonal betritt den Geräteraum, in dem sich das Ultraschallgerät befindet, und erlangt Zugriff auf das Gerät, um gezielt bestimmte Daten zu manipulieren. (AKK, 2023)

GS6: Vertraulichkeit

Das Fachpersonal übergibt das Gerät an eine andere Station, ohne angemessen zu überprüfen, ob die zuvor darauf gespeicherten Daten ordnungsgemäß gelöscht wurden. (AKK, 2023)

Schritt 3: Ermittlung sämtlicher nicht beobachteter Folgen und ihres Schweregrads

FO für GS1: Datensicherheit

Die Nichteinhaltung von Datensicherheitsbestimmungen kann zur unbefugten Offenlegung medizinischer Daten einschließlich der Berichterstattung über den Vorfall an die zuständigen Behörden führen. Eine unbefugte Nutzung kann durch die Offenlegung vertraulicher personenbezogener Daten von Patienten gestattet werden (DKG, 2011)

Schweregrad: gering

FO für GS2: Effektivität

Der Behandlungsprozess wird unterbrochen oder verzögert. Ein Lokalisationsfehler der Punktionsnadel ist feststellbar, der zum Abbruch der Behandlung führt (DKG, 2011)

Schweregrad: Moderat

FO für GS3: Patientensicherheit

Der Arzt ist gezwungen, auf manuelle Techniken umzustellen, was die Wirksamkeit des Einsatzes potenziell verringern oder unerwünschte oder inakzeptable Folgen für den Einsatz haben kann (DKG, 2011)

Schweregrad: gering

FO für GS4: Das Reinigungspersonal unterlässt es, der Intensivstation mitzuteilen, dass es infolge einer Verschiebung des Geräts zu einem Kabelbruch gekommen ist. Dadurch ist das Gerät nicht mehr aufladbar und fällt aus. Das Personal informiert den internen Medizintechniker erst dann, wenn das Gerät während eines Einsatzes benötigt wird, da zuvor kein Defekt am Kabel festgestellt wurde. Dies führt zu Verzögerungen bei den Behandlungen. (AKK, 2023)

Schweregrad: gering

FO für GS5: Löschen führt zum Verlust wichtiger Daten.

Schweregrad: Hoch

FO für GS6: Die Vernachlässigung der ordnungsgemäßen Löschung zuvor gespeicherter Daten kann zur Verletzung des Vertrauens der Patienten und des Fachpersonals führen. (BSI, 2023)

Schweregrad: Moderat

Schritt 4: Abschätzung der Wahrscheinlichkeit des Eintritts

Vorhandene Risikobeherrschungsmaßnahmen:

Das Betriebssystem der Sonographie Modalität ist gehärtet (AKK, 2023):

- Kein Webbrowser verfügbar, nur die im Rahmen der Zweckbestimmung notwendigen Dienste sind zugänglich.
- Zugriffssteuerung ist eingerichtet.
- Modalität befindet sich im „AKKMT“-Netzwerk (VLAN)

Für die Nutzung notwendige, geöffnete Netzwerkports/Protokolle:

- Die Ultraschallmodalität ist mit einer Software-Firewall ausgestattet, welche alle Netzwerk-Ports außer Port 104 sperrt, da dieser für die DICOM-Interoperabilität erforderlich ist (DKG, 2011).
- Instandhaltung nach Herstellervorgaben inklusiver Sicherheitstechnischer Kontrolle nach DIN EN ISO 62353 – Anforderungen der MPBetreibV und der DGUV-Vorschrift 3 erfüllt. (GE-Healthcare, 2023).

Auf der Grundlage dieser Maßnahmen wird die Eintrittswahrscheinlichkeit wie folgt beurteilt:

GS1: Fernliegend

GS2: Selten

GS3: Fernliegend

GS4: Fernliegend

GS5: Fernliegend

GS6: Wahrscheinlich

Schritt 5: Bewertung der Gefahren anhand definierter Akzeptanzkriterien

GS1: Fernliegend → Risikolevel = gering

GS2: Selten → Risikolevel = moderat

GS3: Fernliegend → Risikolevel = gering

GS4: Fernliegend → Risikolevel = gering

GS5: Fernliegend → Risikolevel = gering

GS6: Wahrscheinlich → Risikolevel = vernachlässigbar

Schritt 6: Festlegung und Protokollierung der Maßnahmen zur Risikobeherrschung

Bereits auf Netzwerkebene können praktikable Maßnahmen zur Risikobeherrschung umgesetzt werden:

RB1: Verwendung vorbehaltener Adressbereiche (DHCP) für Sonografie-Geräte. Auf diese Weise ist es möglich, den Netzwerkverkehr zu überwachen, um gezielte Warnungen zu generieren (DKG, 2011)

RB2: Firewalls implementieren, um separate Netzwerke (VLANs) vor unerwünschtem Netzwerkverkehr zu bewahren (DKG, 2011)

RB3: Durchführung eines Performance-Tests, um die Leistungsfähigkeit des Systems zu überprüfen. Anschließend Neukonfiguration der HL7-Schnittstelle. (AKK, 2023)

RB4: Regelmäßige Kontrollen des Geräteraums sollten durchgeführt werden, um sicherzustellen, dass sich keine Personen ohne Dienstkleidung im Raum aufhalten. Sollten Geräte beschädigt werden, ist das Reinigungspersonal verpflichtet, die Station oder das Fachpersonal zu benachrichtigen. (AKK, 2023)

RB5: Auswahl eines sicheren Passworts. Unterschiedliche Administratoren mit jeweils unterschiedlichen Passwörtern. (AKK, 2023)

RB6: Selbsteliminierung der Daten. In den Geräteeinstellungen festlegen, dass die Untersuchungen nicht länger als eine Woche/einen Tag (je nach Untersuchungsumfang frei wählbar) im Gerät gespeichert werden. (AKK, 2023)

Die Implementierung der Maßnahmen RB1, RB2, RB3, RB4, RB5 und RB6 verringert die Eintrittswahrscheinlichkeit der Gefährdungssituation. Obwohl die Eintrittswahrscheinlichkeiten bereits gering waren, werden RB1 und RB2 dennoch als bewährte Verfahren angesehen und umgesetzt. Die Umsetzung von RB3 und die Durchführung eines Performance-Tests müssen von der EDV-Abteilung periodisch durchgeführt werden, um weitere Risiken zu vermeiden. (DKG, 2011)

GS1: Risikolevel → gering

GS2: Risikolevel → moderat

GS3: Risikolevel → gering

GS4: Risikolevel → gering

GS5: Risikolevel → gering

GS6: Risikolevel → vernachlässigbar

<u>Schritt 7: Umsetzung der Maßnahmen</u>

Risikobeherrschungsmaßnahmen sind so umzusetzen, dass sie vor der Zulassung und Inbetriebnahme überprüft werden können.

RB1: Verwendung vorbehaltener Adressbereiche (DHCP) für Sonografie-Geräte kann auf einem derzeit nicht verwendeten Gerät umgesetzt und zur Verifizierung verwendet werden (DKG, 2011).

RB2: Die Einrichtung von Firewalls kann in einem kleinen Labornetzwerk oder im Echtbetrieb während eines Zeitraums für Systemänderungen erprobt werden (DKG, 2011).

RB3: Nach der erfolgten Anpassung der Konfiguration kann die HL7-Schnittstelle validiert werden. Dieser Schritt wird in einem geeigneten Zeitfenster durchgeführt, um den reibungslosen Ablauf des Krankenhausbetriebs nicht zu beeinträchtigen. (AKK, 2023)

RB4: Es ist erforderlich, dass das Fachpersonal eine Schulung erhält, um für alle potenziellen Gefährdungen sensibilisiert zu sein, die von unbefugten Personen ausgehen können. (AKK, 2023)

RB5: Vor der Inbetriebnahme des Gerätes sollten sichere Passwörter in Zusammenarbeit mit den behandelnden Ärzten festgelegt werden, wobei darauf geachtet wird, dass diese nicht auf dem Bildschirm beschriftet werden. (AKK, 2023)

RB6: Ein Mitarbeiter von GE konfiguriert die Funktion zur automatischen Löschung von Daten. Die Berechtigungen für diese Einstellungen werden an die Abteilung für Medizintechnik übertragen. (AKK, 2023)

Schritt 8: Überprüfung der Maßnahmen (AKK, 2023)

RB1: Verifikation

Effektivität: Das Gerät gilt als ordnungsgemäß gegen schadhaften Netzwerkverkehr gesichert. Die Wirksamkeit dieser Schutzmaßnahme kann durch eine logische Beweisführung zur Untermauerung der Annahme verifiziert werden.

Implementierung: Die Gewährleistung der korrekten Zuweisung einer geeigneten IP-Adresse und die Überprüfung der Verbindungsfähigkeit können durch eine Simulation in einer Klinikumgebung getestet werden.

RB2: Verifikation

Effektivität: Der Netzwerkverkehr wird durch eine Firewall abgesichert, die unerlaubte Verbindungsversuche aus dem öffentlichen Internet in das lokale Netzwerk blockiert. Dieser Vorgang wird von der hausinternen EDV überwacht. Die Wirksamkeit dieser Schutzmaßnahme kann durch eine logische Beweisführung zur Untermauerung der Annahme verifiziert werden.

Implementierung: Unerwünschten Netzwerkverkehr simulieren und die Blockierung durch die Firewall sicherstellen.

RB4: Verifikation

Effektivität: Das Personal wird geschult und alle Vorgänge werden ordnungsgemäß dokumentiert.

Implementierung: Die EDV-Abteilung konzipiert verschiedene Szenarien zur Bedrohungsanalyse, um die Wirksamkeit der Schulungen zu evaluieren.

RB5: Verifikation

Effektivität: Während der Inbetriebnahme des Geräts bittet ein Mitarbeiter von GE die behandelnden Ärzte, ein Passwort festzulegen, das den Sicherheitsstandards entspricht.

Implementierung: Das sichere Passwort wird jedem Arzt zur Verfügung gestellt, welches nur von ihm genutzt werden darf.

RB6: Verifikation

Effektivität: Die Leitung der Abteilung Medizintechnik hat nach Rücksprache mit den Ärzten die Entscheidung getroffen, dass keine Befunde intern auf dem Gerät gespeichert werden sollen.

Implementierung: Die automatische Löschung wird vom GE-Mitarbeiter konfiguriert.

Schritt 9: Bewertung aller Risiken durch entstehen der Maßnahmen (DKG, 2011)

Es wurde eine umfassende Bewertung aller potenziell neu entstandenen Risiken aufgrund der zuvor ergriffenen Maßnahmen durchgeführt.

Diese Evaluierung ergab, dass als Ergebnis der ergriffenen Maßnahmen zur Risikobeherrschung keine zusätzlichen Risiken identifiziert wurden.

Schritt 10: Bewertung und Berichterstattung des Restrisikos

Die Bewertung des Gesamtrisikos (Restrisiko) erfolgt objektiv durch eine umfassende Evaluation, auf die anschließend Bericht erstattet wird.

Schnittstellen Risikoanalyse (AKK, 2023)**:**

Ziel dieser Analyse ist die Untersuchung der Schnittstellen zwischen den einzelnen Komponenten. Der Prozess beginnt mit dem Sonographie-Gerät, das über eine Ethernet-Verbindung mit der Silex-Box verbunden ist. Als nächstes wird die Verbindung zwischen der Box und dem Access Point analysiert, der mit WPA2 und EAP-TLS gesichert ist. Anschließend wird der Access Point betrachtet, der eine IPsec-Verbindung zum WLAN-Controller aufweist. Die Zertifikate werden zur Validierung an den Radius-Server gesendet, um eine Authentifizierung der Zertifikate durchzuführen. Die validierten Client-Zertifikate werden anschließend an den WLAN-Controller weitergeleitet und verschlüsselt. Im nächsten Schritt wird die Verbindung zwischen dem WLAN-Controller und der Firewall untersucht. Schließlich wird die Firewall mit den einzelnen VLANs (PACS, Hausnetz/Client, Terminalserver) analysiert.

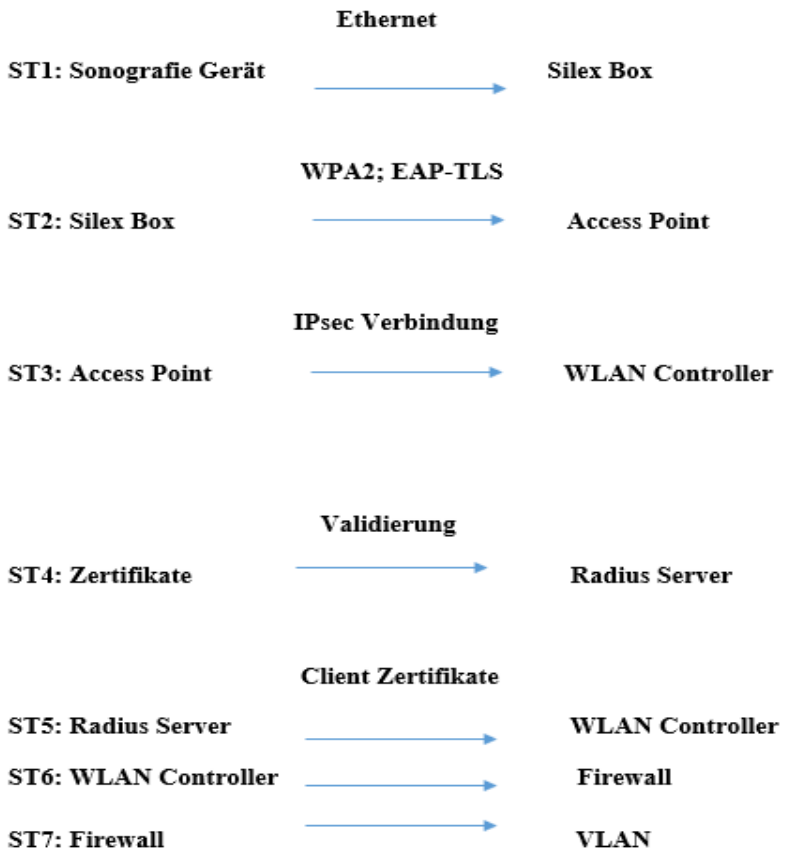

Abbildung 12: Darstellung der zu analysierenden Schnittstellen (Eigene Darstellung nach Anlehnung (AKK, 2023))

Schritt 1: Identifikation der Gefährdungen

G1 für ST1: Manipulation des Datenverkehrs (AKK, 2023)

G2 für ST2: Fehlerhafte Konfiguration (Schnabel Patrick, 2023)

G3 für ST3: Konfigurationsfehler der IPsec-Verbindung (AKK, 2023)

G4 für ST4: Certification Authority/Zertifizierung (Schnabel Patrick, 2023)

G5 für ST5: Validierung/Prüfung der Zertifikate (Schnabel Patrick, 2023)

G6 für ST6: Die Kryptographie könnte eine unzureichende Initialisierung des Pseudozufallszahlengenerators (PRNG) darstellen. (Schnabel Patrick, 2023)

G7 für ST7: Manipulation der Firewall

Schritt 2: Ermittlung der Ursachen und Gefährdungssituationen

Potenzielle Ursachen:

U1 für ST1: Medizinische Bilder oder patientenbezogene Daten könnten durch Manipulation des Datenverkehrs auf der Ethernet-Verbindung geändert werden. Dies könnte die Informationsintegrität verletzen, was zu Fehldiagnosen oder Fehlbehandlungen führen könnte. (AKK, 2023)

U2 für ST2: Ein zusätzlicher Aspekt betrifft inkorrekte Konfigurationen seitens des Nutzers oder die Verwendung von Standardeinstellungen, die dem Anwender bei der Erstinstallation nicht angepasst wurden. Standardpasswörter können aus dem öffentlich sichtbaren WLAN-Namen (SSID) oder der MAC-Adresse der WLAN-Schnittstelle abgeleitet werden. Je geringer die Länge oder Komplexität eines Passworts ist, desto leichter ist es zu erraten und ermöglicht dem Angreifer einen schnelleren Zugriff auf das gesicherte Netzwerk. Ein Angreifer müsste alle denkbaren Kombinationen testen (Brute-Force-Angriff). (Schnabel Patrick, 2023)

U3 für ST3: Bei der Konfiguration einer L2TP/IPSec-Verbindung kann ein häufiger Fehler darin bestehen, dass ein Zertifikat fehlerhaft eingerichtet ist oder nicht vorhanden ist, oder dass ein Pre-Shared-Key fehlerhaft eingerichtet ist oder nicht vorhanden ist. Falls keine verschlüsselte Verbindung zum VPN-Server auf IPSEC-Ebene hergestellt werden kann, bricht die Verbindung ohne Fehlermeldung ab. Hierdurch erhält die L2TP-Ebene keine Antwort auf ihre Anschlussanfrage. Es tritt eine Verzögerung auf, im Durchschnitt 60 Sekunden, wonach eine Fehlermeldung erscheint, dass keine Rückmeldung vom Server oder vom Modem bzw. Datenübertragungsgerät empfangen wurde. (Microsoft, 2023)

U4 für ST4: Erhält ein Hacker erfolgreich Zugriff auf eine Zertifizierungsstelle, kann er sämtliche Zertifikate erstellen. Die Möglichkeit besteht, dass jede Zertifizierungsstelle Zertifikate für jeden beliebigen Hostnamen ausstellen kann. Dies bedeutet, dass es für einen bestimmten Hostnamen mehrere Zertifikate von verschiedenen Zertifizierungsstellen geben kann. Wenn eine Zertifizierungsstelle bei der Ausstellung von Zertifikaten unzureichende Sicherheitsvorkehrungen trifft, besteht das Risiko, dass ein Angreifer ein gültiges Zertifikat für einen fremden Hostnamen erhält. Um eine Man-in-the-Middle-Attacke erfolgreich durchzuführen, ist ein solches Zertifikat von entscheidender Bedeutung, um mögliche Zertifikatsfehler auf der Client-Seite zu umgehen. Durch den geschickten Einsatz dieser Zertifikate können Geheimdienste und Ermittlungsbehörden beispielsweise ihre Identität verschleiern und sich als eine andere Person oder Organisation ausgeben. (Schnabel Patrick, 2023)

U5 für ST5: Oftmals wird ein Zertifikat als gültig akzeptiert, welches nicht verifiziert werden kann. Einige Browser akzeptieren ein ungültiges Zertifikat, auch wenn sie keine Reaktion von der Validierungsstelle oder Zertifizierungsstelle (OCSP) erhalten. Erfolgt keine Antwort, wird die Verbindung hergestellt und verschlüsselt, wobei keine Sicherheit besteht, dass die Verbindung zum richtigen Server hergestellt wurde (fehlende Authentizität). Eine individuelle Überprüfung jedes Zertifikats ist erforderlich, wenn Verschlüsselung und Authentisierung wichtig sind. Zertifikatsprüfung erfolgt sie automatisch und für den Anwender nicht sichtbar. Der Anwender verwendet TLS und vernachlässigt oft die Überprüfung der Identität des Servers, mit dem er eine verschlüsselte Verbindung aufbaut. Die Verschlüsselung kann dadurch entsprechend leichter überwunden werden. Dabei kann ein Dritter durch einen Man-in-the-Middle-Angriff die Verbindung manipulieren und eine vermeintlich sichere Verbindung abhören. (Schnabel Patrick, 2023)

U6 für ST6: Der PRNG weist eine unerwünschte Korrelation zwischen den erzeugten Zufallszahlen auf, was nicht den Anforderungen entspricht. (Schnabel Patrick, 2023)

U7 für ST7: Im Falle einer erfolgreichen unbefugten Zugriffserlangung einer Firewall oder deren Administrationsschnittstelle durch einen Angreifer eröffnen sich verschiedene Möglichkeiten der Dateimanipulation. Dadurch kann er beziehungsweise die Konfiguration der Firewall verändern, zusätzliche Dienste aktivieren oder Malware installieren. Des Weiteren ist dem Angreifer das Abhören von Kommunikationsverbindungen auf dem infiltrierten Computersystem möglich. Es besteht auch die Möglichkeit, die Firewall-Regeln so zu modifizieren, dass ein Zugang aus dem Internet auf die Firewall und das interne Netzwerk der

Institution möglich wird. Zusätzlich kann ein Hacker einen Denial of Service (DoS)-Angriff initiieren, indem er den Zugang zu bestimmten Serverdiensten im Regelwerk blockiert. (BSI, 2023)

Potenzielle Gefährdungssituationen:

GS1: Integrität

Der Angreifer verwendet die Methode ARP-Spoofing, welches die inhärenten Schwachstellen des Ethernet-Systems ausnutzt, indem es gefälschte ARP-Anfragen verwendet, um die Zuordnung von IP-Adressen zu MAC-Adressen zu manipulieren und den Datenverkehr umzuleiten. Durch das ARP-Spoofing kann der Angreifer die Position eines Man-in-the-Middle einnehmen. In dieser Position ist es dem Angreifer möglich, den gesamten Datenverkehr eines Zielrechners abzufangen und ggf. zu manipulieren. (Schnabel Patrick, 2023)

GS2: Vertraulichkeit

Der Angreifer verwendet die Methode der sogenannten Wörterbuch-Attacke, bei der ein WPA-Handshake zwischen dem Access Point und dem WLAN-Client aufgezeichnet wird, sobald der Client versucht, sich mit dem WLAN zu vernetzen. Um den Angriff durchzuführen, zeichnet der Angreifer den WPA-Handshake. Für das Erraten des WLAN-Passworts wird eine Wordlist verwendet, eine Liste mit möglichen Passwörtern. Der Erfolg des Angriffs hängt von der Qualität der Wordlist ab, da das korrekte WLAN-Passwort darin aufgeführt sein muss. Die Herausforderung bei einem Hack eines WPA/WPA2-gesicherten WLANs besteht somit in der Erstellung einer geeigneten Wordlist. (Schnabel Patrick, 2023)

GS3: Verfügbarkeit

Die IPsec-Verbindung ist fehlerhaft konfiguriert aufgrund einer falschen Zertifikatseinrichtung durch einen Mitarbeiter im IT-Bereich. (AKK, 2023)

GS4: Datensicherheit

Durch den geschickten Einsatz von gefälschten Zertifikaten erlangt der Angreifer die Kontrolle über die Verbindung zwischen Client und Server und zwingt/täuscht dem Client ein ungültiges Zertifikat auf. Da dieses Zertifikat jedoch als gültig anerkannt wird, akzeptiert der Client die Verbindung zum Angreifer als authentifiziert. Der Angreifer kann die verschlüsselten Daten entschlüsseln, mitlesen und sogar manipulieren. (Schnabel Patrick, 2023)

GS5: Vertraulichkeit

Der Angreifer nutzt die Methode des Man-in-the-Middle-Angriffs. Dabei greift er in die Kommunikation zwischen zwei vertrauenswürdigen Stationen ein und gibt vor, dass die Datenpakete von einem Rechner stammen, dem das angegriffene Gerät vertraut. Durch die Annahme einer falschen Identität bringt der Angreifer das Zielgerät dazu, alle Datenpakete an ihn zu senden. Diese Pakete können vom Angreifer analysiert und eventuell manipuliert werden. (Schnabel Patrick, 2023)

GS6: Integrität

Bei Verwendung von identischen Startwerten resultiert stets dieselbe Zahlenfolge. Liegen die Startwerte nicht ausreichend weit voneinander entfernt, kann sich der Hacker mit einem Brute-Force-Angriff auf einen begrenzten Wertebereich festlegen. Dadurch lässt sich die Verschlüsselung leichter dechiffrieren. (Schnabel Patrick, 2023)

GS7: Datensicherheit

Ein Hacker initiiert ein Denial of Service (DoS)-Angriff, indem er den Zugang zu bestimmten Serverdiensten im Regelwerk blockiert. (BSI, 2023)

Schritt 3: Ermittlung sämtlicher nicht beobachteter Folgen und ihres Schweregrads (AKK, 2023)

FO für GS1: Integrität/ Patientensicherheit

Eine unbefugte Erfassung und gezielte Manipulation des Datenverkehrs eröffnen dem Angreifer die Möglichkeit, die Befunde von Ultraschallkontrollen zu verfälschen. Diese Modifikationen könnten ungenaue Diagnosen verursachen und potenziell negative Folgen für die Gesundheit der Patienten haben.

Schweregrad: Moderat

FO für GS2: Verfügbarkeit

Ein Hacking des WLAN-Netzwerks kann die Leistung des Ultraschallgeräts beeinträchtigen, was zu Fehlfunktionen bis hin zum Totalausfall führen kann.

Schweregrad: Moderat

FO für GS3: Vertraulichkeit /Datensicherheit

Wird IPsec nicht ordnungsgemäß konfiguriert, kann dies zu einer unzureichend gesicherten Verbindung führen, die es Angreifern ermöglicht, auf den Datenverkehr zuzugreifen oder diesen zu modifizieren.

Schweregrad: Hoch

FO für GS4: Datensicherheit

Durch den geschickten Einsatz gefälschter Zertifikate kann ein Hacker die Verschlüsselung des Kommunikationsverkehrs umgehen und so vertrauliche Patientendaten entziffern und einsehen.

Schweregrad: Katastrophal

FO für GS5: Vertraulichkeit

Es besteht die Gefahr des Missbrauchs dieser Informationen, wenn der Angreifer Zugang zu vertraulichen Patientendaten erhält. Dadurch könnten die Daten für missbräuchliche Zwecke benutzt oder ohne Einwilligung der Betroffenen an Dritte weitergegeben werden.

Schweregrad: Katastrophal

FO für GS6: Integrität/Patientensicherheit

Der Eindringling kann außerdem selektiv Informationen aus den übermittelten Informationen herausfiltern oder modifizieren, was zum Ausfall relevanter Befunde beitragen könnte. Die Folge wäre eine lückenhafte oder fehlerhafte Patientenakte, die die Behandlungsqualität beeinflussen könnte.

Schweregrad: Moderat

FO für GS7: Verfügbarkeit/ Effektivität

Durch einen solchen Angriff könnte es zu Störungen bei der Interaktion des Ultraschallgeräts mit anderen vernetzten Systemen oder Geräten kommen. Die Datenübertragung kann gestört sein. Dies wirkt sich negativ auf die Effizienz und Genauigkeit der Diagnose aus.

Schweregrad: Moderat

Schritt 4: Abschätzung der Eintrittswahrscheinlichkeit

Vorhandene Risikobeherrschungsmaßnahmen:

Das Betriebssystem der Sonographie Modalität ist gehärtet (AKK, 2023):

- Kein Webbrowser verfügbar, nur die im Rahmen der Zweckbestimmung notwendigen Dienste sind verfügbar.
- Zugriffssteuerung ist eingerichtet.
- Modalität befindet sich im „AKKMT“ Netzwerk (VLAN)
- 64 Bit-Betriebssystem Windows 10

Für die Nutzung notwendige, geöffnete Netzwerk-Ports/Protokolle:

- Die Ultraschallmodalität ist mit einer Software-Firewall ausgestattet, welche alle Netzwerk-Ports außer Port 104 sperrt, da dieser für die DICOM-Interoperabilität erforderlich ist (DKG, 2011).
- Instandhaltung nach Herstellervorgaben inklusiver Sicherheitstechnischer Kontrolle nach DIN EN ISO 62353 – Anforderungen der MPBetreibV und der DGUV Vorschrift 3 erfüllt (GE-Healthcare, 2023).
- Virenscanner-ESET (AKK, 2023)
- PACS- Dedalus DeepUnity (AKK, 2023)

Auf der Grundlage dieser Maßnahmen wird die Eintrittswahrscheinlichkeit wie folgt beurteilt:

GS1: Selten

GS2: Selten

GS3: Wahrscheinlich

GS4: Häufig

GS5: Häufig

GS6: Selten

GS7: Selten

Schritt 5: Bewertung der Gefahren anhand definierter Akzeptanzkriterien

GS1: Selten → Risikolevel = moderat

GS2: Selten → Risikolevel = moderat

GS3: Wahrscheinlich → Risikolevel = hoch

GS4: Häufig → Risikolevel = katastrophal

GS5: Häufig → Risikolevel = katastrophal

GS6: Selten → Risikolevel = gering

GS7: Selten → Risikolevel = gering

Schritt 6: Festlegung und Protokollierung der Maßnahmen

RB1: Verschlüsselungstechnologien nutzen, TLS oder SSL. Das Ziel ist die Sicherstellung der Authentizität des angefragten Servers durch ein Zertifikat und die Verschlüsselung der Verbindung zwischen Client und Server. Aktuell empfiehlt es sich, die Verwendung von TLS 1.3 zu nutzen. Alternativ kann auch TLS 1.2 verwendet werden. (Schnabel Patrick, 2023)

RB2: WPA2 mit Pre-Shared-Key gilt als ausreichend sicher, wenn ein sicheres Passwort (Komplexität und Länge) eingesetzt wird. Die Benutzung eines zentralen Radius-Servers für die Authentisierung wird bevorzugt. Erfolgt die Authentifizierung über einen Pre-Shared Key (PSK), wird im Access Point ein Passwort definiert, das von allen WLAN-Clients zur Authentifizierung verwendet werden muss. Entspricht das eingegebene Passwort nicht dem zuvor festgelegten Passwort, lehnt der AP die Authentisierung des Clients ab. Das erfolgreiche Abschließen der Authentifizierung und der Aufbau einer Verbindung ist nur bei richtigem Passwort möglich. (Schnabel Patrick, 2023)

RB3: Durchführung einer gründlichen Analyse der IPsec-Konfiguration, auf mögliche Funktionsfehler oder Schwachstellen. Alle notwendigen Parameter müssen richtig gesetzt werden. Keine unklaren oder überholten Algorithmen zur Verschlüsselung oder Authentifizierung verwenden. (Schnabel Patrick, 2023)

RB4: Um mögliche Schwachstellen in der IT-Infrastruktur der Zertifizierungsstelle zu identifizieren und zu beseitigen, sollten periodisch Sicherheitsaudits und Penetrationstests durchgeführt werden. (Frauenhofer IESE, Andreas Eitel, 2020)

RB5: Passwörter verwenden, die aus einer zufälligen Kombination von Buchstaben, Zeichen und Zahlen bestehen, um ihre Entschlüsselung zu erschweren. (Schnabel Patrick, 2023)

RB6: Empfohlen wird, verschiedene Zufallszahlen zu generieren, um einen kryptografisch sicheren PRNG zu erzeugen. Zusätzlich sollten weitere Parameter wie die Uhrzeit als Startwert verwendet werden, um die Sicherheit zu erhöhen. Es ist entscheidend sicherzustellen, dass ein Angreifer nicht durch einfaches Raten Zugriff auf geschützte Informationen erhält. (Schnabel Patrick, 2023)

RB7: Der Zugriff auf die Firewall ist ausschließlich den vertrauenswürdigen Mitarbeitern der EDV-Abteilung gestattet. Die IT-Mitarbeiter erhalten individuelle Zugriffsrechte, die auf ihren spezifischen Aufgaben basieren. (AKK, 2023)

Die Verwendung von Technologien mit einem hohen Sicherheitsstandard könnte alle Risiken reduzieren. Die für RB1, RB2, RB6 und RB7 genannten Maßnahmen haben eine geringe Eintrittswahrscheinlichkeit, sollten aber dennoch in die Diskussion einbezogen werden. Ein höheres Risiko geht von den Maßnahmen RB3, RB4 und RB5 aus. Die Gewährleistung einer sicheren IT-Infrastruktur im Krankenhaus ist jedoch mit hohen Kosten verbunden. (DKG, 2011)

GS1: Risikolevel → moderat

GS2: Risikolevel → moderat

GS3: Risikolevel → hoch

GS4: Risikolevel → katastrophal

GS5: Risikolevel → katastrophal

GS6: Risikolevel → gering

GS7: Risikolevel → gering

Schritt 7: Umsetzung der Maßnahmen

Risikobeherrschungsmaßnahmen sind so umzusetzen, dass sie vor der Zulassung und Inbetriebnahme überprüft werden können.

RB1: Das derzeitige Vertrauensmodell (Certificate Authority) ist nicht in der Position, eine sichere Authentifizierung und Verschlüsselung für alle Applikationen zu gewährleisten. Um die Sicherheit des Gesamtsystems einigermaßen aufrechtzuerhalten, besteht lediglich die Möglichkeit, Workarounds zu implementieren, um Teilprobleme des TLS und seines fehlerhaften Vertrauensmodells zu beheben. (Schnabel Patrick, 2023)

RB2: Prüfen, ob die WPA2-Verschlüsselung eingerichtet ist und nicht veraltete/ unsichere Verschlüsselungsstandards wie beispielsweise WEP, WPA oder WPS eingesetzt werden. (Schnabel Patrick, 2023)

RB3: Implementierung einer Authentifizierungsmethode wie beispielsweise. digitale Zertifikate oder Pre-Shared Keys zur Sicherstellung der Zugangsberechtigung zum Netzwerk. (Schnabel Patrick, 2023)

RB4: Periodisch Sicherheitsaudits und Penetrationstests durchführen. (Frauenhofer IESE, Andreas Eitel, 2020)

RB5: Ein Sicherheitskonzept implementieren wie die. Zero Trust. Es basiert auf dem Prinzip des generellen Misstrauens gegenüber jeglichem, herkunftsunabhängigem Netzwerkverkehr. Dabei wird jeder Zugriff auf Ressourcen einer strengen Zugangskontrolle unterzogen. Jede Verbindung wird durch Verschlüsselung geschützt. (Schnabel Patrick, 2023)

RB6: Verschiedene Zufallszahlen zu generieren, um einen kryptografisch sicheren PRNG zu erzeugen. (Schnabel Patrick, 2023)

RB7: Sichere Konfiguration der Firewall. (BSI, 2023)

Schritt 8: Überprüfung der Maßnahmen

RB1: Verifikation

Effektivität: Die Authentifizierung und Verschlüsselung des Netzwerkverkehrs erfolgen über das EAP-TLS-Protokoll (AKK, 2023).

Implementierung: Bei der Verwendung von TLS-Implementierungen ist es sinnvoll, auf geprüfte Lösungen zu vertrauen. Durch die öffentliche Zugänglichkeit des Quellcodes wird die Zuverlässigkeit derartiger Umsetzungen gewährleistet. Dies ermöglicht grundsätzlich eine Codeüberprüfung auf Schwachstellen und Hintertüren. Zudem sind Aktualität und Pflege einer Software oder eines Produktes relevant. (Schnabel Patrick, 2023)

RB2: Verifikation

Effektivität: Es wird davon ausgegangen, dass das Gerät angemessen gegen schädlichen Netzwerkverkehr geschützt ist. Die Wirksamkeit dieser Schutzmaßnahme kann durch eine logische Argumentation zur Untermauerung der Annahme verifiziert werden. (DKG, 2011)

Implementierung: In der Krankenhaus IT-Infrastruktur wird WPA2 genutzt. (AKK, 2023)

RB3: Verifikation

Effektivität: In der IT-Infrastruktur sollten Pre-Shared Keys implementiert werden. (Schnabel Patrick, 2023)

Implementierung: Die Umsetzung erfolgt in einer VPN-Software zur Unterstützung der Authentisierung. Die Authentifizierung kann auf der Basis einer Maschine oder einer Person stattfinden. (AKK, 2023)

Bei der maschinenbasierten Authentifizierung wird der Pre-Shared Key (PSK) in Klartext oder verschleierter Form hinterlegt. Die Verschleierung bedeutet, dass die Klartextform des PSK nicht ohne weitere Informationen aus der gespeicherten Form erschlossen werden kann. Eine Möglichkeit besteht darin, den PSK mithilfe eines vorprogrammierten symmetrischen

Schlüssels in der VPN-Software zu kodieren. Bei der personenabhängigen Authentifizierung erfolgt die Eingabe des Schlüssels entweder durch die zu authentifizierende Person selbst oder der Schlüssel liegt verschlüsselt auf einem Speichermedium vor und lässt sich nur mit dem vom Benutzer angegebenen Passwort decodieren. (BSI, 2023)

RB4: Verifikation

Effektivität: Die Annahme ist, dass in der Firewall keine fehlerhaften Konfigurationen vorhanden sind. Die Wirksamkeit dieser Schutzmaßnahme kann durch eine logische Argumentation zur Untermauerung der Annahme verifiziert werden. (AKK, 2023)

Implementierung: Nach Abschluss der organisatorischen Vorkehrungen, Abstimmungen, Terminvereinbarungen und Informationsabfragen wird nach Freigabe ein Penetrationstest gegen den entsprechenden IP-Adressbereich durchgeführt. Dabei werden ungesicherte Schnittstellen identifiziert, die bereitgestellten Dienste analysiert und mögliche Sicherheitslücken untersucht. Anschließend werden die vorhandenen Dokumente zu IT-Sicherheitsrichtlinien, Sicherheitskonzepten, Verfahrensanweisungen, Prozessen, Netzplänen und anderen Sicherheitsdokumenten gesichtet. (Frauenhofer IESE, Andreas Eitel, 2020)

RB5: Verifikation

Effektivität: Es wird davon ausgegangen, dass das Krankenhaus angemessen gegen schädlichen Netzwerkverkehr geschützt ist. Die Wirksamkeit dieser Schutzmaßnahme kann durch eine logische Argumentation zur Untermauerung der Annahme verifiziert werden. (DKG, 2011)

Implementierung: Aktuelle Herausforderungen bei der Implementierung einer Zero-Trust-Architektur umfassen die Reife der Anbieterprodukte, die Fähigkeit und Bereitschaft der Organisation zur Umstellung, Sicherheitsbedenken, Interoperabilitätsüberlegungen und die Benutzererfahrung. (National Cybersecurity Center of Excellence National Institute of Standards and Technology, 2023)

RB6: Verifikation

Effektivität: Es wird davon ausgegangen, dass das Krankenhaus angemessen gegen schädlichen Netzwerkverkehr geschützt ist. Die Wirksamkeit dieser Schutzmaßnahme kann durch eine logische Argumentation zur Untermauerung der Annahme verifiziert werden. (DKG, 2011)

Implementierung: Für die Implementierung des vereinbarten PRNG-Algorithmus sollte eine geeignete Software eingesetzt werden. Sicherstellen, dass die Implementierung solide ist und mögliche Schwachstellen abdeckt. (AKK, 2023)

RB7: Verifikation

Effektivität: Der Schutz des Netzwerkverkehrs ist durch eine Firewall gewährleistet. Die Wirksamkeit dieser Schutzmaßnahme kann durch eine logische Argumentation zur Untermauerung der Annahme verifiziert werden. (DKG, 2011)

Implementierung: Vor der Implementierung einer Firewall ist diese sicher zu konfigurieren. Alle Änderungen an der Konfiguration sind rückverfolgbar zu protokollieren. Die Integrität der Konfigurationsdateien muss geschützt werden und Zugangspasswörter sollten mit kryptografischen Verfahren abgesichert werden. Die Firewall sollte nur die notwendigen Dienste ermöglichen, und bei Verwendung von Erweiterungen müssen die Sicherheitsrichtlinien der Organisation eingehalten werden. Nicht benötigte Dienste und Erweiterungen sollten deaktiviert oder entfernt werden. Interne Informationen zum Konfigurations- und Betriebszustand sollten vor Fremdzugriffen geschützt werden. (BSI, 2023)

Schritt 9: Bewertung aller Risiken durch entstehen der Maßnahmen (DKG, 2011)

Es wurde eine umfassende Bewertung aller potenziell neu entstandenen Risiken aufgrund der zuvor ergriffenen Maßnahmen durchgeführt.

Diese Evaluierung ergab, dass als Ergebnis der ergriffenen Maßnahmen zur Risikobeherrschung keine zusätzlichen Risiken identifiziert wurden.

Schritt 10: Bewertung und Berichterstattung des Restrisikos (DKG, 2011)

Das Restrisiko, welches die Einschätzung des Gesamtrisikos darstellt, wird mittels einer umfassenden Bewertung objektiv beurteilt. Im Anschluss werden die Ergebnisse in einem Bericht dokumentiert.

5 Zusammenfassung und Diskussion

Das Hauptziel dieser wissenschaftlichen Arbeit bestand darin, eine umfassende Risikobewertung der IT-Schnittstellen im Zusammenhang mit der Integration von Sonografie-Geräten in die Krankenhauslandschaft durchzuführen.

Die Beschaffung der für diese Arbeit notwendigen Dokumente stellte eine Herausforderung dar, da verschiedene Abteilungen des Krankenhauses getrennt voneinander dokumentierten. Dies führte zu einer Vielzahl von Dokumenten, die gesammelt und analysiert werden mussten. Die enge Zusammenarbeit zwischen dem Hersteller GE HealthCare und den internen Abteilungen des Krankenhauses war entscheidend, um sicherzustellen, dass keine wichtige Dokumentation fehlt.

Die Tatsache, dass alle Anlagen neu in Betrieb genommen wurden und die Dokumentation auf dem aktuellen Stand war, erleichterte die Risikoanalyse erheblich. Durch den Einsatz wissenschaftlicher Methoden konnten mögliche Gefahren frühzeitig identifiziert und angemessene Vorkehrungen getroffen werden, um potenzielle Schäden oder Sicherheitsrisiken zu verhindern.

Es ist jedoch bemerkenswert, dass die Anwendung der Norm IEC 80001-1 bisher nicht in Betracht gezogen wurde und keine entsprechenden Referenzprojekte vorliegen. Dies deutet darauf hin, dass die Integration von Sonografie-Geräten in die Krankenhauslandschaft möglicherweise nicht ausreichend auf potenzielle IT-Sicherheitsrisiken überprüft wurde. Die Anwendung der Norm könnte dazu beitragen, die Sicherheit und den Schutz von Patientendaten zu verbessern und mögliche Risiken zu minimieren.

Die umfangreiche Abteilung für Risikomanagement im Alfried Krupp Krankenhaus spielt eine wichtige Rolle bei der Identifizierung potenzieller Gefahren im gesamten Krankenhaus. Die Zusammenarbeit zwischen dem Krankenhaus und dem Hersteller GE HealthCare zeigt jedoch ein hohes Maß an Engagement für die Sicherheit und den Schutz der Patienten.

Im Umfang der zur Verfügung stehenden Zeit wurde eine exemplarische Untersuchung der Risiken für Sonografie-Geräte und WLAN-Adapter durchgeführt. Zusätzlich werden im Rahmen dieser Diskussion die wichtigsten Erkenntnisse und Ergebnisse der Risikoanalyse zusammengefasst und kritisch betrachtet.

Die Netzwerkanalyse ergab, dass die WLAN-Verbindung der Sonografie-Geräte stabil und zuverlässig ist und eine schnelle Übertragungsrate für die Bilder an das PACS ermöglicht.

Eine zentrale Erkenntnis dieser Risikoanalyse ist, dass die Anbindung von Sonografie-Geräten an das IT-Netzwerk erhebliche Sicherheitsrisiken mit sich bringt. Durch die Vernetzung der Geräte mit dem Internet eröffnen sich verschiedene Angriffsmöglichkeiten für Cyberkriminelle. Diese könnten sensible Patientendaten stehlen oder das Gerät manipulieren.

Eine der größten Schwachstellen besteht darin, dass viele Sonografie-Geräte standardmäßig unsichere Passwörter verwenden oder sogar gar keine Passwörter erfordern. Dadurch wird unbefugten Personen der Zugriff auf das Gerät und sensible Patientendaten erleichtert.

Die Übertragung von Malware stellt ein erhebliches Risiko für das Krankenhausnetzwerk dar, da dies zu Verlust oder Manipulation von Patientendaten sowie zum Ausfall wichtiger medizinischer Geräte führen kann. Um dieses Risiko zu minimieren, sollten Krankenhäuser geeignete Sicherheitsmaßnahmen wie Antivirensoftware implementieren und das Personal regelmäßig schulen.

Fehlerhafte Konfigurationen der Schnittstellen wurden ebenfalls als potenzielle Sicherheitslücken identifiziert, die Angreifern unbefugten Zugriff auf das Netzwerk ermöglichen können. Daher ist es entscheidend, dass Krankenhäuser regelmäßige Überprüfungen der Gerätekonfiguration durchführen und sicherstellen, dass alle Sicherheitsrichtlinien eingehalten werden.

Der Faktor Mensch wurde als eine der größten Schwachstellen in Bezug auf die Sicherheit des Krankenhausnetzwerks identifiziert, da Mitarbeiterinnen und Mitarbeiter unzureichend über die Gefahren von USB-Sticks und Malware informiert sind. Dies führt zu unsachgemäßem Umgang mit den Geräten und erhöht das Risiko von Datenverlust oder -manipulation. Es ist daher äußerst wichtig, dass Krankenhäuser Schulungsprogramme einführen, um das Bewusstsein für IT-Sicherheit zu erhöhen und das Risikobewusstsein der Angestellten zu stärken.

Es wurde auch festgestellt, dass eine fehlerhafte Konfiguration der IPsec-Validierung zu Schwachstellen im Netzwerk führen kann. Daher ist es entscheidend, dass alle Sicherheitsmechanismen ordnungsgemäß konfiguriert sind und regelmäßig überprüft werden, um solche Schwachstellen zu identifizieren und zu beheben.

Ein weiterer untersuchter Aspekt ist der Zugriff auf eine Zertifizierungsstelle. Angemessene Sicherheitsvorkehrungen müssen getroffen werden, um solche Angriffe zu verhindern.

Darüber hinaus wurde erkannt, dass ein unbefugtes Eindringen in eine Firewall schwerwiegende Folgen für die Netzwerksicherheit haben kann. Dies stellt eine bedeutende Gefahr dar und erfordert regelmäßige Überprüfungen der Firewall-Einstellungen sowie starke Authentifizierungs- und Autorisierungsmethoden, um solche Angriffe zu vermeiden.

Ein weiterer Aspekt, der in dieser Risikoanalyse beleuchtet wurde, ist die Verletzung der Patientenprivatsphäre. Durch eine unsichere Anbindung von Ultraschall-Modalitäten an das IT-Netzwerk könnten unbefugte Personen Zugriff auf sensible medizinische Daten erhalten. Dies stellt nicht nur einen Verstoß gegen Datenschutzbestimmungen dar, sondern gefährdet auch das Vertrauen der Patienten in das Gesundheitssystem.

Um diese Risiken zu minimieren, sind umfangreiche Sicherheitsmaßnahmen erforderlich. Dazu gehören unter anderem die Implementierung von Firewalls und Intrusion-Detection-Systemen, regelmäßige Updates der Gerätesoftware, Schulungen für das medizinische Personal zur Sensibilisierung für IT-Sicherheit sowie die Einhaltung von Datenschutzbestimmungen.

6 Ausblick

IT-Systeme können potenzielle Risiken minimieren und die Sicherheit der Patientendaten gewährleisten. In Zukunft kann das Alfried Krupp Krankenhaus die Anwendung der Norm IEC 80001-1 in Betracht ziehen und entsprechende Referenzprojekte durchführen, um die Integration von medizinischen IT-Systemen sicherer zu gestalten. Dies würde dazu beitragen, potenzielle Risiken frühzeitig zu erkennen und geeignete Maßnahmen zur Risikominderung zu ergreifen.

Insgesamt hat diese wissenschaftliche Arbeit gezeigt, dass eine umfassende Risikobewertung der IT-Schnittstellen im Zusammenhang mit der Integration von Sonografie-Geräten in die Krankenhauslandschaft von großer Bedeutung ist. Die Verwendung der Norm IEC 80001-1 als Grundlage für die Risikoanalyse kann dazu beitragen, potenzielle Gefahren zu identifizieren und geeignete Maßnahmen zur Risikominderung zu ergreifen. Die vorliegende Risikoanalyse zeigt deutlich, dass die Anbindung von Sonografie-Geräten an das IT-Netzwerk mit erheblichen Sicherheitsrisiken verbunden ist. Es ist daher unerlässlich, geeignete Maßnahmen zu ergreifen, um diese Risiken zu minimieren und die Sicherheit der Patientendaten zu gewährleisten.

In Zukunft sollten weitere Forschungsarbeiten durchgeführt werden, um neue Technologien und Ansätze zur Verbesserung der IT-Sicherheit in medizinischen Umgebungen zu untersuchen. Insbesondere die Entwicklung von sicheren Kommunikationsprotokollen und Verschlüsselungstechnologien könnte dazu beitragen, die Vertraulichkeit und Integrität der übertragenen Daten zu gewährleisten. Darüber hinaus sollte auch das Bewusstsein für IT-Sicherheit im Gesundheitswesen gestärkt werden. Eine kontinuierliche Schulung des medizinischen Personals in Bezug auf sichere Praktiken und den Umgang mit sensiblen Patientendaten ist unerlässlich.

Abschließend lässt sich sagen, dass die Anbindung von Ultraschallgeräten an das IT-Netzwerk ein komplexes Thema ist, das eine sorgfältige Risikoanalyse erfordert. Durch die Implementierung geeigneter Sicherheitsmaßnahmen und die kontinuierliche Überwachung der IT-Netzwerke können die Risiken reduziert werden. Es ist wichtig anzumerken, dass Cyberangriffe eine ständige Bedrohung darstellen und dass keine einzelne Maßnahme alle Risiken vollständig ausschließen kann. Daher sollte das Alfried Krupp Krankenhaus eine ganzheitliche Sicherheitsstrategie entwickeln, die kontinuierlich überwacht und aktualisiert wird, um mit den sich ständig weiterentwickelnden Bedrohungen Schritt zu halten.

7 Literaturverzeichnis

Ahlbrandt, Ahlbrandt, J., Röhrig, R., Dehm, J., Wrede, C., & Imhoff, M. (2013). *Risikomanagement für medizinische Netzwerke in der Intensiv- und Notfallmedizin. Gemeinsames Positionspapier zur Norm IEC 80001-1.* GMS Medizinische Informatik, Biometrie und Epidemiologie.

AKK, I. M. (11. 09 2023). Risikomanagment im IT. (S. Yilmaz, Interviewer)

Alfried Krupp Krankenhaus. (01. 11 2023). Von Alfried Krupp Krankenhaus: https://www.krupp-stiftung.de/institutionen/alfried-krupp-krankenhaus/ abgerufen

Armin, G. (2012). *DIN EN 80001-1: Chancen und Potenziale für vernetzte Medizintechnik.* Erkrath: Ingenieurbüro für Medizintechnik.

Birnbaum, J., & Albrecht, R. (2007). *Ultraschallgestützte Regionalanästhesie.* Springer Verlag.

Bless, R., Mink, S., Conrad, M., Kutzner, K., Blaß, E.-O., Hof, H.-J., & Schöller, M. (2005). *Sichere Netzwerkkommunikation: Grundlagen, Protokolle und Architekturen.* Springer Verlag.

Brusis, T. (2011). *In Geschichte der deutschen Hals-Nasen-Ohren_Kliniken im 20. Jahrhundert.* Essen: Springer Berlin Heidelberg.

BSI. (05. 11 2023). *Aufbau von Virtual Private Networks (VPN) und Integration.* Abgerufen am 2006 von Bundesamt für Sicherheit in der Informationstechnik: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Internetsicherheit/vpn_pdf.pdf?__blob=publicationFile

BSI. (03. 11 2023). *BSI- Bundesamt für Sicherheit in der Informatiionssicherheit.* Von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Themen-Downloads/Gesundheit/risikoanalyse_krankenhaus-it_langfassung.pdf?__blob=publicationFile&v=4 abgerufen

BSI. (04. 11 2023). *BSI- IT-Grundschutzkatalog.* (BSI, Hrsg.) Von https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf abgerufen

BSI. (05. 11 2023). *NET.3.2 Firewall.* Abgerufen am 2021 von https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/09_NET_Netze_und_Kommunikation/NET_3_2_Firewall_Edition_2023.pdf?__blob=publicationFile&v=4

Bundesamt für Sicherheit in der Informationstechnik. (26. 10 2023). *BSI-Standard 200-3.* (BSI, Hrsg.) Von

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2 abgerufen

Conteg. (22. 10 2023). *Conteg*. Von https://www.myconteg.de/warm-kaltgang abgerufen

Crocetti, P. (25. 10 2023). *ComputerWeekly.de*. Von https://www.computerweekly.com/de/definition/Backup-auf-Datenband-Tape-Backup#:~:text=Unter%20Tape%20Backup%20oder%20auch,oder%20%2Dausfall%20wiederhergestelltwerden%20k%C3%B6nnen abgerufen

Darms, M., Haßfeld, S., & Fedtke, S. (2019). *IT-Sicherheit und Datenschutz im Gesundheitswesen: Leitfaden für Ärzte, Apotheker, Informatiker und Geschäftsführer in Klinik und Praxis.* Springer Verlag.

Dehn, S. (2017). *Netzwerke Netzwerktechnik* (Bd. 9.Ausgabe). Herdt.

Deutsche Krankenhausgesellschaft e.V. (kein Datum). *Deutsche Krankenhausgesellschaft e.V.* Von https://www.dkgev.de/themen/digitalisierung-daten/informationstechnik-im-krankenhaus/ abgerufen

Dittel, E. E., & Kopacek, P. (1995). *EDV-Einsatz in Krankenanstalter.* Springer Verlag.

DKG. (2011). *Anwendung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten (DIN EN 80001-1:2011)* (Bd. 1.Auflage). Deutsche Krankenhaus Verlagsgesellschaft mbG.

Dössel, O. (2016). *Bildgebende Verfahren in der medizin: von der Technik zur medizinischen Anwendung* (Bd. 2.Auflage). Springer Verlag.

Eckert, C. (2012). *IT-Sicherheit: Konzept- Verfahren-Protokolle* (Bde. 7., überarbeitete und erweiterte Auflage). Oldenbourg Wissenschaftsverlag .

Frauenhofer IESE, Andreas Eitel. (2020). IT-Security (1/4): IT-Sicherheitsaudits zur Evaluation und Absicherung Ihrer Infrastruktur. *Blog des Fraunhofer-Institut für Experimentelles Software Engineering*. Von https://www.iese.fraunhofer.de/blog/it-security-teil1/ abgerufen

Gärtner, A. (2010). *Medizinische Netzwerke und Software als Medizinprodukt, Medizinproduktesicherheit* (Bd. 5). TÜV Media.

GE-Healthcare. (05. 11 2023). *GE Ultraschall Service*. Von https://www.gehealthcare-ultrasound.de/service/ abgerufen

Herrmann, T. A., Kleinbeck, U., & Ritterskamp, C. (2009). *Innovationen an der Schnittstelle zwischen technischer Dienstleistung und Kunden 2.* Springer Verlag.

Hollberg, N., Pleuss, B., & Rittersbacher, H. (1973). *Computer: Aufgaben im Gesundheitswesen: Kolloquien "Computer in der Medizin-Ergebnisse und künftige Entwicklungen"*. Springer Verlag.

Huang, H. B. (2003). Enterprise PACS and image distribution. *Computerized Medical Imaging and Graphics*, 241-253.

Isselhorst, Dr. Hartmut. (2016). *BSI- IT-Grundschutz 15. Ergänzungslieferung.* Von IT-Grundschutz-Kataloge: https://download.gsb.bund.de/BSI/ITGSK/IT-Grundschutz-Kataloge_2016_EL15_DE.pdf abgerufen

Königs, H. P. (2017). *IT-Risikomanagement mit System: Praxisorientiertes Management von Informationssicherheits-, IT- und Cyber-Risiken* (Bd. 5.Auflage). Springer Verlag.

Kramme, R. (2011). *Medizintechnik, Verfahren - Systeme - Informationsverarbeitung* (Bd. 4.Auflage). Springer.

Kramme, R. (2017). *Medizintechnik Verfahren - Systeme - Informationsverarbeitung.* Springer Berlin, Heidelberg.

Kruber, D. K. (2015). *Handbuch Klinisches Risikomanagement* (Bd. 1.Auflage). Springer Verlag.

Microsoft. (05. 11 2023). *Problembehandlung bei einer Microsoft L2TP/IPSec-Clientverbindung für ein virtuelles privates Netzwerk*. Von https://learn.microsoft.com/de-de/troubleshoot/windows-client/networking/l2tp-ipsec-vpn-client-connection-issue abgerufen

Miller, Katharina. (01. 11 2023). *Yaveon*. Von https://www.yaveon.de/glossar/edv/#:~:text=Im%20Wesentlichen%20sind%20EDV%2DAbteilungen,mit%20Programmen%20sowie%20Betriebssystemen%20gibt abgerufen

National Cybersecurity Center of Excellence National Institute of Standards and Technology. (01. 11 2023). *Implementimg a zero trust architecture.* Abgerufen am 2020

P.Gocke, & Debatin, J. (2011). *IT im Krankenhaus; Von der Theorie in die Umsetzung* . Medizinisch Wissenschaftliche Verlagsgesellschaft.

Schnabel Patrick. (01. 11 2023). *Elektonik Kompendium*. Abgerufen am 2013 von https://www.elektronik-kompendium.de/sites/net/1906041.htm#:~:text=Schwachstelle%3A%20Validierung%20%2F%20Pr%C3%BCfung%20der%20Zertifikate&text=Nach%20dem%20Motte%3A%20Egal%20mit,unterschiedlicher%20Hostname%20im%20Zertifikat

Seilbold, H. (2006). *IT-Risikomanagement* . Oldenbourg Verlag, München Wien .

Silex Technologie. (15. 09 2023). *Silex Technologie*. Von https://www.silextechnology.com/de/konnektivit%C3%A4tsl%C3%B6sungen/display-konnektivit%C3%A4t/br-300an abgerufen

Wolfgang, H., & Ehrenbaum, K. (2011). *Umfassendes Risikomanagement im Krankenhaus Risiken beherrschen und Chancen erkennen* (Bd. 1. Auflage). Medizinisch Wissenschaftliche Verlagsgesellschaft.

9 Anhang

Abbildungsverzeichnis

Tabellenverzeichnis