Forschungsinstitut
Cyber Defence
Universität der Bundeswehr München

gefördert durch
Bayerisches Staatsministerium für
Gesundheit und Pflege

SMART HOSPITALS

MAßNAHMENKATALOG ZUR VERBESSERUNG DER IT-SICHERHEIT IN BAYERISCHEN KRANKENHÄUSERN

AUSGABE 2021/2022

der Bundeswehr
Universität München

Michael Steinke, Laura Stojko, Siegfried Brunner, Volker Eiseler, Julia Hofmann,
Marko Hofmann, Wolfgang Hommel, Uwe Langer, Jasmin Riedl

Entstanden im Rahmen des Projekts
Smart Hospitals – Sichere Digitalisierung bayerischer Krankenhäuser,
gefördert durch das Bayerische Staatsministerium für Gesundheit und Pflege (StMGP),
durchgeführt vom Forschungsinstitut Cyber Defence (CODE),
Universität der Bundeswehr München
https://www.unibw.de/code/smart-hospitals

Kontakt
Forschungsinstitut Cyber Defence (CODE)
Universität der Bundeswehr München
Carl-Wery-Straße 22
81739 München
https://www.unibw.de/code/

Umschlaggestaltung: Siegfried Brunner
Satz: Michael Steinke, Jasmin Riedl
Druck: Alfred Hintermaier, Offsetdruckerei + Verlag, München
Lektorat: Désirée Warntjen

ISBN 978-3-943207-53-8 (Print)
ISBN 978-3-943207-54-5 (ePDF)

Wir bedanken uns insbesondere bei Herrn Herbert Motzel vom Klinikum Fürth für die außerordentliche Unterstützung bei der Erstellung der Vorlagen für die ISMS-Dokumente. Wir bedanken uns auch bei Herrn Thomas Havekost, der im Rahmen seiner Bachelorarbeit an der Entstehung der Informationssicherheitsmanagement-Templates mitgewirkt hat.

Wir verzichten aus Gründen der besseren Lesbarkeit auf eine gleichzeitige Verwendung von männlicher und weiblicher Sprachform. Die Personenbezeichnungen gelten für alle Geschlechter.

gefördert durch
Bayerisches Staatsministerium für
Gesundheit und Pflege

Grußwort von Staatsminister Klaus Holetschek

Sehr geehrte Damen und Herren,

die Corona-Pandemie führt uns einmal mehr vor Augen, wie wichtig eine gut funktionierende, flächendeckende medizinische Versorgung ist. Die Erwartungen an unsere Gesundheitseinrichtungen sind hoch: Sie müssen konstant und reibungslos funktionieren – auch unter den erschwerten Bedingungen einer Pandemie. Krankenhäuser nehmen dabei eine Schlüsselstellung ein, denn sie sind eine der ersten Anlaufstellen für die akute Versorgung der Menschen. Auch deshalb ist es ein wesentlicher Schwerpunkt bayerischer Gesundheitspolitik, eine leistungsfähige Krankenhausversorgung in allen Landesteilen Bayerns sicherzustellen.


© Andi Frank

Die Digitalisierung mit ihren vielfältigen Unterstützungsmöglichkeiten im Krankenhausalltag ist ein wichtiger Baustein zur Optimierung der Patientenversorgung. Um Datenverluste und Systemausfälle zu vermeiden, gilt es, bei der Anwendung der Techniken wachsam zu sein und vorzusorgen. Das vom bayerischen Gesundheitsministerium im Rahmen der Digitalisierungsoffensive BAYERN DIGITAL II seit 2018 geförderte Projekt „Smart Hospitals“ der Universität der Bundeswehr München will dabei unterstützen. Bereits für die Jahre 2020/2021 wurde ein Maßnahmenkatalog erarbeitet, der als Leitfaden für einen datengeschützten und datentechnisch reibungslosen Krankenhausalltag dient. Da die Zeit vor allem bei der Digitalisierung nicht stehen bleibt, versteht sich die aktuelle Fortschreibung des Katalogs von selbst.

Um die Anwendungsfelder der Digitalisierung in den Kliniken abdecken zu können, wurde der Maßnahmenkatalog 2021/2022 ergänzt und ist noch umfangreicher als sein Vorgänger. Er umfasst etwa Maßnahmen zu Cloud-Diensten, einen Maßnahmenblock zum Datenschutz und die im Anhang realisierten Dokumentenvorlagen. Mein Dank gilt den Krankenhäusern, die sich hier aktiv und engagiert eingebracht haben, damit dieses praxis- und zukunftsorientierte Werk erstellt werden konnte. Die Autorinnen und Autoren und ich hoffen auch weiterhin auf Ihre Unterstützung!

Ich wünsche Ihnen eine interessante und für Ihre Arbeit verwertbare Lektüre, damit Sie die immensen Vorteile der Digitalisierung zum Wohle der Patientinnen und Patienten sicher nutzen können.

Klaus Holetschek MdL
Bayerischer Staatsminister für Gesundheit und Pflege

Grußwort des Landesamts für Sicherheit in der Informationstechnik

Die fortschreitende Digitalisierung im Bereich der medizinischen Versorgung bietet neuartige, verbesserte Möglichkeiten für die Patientenversorgung, beispielsweise durch elektronische Patientenakten, verstärkte digitale Vernetzung und Datenaustausch innerhalb der Klinik und mit Kooperationspartnern wie Fachkliniken, Arztpraxen und Laboren und über die Anbindung an die Telematik-Infrastruktur.

Neben den durch die Digitalisierung erzielten und erreichbaren Vorteilen wächst gleichzeitig die Abhängigkeit von funktionierenden IT-Systemen. Vorfälle, wie der Verschlüsselungstrojaner im September 2020 an der Universitätsklinik Düsseldorf oder die Veröffentlichung von Patientendaten im Mai 2021 in Irland, haben gezeigt, dass die Informationstechnik bei Betreibern medizinisch kritischer Infrastrukturen ausreichend robust gegenüber Cyber-Angriffen abgesichert sein muss. Tagtäglich werden neue Schwachstellen bekannt. Von der Microsoft Exchange Server Schwachstelle waren allein in Deutschland zehntausende Mailserver betroffen, darunter auch einige in Kliniken.

Kliniken müssen die Versorgung der Patienten im Krankenhaus rund um die Uhr gewährleisten können. Cyber-Angriffe richten sich nicht nur gegen die großen KRITIS-Krankenhäuser, die ihre getroffenen Vorbeugemaßnahmen regelmäßig gegenüber dem BSI nachweisen müssen, sondern im gleichen Maß gegen alle Arten von Krankenhäusern unabhängig von ihrer Größe. Der Gesetzgeber reagierte auf den technischen Fortschritt und die daraus resultierenden Risiken mit dem neuen §75c SGB V (Patientendatenschutzgesetz). Ab 1. Januar 2022 sind nun alle Krankenhäuser unabhängig ihrer Größe verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zum Schutz ihrer IT-Systeme zu treffen.

Kernaufgaben des LSI sind der aktive Schutz und die Gefahrenabwehr der staatlichen IT-Systeme, die Information zu aktuellen IT-Sicherheitsgefahren und die Beratung von öffentlichen Betreibern kritischer Infrastrukturen zur Steigerung des Schutzniveaus. Im Bereich „IT-Sicherheitsberatung für den Sektor Gesundheit“ hat das LSI die Orientierungshilfe „IT-Sicherheit in Kliniken“ entwickelt und arbeitet eng mit dem Bayerischen Gesundheitsministerium und der Arbeitsgruppe „Smart Hospitals“ im Forschungsinstitut Cyber Defence (FI CODE) der Universität der Bundeswehr zusammen. Die Orientierungshilfe „IT-Sicherheit in Kliniken“ und der vorliegende Maßnahmenkatalog wurden eng aufeinander abgestimmt. Beide Ansätze ergänzen sich gegenseitig und bieten eine niederschwellige Arbeitshilfe zur besseren Absicherung der kritischen IT-Dienstleistungen im Klinikumfeld.

Auf die weitere zukünftige Zusammenarbeit mit der Smart-Hospitals-Projektgruppe freue ich mich. Der Maßnahmenkatalog der Universität der Bundeswehr in München bietet aus unserer Sicht sehr fundierte, detaillierte Maßnahmenempfehlungen zur Härtung der digitalen Krankenhaus-Infrastruktur. Die IT-(Sicherheits-)Verantwortlichen der bayerischen Plankrankenhäuser lade ich herzlich ein, das Beratungsangebot des LSI und die kommenden Veranstaltungsreihen als Plattformen zur Vernetzung zu nutzen.

Daniel Kleffel
Präsident des LSI in Nürnberg

Vorwort der Universität der Bundeswehr München

Sehr geehrte Damen und Herren,

© UniBw M / Herr Siebold

Gerade in Pandemiezeiten ist das Thema Digitalisierung und Vernetzung in vielen Bereichen des alltäglichen Lebens und in der Arbeitswelt in den Fokus gerückt. Auch weil es zu einem wesentlichen wirtschaftlichen Faktor geworden ist, fördert die Politik derartige Projekte auch im Öffentlichen Sektor und im Gesundheitswesen. Doch mit dem Ausbau der Digitalisierung werden die IT-Sicherheitsrisiken gerade in Krankenhäusern – als einem systemrelevanten und höchst sensiblen Ort – tendenziell stark zunehmen und die Mitarbeitenden stehen vor zusätzlichen Herausforderungen.

Die Universität der Bundeswehr München ist seit vielen Jahrzehnten ihrem Leitbild „Sicherheit in Technik und Gesellschaft" verpflichtet. Die interdisziplinäre Zusammenarbeit über Fächergrenzen hinweg und das breite Themenspektrum der Forschung zeigt sich auch in den vielen, langjährigen Kooperationen mit dem Öffentlichen Sektor. So wird das Projekt „Smart Hospitals – Sichere Digitalisierung bayerischer Krankenhäuser" vom Bayerischen Staatsministerium für Gesundheit und Pflege (StMGP) gefördert und die Arbeitsgruppe agiert unter Federführung des Forschungsinstituts Cyber Defence (CODE) der Universität der Bundeswehr München, mit Beteiligung der Fakultät für Informatik und der Fakultät für Staats- und Sozialwissenschaften. Sehr erfreulich ist, dass die Ergebnisse des Projekts „Smart Hospitals" nunmehr als Maßnahmenkatalog zur Verbesserung der IT-Sicherheit in bayerischen Krankenhäusern in einer 2. Auflage erscheinen.

Zum einen bietet der Maßnahmenkatalog dem Personal einen guten Einstieg ins Thema IT-Sicherheit. Zum anderen erhalten die Mitarbeitenden wertvolle Informationen, beispielsweise zu Besonderheiten bei der Absicherung medizinischer Großgeräte oder im Umgang mit Datensätzen. Es werden konkrete Hinweise auf Verbesserungsmöglichkeiten benannt, die einfach umzusetzen sind. Insbesondere die Mitarbeitenden, die für die Gesundheitsversorgung der Patientinnen und Patienten verantwortlich sind, haben oftmals eng getaktete Abläufe und viele Faktoren im Betrieb abzuwägen. Umso wichtiger ist es, dass sie passgenaue Hilfsmittel mit hohem Nutzen an der Hand haben, die zwar von den theoretisch sichersten Lösungen abweichen können, sich aber dennoch als praktisch und effizient erweisen.

Der Katalog mit seinen mittlerweile rund 40 beschriebenen technischen und organisatorischen Maßnahmen soll den Mitarbeitenden als Leitfaden dienen und bildet die Erfahrungen von Geschäftsleitung, IT-Verantwortlichen, Ärztinnen und Ärzten sowie Pflegerinnen und Pflegern mit ab. Er lebt vom geübten Blick der Praxis und Akteuren, die bereit für Veränderungen sind. Daher begrüße ich es, wenn sie sich weiter so engagiert einbringen. Das gemeinsame Ziel ist eine sichere und nachhaltige Digitalisierung im Gesundheitswesen, die Abläufe effizient macht und die Institution Krankenhaus für Mitarbeitende und Patienten gleichermaßen attraktiv hält.

Univ.-Prof. Dr.-Ing. habil. Dr. mont. Eva-Maria Kern, MBA
Vizepräsidentin für Forschung und Wissenschaftlichen Nachwuchs

Vorwort der Autoren

Liebe Leserinnen und Leser,

die Ihnen vorliegende zweite Ausgabe dieses Maßnahmenkatalogs entstand im Rahmen des Projekts *Smart Hospitals – Sichere Digitalisierung bayerischer Krankenhäuser*. Dieses Projekt wird vom bayerischen Staatsministerium für Gesundheit und Pflege (StMGP) gefördert und vom Forschungsinstitut Cyber Defence (FI CODE) der Universität der Bundeswehr München in enger fachlicher Abstimmung mit dem bayerischen Landesamt für Sicherheit in der Informationstechnik (LSI) durchgeführt.

Die Grundidee dieses Dokuments, baukastenartige Musterlösungen zur IT-Sicherheit für die Verwendung sowohl in bestehenden IT-Infrastrukturen als auch bei anlaufenden Digitalisierungsprojekten in Krankenhäusern zusammenstellen, wurde erfreulich positiv aufgenommen und entsprechend beibehalten. Unser besonderer Dank gilt allen, die uns mit ihren Rückmeldungen, Anregungen zu weiteren zu behandelnden Themen, Erfahrungsberichten aus dem praktischen Einsatz und durch die Bereitstellung von zum Teil sehr umfangreichen Unterlagen, die zu Dokumentenvorlagen verarbeitet wurden, unterstützt haben.

Trotz des gegenüber der vorherigen Ausgabe um rund ein Drittel gewachsenen Umfangs war unser Ziel weiterhin, jede einzelne Maßnahme kompakt – auf einer oder zwei Seiten – und dennoch spezifisch für die Anwendung in Krankenhäusern zu beschreiben. Unabhängig von der Größe und Aufgabenstellung Ihres Hauses sollen Sie damit einen schnellen Einstieg in die jeweilige Materie finden und bei der Maßschneiderung für Ihre eigene Umgebung unterstützt werden. Für weiterführende Details wird in bewährter Form auf Standards, Good Practices und weitere Literatur verwiesen, wobei wir Ihnen insbesondere die parallele Nutzung der vom LSI herausgegebenen Orientierungshilfe „IT-Sicherheit in Kliniken“ empfehlen, die ebenfalls auf sehr positive Resonanz gestoßen ist, inhaltlich mit dem vorliegenden Maßnahmenkatalog eng verzahnt wurde und einen dazu komplementären Ansatz verfolgt.

Das Management der Informationssicherheit in Krankenhäusern steht anhaltend vor der Herausforderung, mit zum Teil stark begrenzten Ressourcen ein komplexes und sehr breites Themenfeld bearbeiten zu müssen, bei dem die Akzeptanz der umgesetzten Maßnahmen durch alle beteiligten Personen und die enge Abstimmung mit einer großen Palette an Geschäfts- und IT-Service-Management-Prozessen zentrale Schlüsselkriterien für den nachhaltigen Erfolg darstellen. Unser Ziel ist es, Ihnen konkrete Empfehlungen für den praktischen Einsatz an die Hand zu geben, erfolgreiche Lösungen bayerischer Krankenhäuser in der Breite bekannter und zugänglicher zu machen sowie aktuellen Herausforderungen rund um die sichere Digitalisierung mit gezielten Ratschlägen zu begegnen.

Bitte unterstützen Sie uns weiterhin, beispielsweise durch Themenvorschläge, Rückfragen bei Unklarheiten und mit eigenen Erfahrungsberichten.

Weitere Informationen zum Projekt finden Sie auf der Webseite https://www.unibw.de/code/smart-hospitals. Wir freuen uns auf Ihr Feedback per E-Mail an projekt-smarthospitals@unibw.de.

Das Smart-Hospitals Projekt-Team im Juli 2021
Dr. Siegfried Brunner, Volker Eiseler, Dr. Julia Hofmann, Prof. Dr. Marko Hofmann, Prof. Dr. Wolfgang Hommel, Dr. Uwe Langer, Prof. Dr. Jasmin Riedl, Michael Steinke, Laura Stojko

Inhaltsverzeichnis

Prävention: ■ ***Detektion:*** ■ ***Reaktion:*** ■

Kapitel 1

Benutzung dieses Maßnahmenkatalogs

IT-Sicherheit ist keine Dienstleistung, die Einzelpersonen aus der IT-Abteilung für ein gesamtes Krankenhaus erbringen können. Vielmehr steht und fällt sie mit dem Bewusstsein für das Thema und dem Handeln des Arbeitgebers und der gesamten Belegschaft.

Ein Maßnahmenkatalog, der für das breite Spektrum bayerischer Krankenhäuser konkrete, aber doch flexibel an die jeweilige IT-Umgebung anpassbare Handlungsempfehlungen enthält, benötigt eine primäre Zielgruppe. Dieser Schwierigkeit stellen wir uns, indem jede Maßnahme einleitend knapp und möglichst allgemeinverständlich zusammengefasst wird und die Zuständigkeiten der relevanten Personengruppen, wie Geschäftsführung, IT-Abteilung und Nutzer, übersichtlich dargestellt und kurz begründet werden. Die weiteren Ausführungen pro Maßnahme wenden sich vorrangig an die für die Umsetzung zuständigen Gruppen. Es ist naheliegend, dass es sich dann häufig doch wieder um die IT-Abteilung handelt. Auch bei dieser Zielgruppe berücksichtigen wir, dass nicht alle Beteiligten als IT-Sicherheitsexperten in ihren Beruf gestartet sind und üblicherweise dringendere Aufgaben anliegen als das intensive Studium von Handreichungen wie dieser. Die Beschreibungen der Maßnahmen beschränken sich deshalb in der Regel auf ein bis zwei Seiten Text, um die wichtigsten Inhalte zu vermitteln. Für weiterführende und vertiefende Informationen sind Referenzen auf andere Dokumente angegeben, die die Sachverhalte aus unserer Sicht bereits hervorragend darlegen. Wesentlich aufwendiger sind die erforderlichen eigenen Überlegungen zu den jeweiligen Themen sowie die Konzeption, die Umsetzung und der laufende Betrieb der einzelnen Maßnahmen. Diesen Hauptteil der Arbeit können wir Ihnen nicht abnehmen, wir wollen ihn aber zumindest initial unterstützen und Ihnen einige Argumente für die interne Diskussion an die Hand geben.

In diesem Kapitel werden einleitend Hintergrund, Konzept und Anwendung dieses Maßnahmenkatalogs beschrieben.

1.1 Geltungsbereich und Hintergrund

Dieser Maßnahmenkatalog wendet sich an alle bayerischen Krankenhäuser, unabhängig von ihrer Größe und Aufgabenstellung (z. B. Versorgungsstufe I, II, III oder Fachkrankenhaus gemäß Krankenhausplan des Freistaats Bayern). Die beschriebenen Maßnahmen sind unverbindlich in dem Sinn, dass Ihnen die Auswahl und Umsetzung der für Ihr Krankenhaus relevanten Maßnahmen aus Sicht des Projekts „Smart Hospitals“ selbstverständlich freigestellt bleibt, da es im Einzelfall gute fachliche Gründe dafür geben kann, Maßnahmen bewusst nicht umzusetzen.

Im Umkehrschluss ergibt sich selbst durch die Umsetzung aller Maßnahmen nicht automatisch eine Konformität mit allen relevanten Compliance-Auflagen und Standards, wie sie beispielsweise für Zertifizierungen und die damit verbundenen Audits erforderlich ist. Der Maßnahmenkatalog soll Sie vielmehr in die Lage versetzen, sich den vielen Themenbereichen der IT-Sicherheit systematisch und strukturiert zu nähern, den Reifegrad der in Ihrem Krankenhaus bereits vorhandenen Maßnahmen beurteilen zu können und abzuschätzen, wo im Hinblick auf eine möglichst breite Abdeckung des Themas IT-Sicherheit noch Handlungsbedarf besteht und wie dieser zu priorisieren ist.

Die vorliegende zweite Fassung basiert auf der im vergangenen Jahr erschienenen Ausgabe 2020/2021 des Maßnahmenkatalogs. Dank der Rückmeldung zahlreicher Krankenhäuser, die die letzte Ausgabe bereits in ihren Praxisalltag integriert haben, konnten wir zum einen die bestehenden Maßnahmen teilweise überarbeiten, zum anderen jedoch auch neue Schwerpunkte umsetzen. Dazu zählen beispielsweise eine stärkere Einbeziehung des Themas Cloud Computing, das neue Kapitel zum Thema Datenschutz und rechtliche Konformität sowie die an diese Version neu angehängten Vorlagen für einige typische Dokumente, die im Rahmen eines Informationssicherheits-Managementsystems (ISMS) zu erstellen sind.

Wie in der vorangegangen sind auch in dieser Ausgabe die Beschreibungen der neuen Maßnahmen und die Inhalte des Maßnahmenkatalogs auf möglichst große Praxisnähe und Verständlichkeit ausgelegt.

Konzept und Anwendung des Katalogs

In Kapitel 2 wird zunächst eine vereinfachte und verallgemeinerte Sicht auf die IT-Infrastruktur eines Krankenhauses beschrieben. Trotz zum Teil sehr ähnlicher Eckdaten ist jedes Krankenhaus bzw. jeder Verbund von Krankenhäusern anders und hat individuelle Stärken und Handlungsbedarfe im Bereich IT-Sicherheit. Zur Veranschaulichung der einzelnen Maßnahmen orientieren wir uns deshalb an diesem fiktiven Beispiel und hoffen, dass Sie sich darin zumindest teilweise gut wiederfinden können.

Ab Kapitel 3 finden Sie die einzelnen Maßnahmen, die zu logisch zusammengehörenden Themenblöcken gebündelt wurden. Der Bogen spannt sich von organisatorischen Maßnahmen, zu denen auch alles rund um das IT-Sicherheitsbewusstseins des Personals gehört, über technische Maßnahmen zur Absicherung von Netzen, Geräten, Diensten und dem Gebäude bis hin zu Themen des Datenschutzes und seinen rechtlichen Aspekten.

In jedem Kapitel sind die Maßnahmen in der Reihenfolge aufgeführt, die wir für eine systematische Umsetzung empfehlen. Diese Reihenfolgen sind zwar nicht zwingend einzuhalten, doch sie sollten bei der individuellen Priorisierung je nach Eignung berücksichtigt werden. Allgemein ist es eher empfehlenswert, Maßnahmen aus allen Bereichen umzusetzen, als nur in einzelnen Bereichen alle Maßnahmen auf einmal anzugehen. Darüber hinaus ist zu beachten, dass auch dem Sicherheitsmanagement die Idee der kontinuierlichen Verbesserung zugrunde liegt: IT-Infrastruktur und IT-Dienste, Bedrohungen und verfügbare Sicherheitsmaßnahmen entwickeln sich ständig weiter, sodass alle Themenbereiche regelmäßig erneut zu betrachten sind.

Jede Maßnahme ist bereits im Inhaltsverzeichnis mit farbigen Quadraten gekennzeichnet. Grüne Quadrate markieren Maßnahmen, die präventiv wirken sollen, also das Eintreten von IT-Sicherheitsvorfällen von vornherein verhindern können. Ein blaues Quadrat signalisiert, dass die Maßnahme dabei unterstützen kann, eingetretene IT-Sicherheitsprobleme schnell zu erkennen. Rote Quadrate kennzeichnen Maßnahmen, die bei IT-Sicherheitsvorfällen dazu beitragen können, professionell zu reagieren und schnellstmöglich wieder zum Soll-Zustand des IT-Betriebs zurückzukehren. Zwar scheinen die präventiven Maßnahmen in mancherlei Hinsicht als am wichtigsten und attraktivsten, dennoch dürfen die anderen Kategorien nicht vernachlässigt werden, da es keinen perfekten Schutz und keine Garantien geben kann, dass nicht trotz aller Bemühungen der ein oder andere IT-Sicherheitsvorfall eintritt.

Eine Maßnahmenbeschreibung folgt einer einheitlichen, kompakten Struktur: Nach einer einleitenden Kurzbeschreibung, die darlegt, welche fachlichen Ziele die Maßnahme verfolgt, werden die typischen Zuständigkeiten für die Umsetzung und die Genehmigung der Maßnahme sowie die jeweils an ihr Beteiligten in einer Tabelle dargestellt. Rollenbezeichnungen, wie beispielsweise die Geschäftsführung und die IT-Abteilung, sollten dabei spezifisch für die eigene Umgebung konkretisiert und präzisiert werden. Darauf folgt die Erläuterung zur Umsetzung der Maßnahme, wobei im Regelfall mehrere Phasen und damit implizit eine Reihenfolge der Handlungsschritte vorgesehen sind. Teilweise werden, insbesondere bei den technischen Maßnahmen, exemplarische Software-Werkzeuge genannt, die bei der Umsetzung unterstützen können. Hier haben wir uns, soweit möglich, auf kostenfrei nutzbare Open-Source-Software beschränkt. Diese Beispiele sind nicht als Ersatz für eigene Recherchen und Auswahlprozesse gedacht, sondern sollen es Ihnen ermöglichen, sich vor der Entscheidung für ein konkretes Produkt ohne allzu großen Aufwand näher mit der Materie zu beschäftigen und fundierte Vergleiche zwischen der Leistungsfähigkeit durchzuführen. Am Ende jeder Maßnahmenbeschreibung finden sich Referenzen auf die korrespondierenden Abschnitte von Standards und anderen Dokumenten; diese können zur Vertiefung herangezogen werden und sind insbesondere dann relevant, wenn eine Auditierung, ggf. mit dem Ziel einer Zertifizierung oder eines anderen formellen Nachweises der umgesetzten IT-Sicherheitsmaßnahmen, geplant ist.

Die neu hinzugekommenen Vorlagen für Dokumente des Informationssicherheitsmanagements sind ebenfalls einfach zu bearbeiten. Gelb markierte Textpassagen und Inhalte dienen als Kennzeichnung für von den Krankenhäusern selbst vorzunehmende notwendige Anpassungen. Soweit möglich, sollen die entsprechenden Hinweise Sie bei den Anpassungen unterstützen. Auch hier haben wir auf weiterführende Quellen verwiesen. Die einzelnen Dokumente liegen in gängigen Dokumenten-Formaten vor, die ebenfalls über kostenlose Open-Source-Software bearbeitet werden können. Die Dateien können von der Projekt-Website `https://www.unibw.de/code/smart-hospitals` kostenlos und ohne Registrierung heruntergeladen werden. Auf passende Vorlagen wird einerseits direkt aus den Maßnahmen selbst heraus verwiesen, andererseits bietet Anhang A.1 ein Reifegradmodell für Dokumente des Informationssicherheitsmanagements, das in Abstimmung mit Krankenhäusern eine mögliche sinnvolle Reihenfolge und Übersicht bietet.

Somit ist dieser Maßnahmenkatalog nicht notwendigerweise von vorne nach hinten zu lesen und abzuarbeiten; vielmehr sollte die Modularität genutzt werden, um auf Basis eigener Überlegungen zu relevanten Bedrohungen und Herausforderungen gezielt die dazu passenden Maßnahmen herauszusuchen.

1.2 Einordnung der behandelten Maßnahmen und Neuerungen

Abbildung 1.1 zeigt anhand der Kategorien für Sicherheitsmaßnahmen der internationalen Norm ISO/IEC 27001, welche Themenbereiche durch den vorliegenden Maßnahmenkatalog bereits adressiert werden. Mit dem Maßnahmenkatalog streben wir dabei keine vollständige Abdeckung angestrebt, da bestehende Ansätze nicht ersetzt oder wiederholt werden sollen, sondern er zielt vielmehr auf einen gelungenen Einstieg in den jeweiligen Themenkomplex ab.

Das Landesamt für Sicherheit in der Informationstechnik (LSI) hat parallel die Orientierungshilfe „IT-Sicherheit in Kliniken“ entwickelt und mit dem vorliegenden Maßnahmenkatalog abgestimmt. Die LSI-Orientierungshilfe bietet einen kompakten Überblick zu den genannten und weiteren IT-Sicherheitsmaßnahmen in Form prägnanter Beschreibungen sowie Orientierungsfragen zu deren Umsetzung. Ein Vorgehensmodell in Form eines Stufenplans ist ebenfalls enthalten.

Die LSI-Orientierungshilfe erhalten Sie per E-Mail-Anfrage an beratung-kritis@lsi.bayern.de.

In der zweiten Version dieses Maßnahmenkatalogs wurden basierend auf den Anregungen durch Nutzer der ersten Version die folgenden neuen Themen und Inhalte integriert:

- Das Thema „Krankenhäuser und Cloud-Dienste“ wird in Kapitel 7.6 behandelt und enthält einen Überblick über technische und rechtliche Aspekte, die beim sicheren Einsatz von externen Cloud-Diensten notwendig sind.
- Das neue Kapitel 9 „Datenschutz und rechtliche Konformität“ enthält sowohl Maßnahmen, die einen Überblick über einige datenschutzrelevante Themen (Datenverarbeitung, Datenschutzmanagement usw.) geben, als auch eine Zusammenfassung der rechtlichen Anforderungen beim Einsatz von Bring Your Own Device (BYOD), Telearbeit, externen Dienstleistern und beim datenschutzkonformen Informationsaustausch im Krankenhaus.
- Diverse Maßnahmen empfehlen die Dokumentation und Erstellung von Sicherheitsrichtlinien, Sicherheitsvorfällen etc. Dazu wurden Vorlagen erarbeitet, die Ihnen eine Grundlage für die Erstellung eigener Dokumente liefern. Sie finden die Vorlagen im Anhang A des Maßnahmenkatalogs und zum Download auf unserer Webseite.

Für Anregungen zu den Inhalten per E-Mail an die Adresse projekt-smarthospitals@unibw.de sind wir Ihnen dankbar.

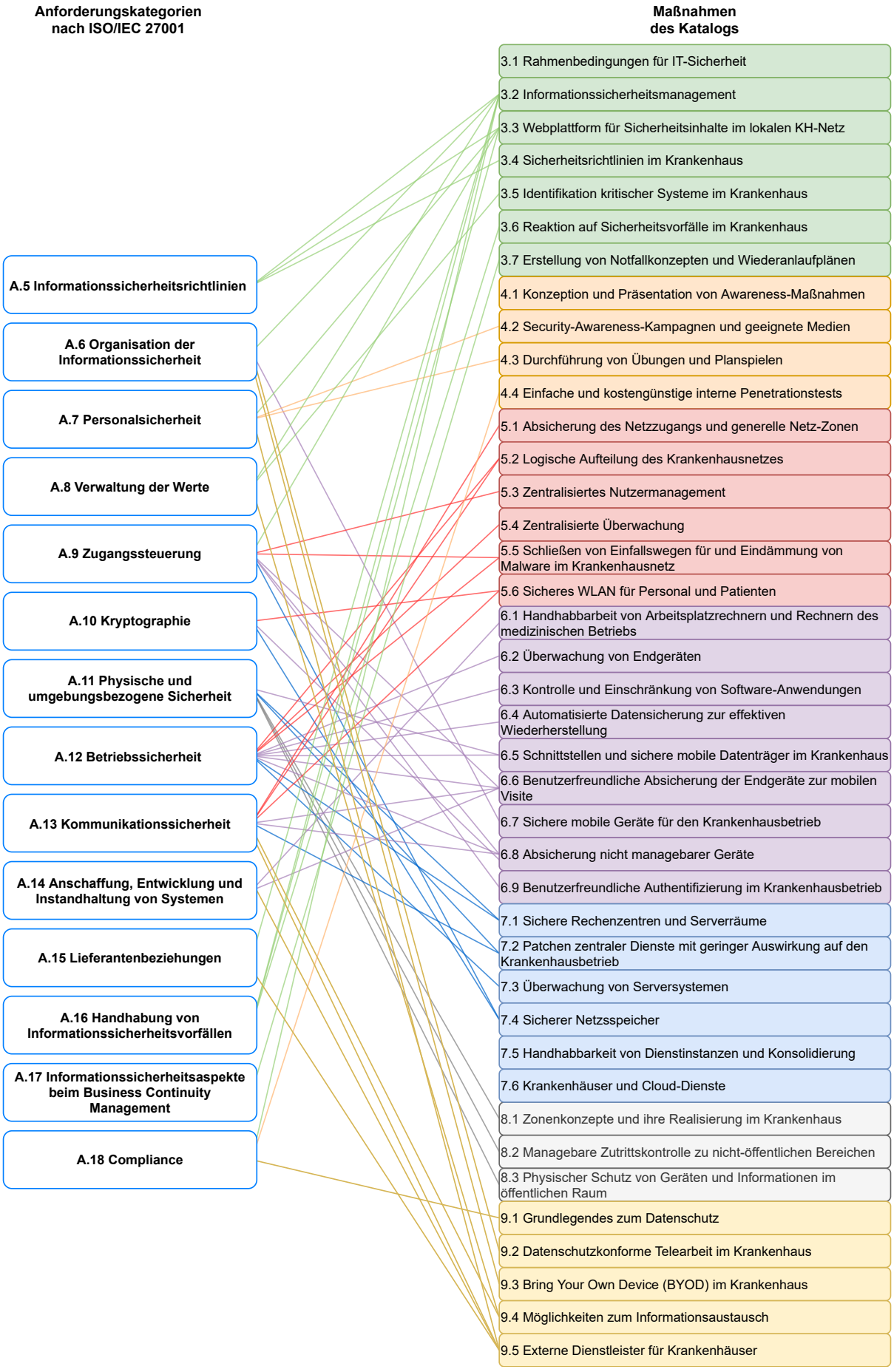


Abbildung 1.1: Abbildung der ISO/IEC 27001-Anforderungskategorien auf Maßnahmen dieses Katalogs

Kapitel 2

Exemplarische IT-Infrastruktur im Krankenhaus

Jedes Krankenhaus ist trotz Gemeinsamkeiten in der Struktur und Organisation unterschiedlich aufgebaut. In Abbildung 2.1 (folgende Seite) ist dennoch grob skizziert, wie die IT-Infrastruktur in einem Krankenhaus gestaltet ist. Unser Modell-Krankenhaus dient uns als Beispiel bei den Beschreibungen der Maßnahmen. Es ist zwar fiktiv, aber sein Konzept berücksichtigt alle gängigen Strukturen.

Ein Krankenhaus kann aus **einem** oder auch aus **mehreren Standorten** bestehen, entweder im Rahmen eines Krankenhausverbundes oder durch die Verteilung auf mehrere Gebäude, zum Beispiel innerhalb einer Stadt. Oft sind verteilte Standorte zum Datenaustausch und zur gemeinsamen Dienstnutzung miteinander verbunden. In der Regel sind in einem Krankenhaus mindestens drei Bereiche zu finden, durch deren Zusammenarbeit die verschiedenen Dienste erbracht werden können: der **medizinische Bereich**, der **Verwaltungsbereich** und der **technische Bereich**. Dabei stellt der technische Bereich (evtl. unterstützt durch externe Dienstleister) den anderen Bereichen IT-Infrastruktur und IT-Dienstleistungen zur Verfügung, auf die sie angewiesen sind. Dazu zählt beispielsweise der grundlegende Dienst **Netz** und **Netzinfrastruktur**, d. h. die Bereitstellung, Wartung und Pflege von Netzkomponenten wie Switches und Routern, durch welche Client- und Server-Systeme in einem gemeinsamen lokalen Netz verbunden sind. In der Verwaltung kommen üblicherweise klassische **Arbeitsplatzrechner** und Infrastruktur zum Einsatz: Notebooks, Desktop-PCs und Drucker. Im medizinischen Bereich sind Arbeitsplatzrechner in ähnlicher Weise im Einsatz, beispielsweise zur Patienten- und Behandlungsdokumentation. Gleichzeitig werden auch hier **mobile Geräte** immer häufiger genutzt, beispielsweise in der mobilen Visite oder in Rettungswagen. Jedoch sind im medizinischen Bereich auch spezialisierte **(Groß-)Geräte**, wie MRT- und Röntgen-Geräte, an das Krankenhausnetz angeschlossen. Der moderne effiziente Krankenhausbetrieb ist jedoch auch schon länger auf **zentrale Dienste** angewiesen, welche durch den technischen Bereich bereitgestellt werden. Dazu zählen spezielle domänenspezifische Anwendungen, wie ein **Krankenhaus-** oder **Laborinformationssystem** (KIS/LIS) und **Picture Archiving and Communication Systems** (PACS) zur Verwaltung von medizinischem Bildmaterial, sowie auch klassische IT-Dienste.

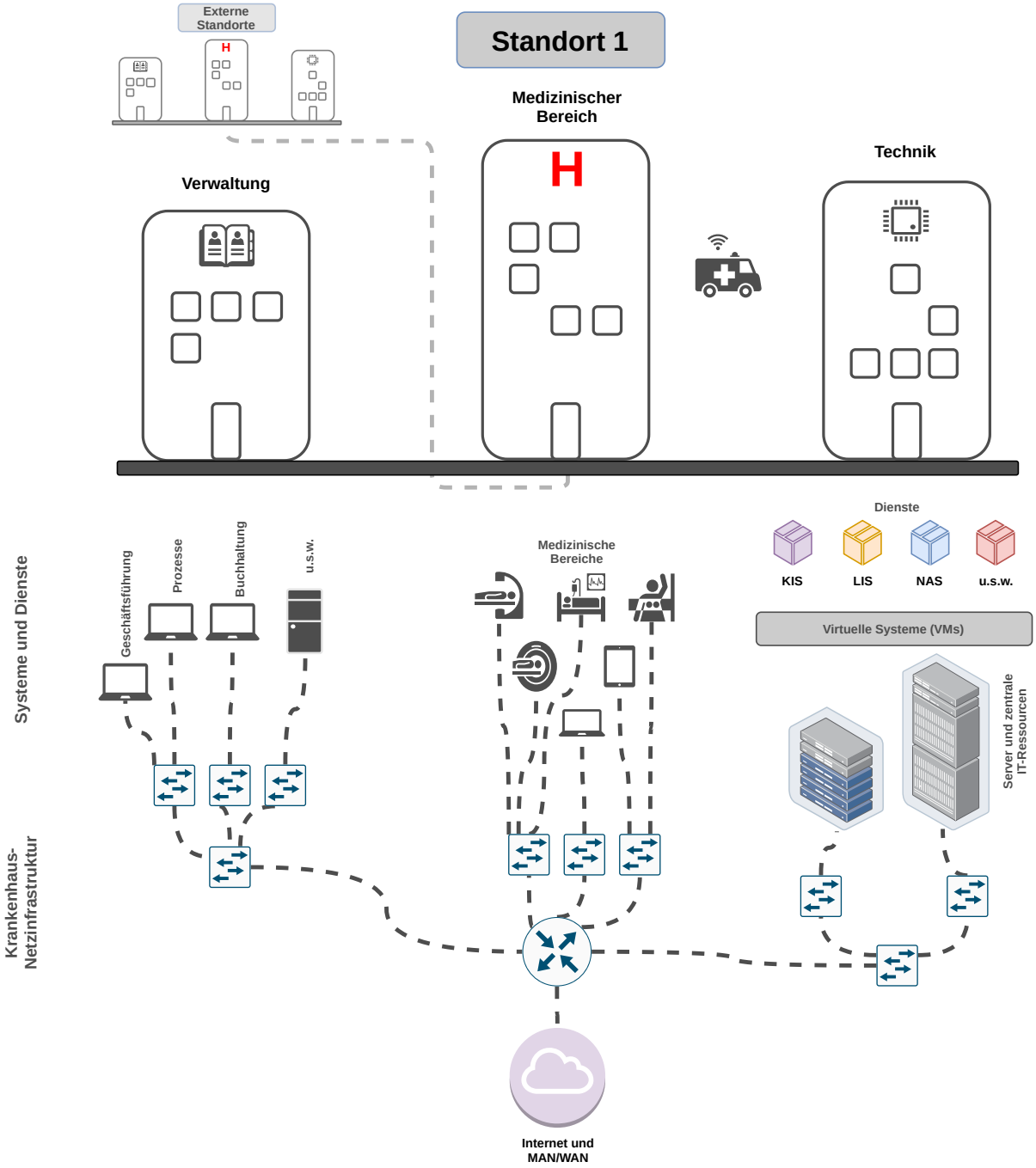


Abbildung 2.1: Vereinfachte Darstellung einer IT-Infrastruktur im Krankenhaus

Kapitel 3

Organisatorische Aspekte der Informationssicherheit

Im Informationssicherheitsmanagement bilden organisatorische Maßnahmen eine wesentliche Säule des Schutzes von Systemen und Daten. Hier geht es darum, eine Sicherheitskultur aufzubauen mit organisatorischen Strukturen wie Sicherheitszielen, notwendigen Prozessen, Dokumenten, Verhaltensweisen, Kommunikationswegen, Rollen und Gruppen, sowie auch eine Sicherheitskultur für Aufgaben und Zuständigkeiten. Die Strukturen sollten regelmäßig aktualisiert und an sich neu ergebende Umstände angepasst werden. Wesentliche Einzelmaßnahmen dafür sind im Rahmen dieses Kapitels sinnvoll aufeinander aufbauend angeordnet. Es sollten

- Rahmenbedingungen für Informationssicherheit geschaffen,
- grundlegende Elemente im organisatorischen Sicherheitsmanagement umgesetzt,
- eine grundlegende technische Infrastruktur für die Organisation aufgebaut,
- krankenhausweite einheitliche Verhaltensweisen festgelegt,
- essenzielle Prozesse, Dienste und Systeme im eigenen Krankenhausbetrieb identifiziert,
- ein Konzept zur Behandlung von (in der Realität praktisch unvermeidbaren) Sicherheitsvorfällen erstellt
- und schließlich auch für Notfälle geplant werden.

Die Maßnahmen in diesem Kapitel richten sich vor allem an die Geschäftsführung und die Entscheidungsträger eines Krankenhauses.

3.1 Rahmenbedingungen für IT-Sicherheitsmanagement ■

Abbildung 3.1: Bausteine einer Sicherheitskultur im Krankenhaus

Kurzbeschreibung

*Aus organisatorischer Sicht ist es von großer Bedeutung, dass die Rahmenbedingungen für das IT-Sicherheitsmanagement im Krankenhaus gut im Alltag umsetzbar gestaltet sind. In vielen Krankenhäusern sind diese Bedingungen bereits (explizit gewollt oder mit der Zeit etabliert) gegeben. In dieser Maßnahme werden die auf Basis der für diesen Katalog vorgelagerten durchgeführten Datenerhebung gesammelten wichtigsten Punkte dazu genannt. Die Maßnahme **richtet sich explizit an die Geschäftsführung** in Krankenhäusern.*

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung	•		
IT-Abteilung			•
Personal/Nutzer			•

Die Gestaltung und Umsetzung geeigneter Rahmenbedingungen für das IT-Sicherheitsmanagement sollte die Geschäftsführung selbst definieren und realisieren. Sämtliche involvierten Gruppen sollten sowohl mit geeigneten Vertretern als auch gesamt mit einbezogen werden: Die IT-Abteilung als Instanz zur Planung und Schaffung von IT-Sicherheitsmanagement sowie das gesamte Personal als von den Maßnahmen berührte Nutzer.

Umsetzung der Maßnahme

Folgende Punkte müssen in einem Krankenhaus gegeben sein, damit die Umsetzung des IT-Sicherheitsmanagements gut funktionieren kann.

Bewusstsein bei der Geschäftsführung

Zunächst muss die Geschäftsführung selbst ein Bewusstsein für den unbedingten **Bedarf an IT-Sicherheit** entwickeln. Dazu gehört die Erkenntnis, dass der Digitalisierungsprozess in Krankenhäusern zahlreiche neue **Gefahren** mit sich bringt, die in unterschiedlichster Weise Schaden nach sich ziehen können, beispielsweise ein finanzieller Schaden oder ein Reputationsverlust. Ein langfristiger Ausfall von IT-Diensten oder das Ausspähen von sensiblen Patientendaten zieht beispielsweise oft beides nach sich.

Die Geschäftsführung sollte deshalb den Willen zur **Etablierung einer Sicherheitskultur** haben und die Umsetzung, wann immer möglich, optimal unterstützen.

Eine geeignete Organisationsstruktur

Es muss eine geeignete Organisationsstruktur vorhanden sein, die die Umsetzung von IT-Sicherheit unterstützt. Dazu gehört beispielsweise die Einrichtung einer **Stabsstelle** für IT-Sicherheit nahe der Geschäftsführung oder die Einführung von regelmäßigen Personalgruppen-übergreifenden **Gremien und Jours Fixes**. Die Umsetzung der Organisationsstruktur wird insbesondere auch in Maßnahme 3.2 Informationssicherheitsmanagement ■ erläutert. Die Geschäftsführung ist bei der Umsetzung maßgeblich gefordert.

Anerkennung bei Personal/Nutzern

Im medizinischen Alltag und Betrieb werden IT-Sicherheit und damit verbundene Maßnahmen vom medizinischen Personal oft als hinderlich empfunden. Auch wenn die medizinische Versorgung der Patienten im Krankenhaus die höchste Priorität hat, muss dem medizinischen Personal bewusst sein, dass der medizinische Betrieb **stark abhängig** von IT-Diensten und -Infrastruktur ist und die Expertise dieser Systeme in der Regel bei der IT-Abteilung des Krankenhauses liegt. Ein nach wie vor im Bewusstsein einiger Ärzte etabliertes **Hierarchiegefälle** zwischen medizinischem Personal und administrativem Personal erschwert die Umsetzung von Sicherheitsmaßnahmen oft enorm.

Die Geschäftsführung sollte sich deshalb entsprechend auch um die **Anerkennung der Kompetenz** des IT-Personals in Sachen IT-Infrastruktur und IT-Sicherheit beim medizinischen und dem weiteren administrativen Personal bemühen.

Freiheitsgrade

Zu dem vorangegangenen Punkt zählt auch, dass der IT-Abteilung im Krankenhaus **ausreichende Freiheiten**

bei der Umsetzung von Sicherheitsmaßnahmen zugestanden werden. Die IT-Abteilung kann selbst dazu beitragen, indem sie sich an einem geeigneten Kompromiss zwischen **Sicherheit**, **Fortschritt** sowie **Nutzerfreundlichkeit** orientiert. Ein häufig im Sicherheitsmanagement auftretendes Problem ist die Ablehnung von als zu einschränkend empfundenen Sicherheitsmaßnahmen durch die eigentlichen Nutzer. In solchen Fällen haben Sicherheitsmaßnahmen, auch wenn ihr Gedanke noch so sinnvoll und wichtig ist, ihren Zweck verfehlt, da sie dann seltener eingehalten werden.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 1 (Geschäftsführung/Leitung), 2 (Beauftragter für Informationssicherheit)

3.2 Informationssicherheitsmanagement ■

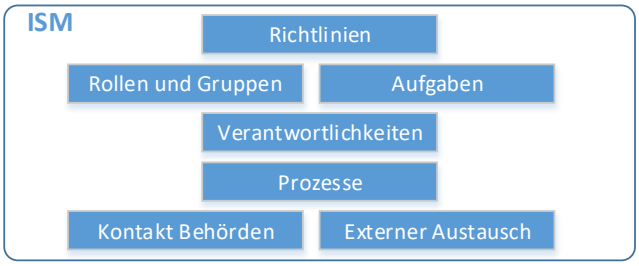


Abbildung 3.2: Elemente im Sicherheitsmanagement

Kurzbeschreibung

Informationssicherheitsmanagement (ISM) bildet die grundlegende organisatorische Basis, um Sicherheit im Betrieb zu koordinieren. Es legt vor allem Rollen, Aufgaben, klare Verantwortlichkeiten, Abläufe und den Geltungsbereich fest.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung	•	•	
IT-Abteilung	•		
Personal/Nutzer			•

Das Einbeziehen von Vertretern des Personals bei der Planung von Sicherheitsmaßnahmen erhöht die Nutzerakzeptanz.

Umsetzung der Maßnahme

Die Organisation von ISM ist auch im kleinen Stil machbar. Zunächst geht es vor allem darum, wichtige Überzeugungen, Strukturen und Prozesse **niederzuschreiben**, um das Einvernehmen mit den Richtlinien und Maßnahmen zur Sicherheit und ihre Gültigkeit zu fixieren. Eine geeignete Vorgehensweise zum Aufbau der Organisation kann wie folgt gestaltet sein:

Zunächst sollte ein designierter **Informationssicherheitsbeauftragter** berufen werden. Die jeweilige Person sollte sich mit IT-Sicherheit, der IT-Umgebung und den Abläufen im Krankenhaus bereits gut auskennen. In manchen Krankenhäusern hat es sich bewährt, die Stelle als **Stabsstelle** nahe der Geschäftsführung einzurichten.

Die Planung der Organisation sollte anhand einer **Informationssicherheitsleitlinie** erarbeitet und durch sie kommuniziert werden. Dazu kann die Vorlage aus Anhang A.2 genutzt werden.

Die Informationssicherheitsleitlinie muss dem **Personal zugänglich** sein (vergleiche auch Maßnahme 3.3 Webplattform für Sicherheitsinhalte im lokalen Krankenhausnetz ■) und aktiv kommuniziert werden. Bei Veröffentlichung müssen interne Informationen entfernt werden.

Neben Einzelrollen in der Organisation von ISM sollten auch personalgruppenübergreifende Arbeitskreise, z. B. ein **Arbeitskreis Security**, gebildet werden, vor allem mit erfahrenen und anerkannten Vertretern der Ärzteschaft, Pflege und Geschäftsführung. Die Ärzteschaft und die Pflege ist durch Security-Maßnahmen oft am stärksten im Betrieb betroffen. Sie sollten unbedingt mit einbezogen werden, da ihre Akzeptanz der Maßnahmen für eine gut funktionierende Umsetzung in ihren Bereichen wichtig ist. Die übergreifenden Arbeitskreise sollten sich regelmäßig, z. B. im zwei- bis dreiwöchigen Rhythmus, treffen und vor allem auch Alltagsprobleme durch Security-Maßnahmen thematisieren. Die wichtigsten Themen, Erkenntnisse und Beschlüsse der Treffen müssen **dokumentiert** werden, um in der Praxis bindend zu werden.

Sobald organisatorische Strukturen (Rollen, Gruppen, Verantwortlichkeiten, Leitlinie) existieren und dokumentiert sind, sollten auch wichtige Prozesse definiert und dokumentiert werden. Sie dienen dazu, Abläufe zu standardisieren und Fehler zu vermeiden. Auch helfen sie dabei, durch gute Dokumentation Zeit zu sparen, beispielsweise beim Einlernen neuer Mitarbeiter. Die Prozesse müssen keinesfalls alle security-bezogen sein. Wunddokumentation, Patienten-Überweisungen oder -Entlassungen, usw. sollten ebenfalls dokumentiert werden.

Neben organisatorischen Strukturen sollten die Dokumentationen auch IT-Ressourcen und -Strukturen erfassen. Dazu zählt beispielsweise eine **Netz-Dokumentation** (Netze und Netzkomponenten), die als wichtige Grundlage für viele Entscheidungen notwendig ist.

Unter Umständen ist es notwendig, externe Kontakte herzustellen, zum Beispiel mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Meldung von Vorfällen.[1] Eine Übersicht zu Meldepflichten ist ebenfalls im B3S-KH in Kapitel 7.3 beschrieben. Auch externe Arbeitskreise, beispielsweise von KIS-Anwendern oder Security-AKs, sollten zum Austausch von Maßnahmen und Ideen genutzt werden.

[1] https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/DigitaleDienste/Meldungen/meldungen_node.html

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 1 (Geschäftsführung/Leitung), 2 (Beauftragter für Informationssicherheit), 4 (Prozess-/Anwendungsverantwortlicher), 15 (Interne Kommunikation), 16 (Externe Informationsversorgung und Kommunikation)
- **B3S im Krankenhaus** – Kap. 5.2 (Ergänzende Regelungen zum Geltungsbereich), Kap. 7.2 (Organisation der Informationssicherheit), Kap. 7.3 (Meldepflichten), Kap. 7.5 (Asset Management), Kap. 7.9 (Vorfallerkennung und Behandlung)
- **ISO/IEC 27001** – Maßnahmenziele A.5 (Informationssicherheitsrichtlinien), A.6 (Interne Organisation), A.8 (Verwaltung der Werte), A.15 (Lieferantenbeziehungen), A.16 (Handhabung von Informationssicherheitsvorfällen), A.18 (Compliance)
- **BSI IT-Grundschutz-Kompendium** – ISMS.1 (Sicherheitsmanagement), ORP.1 (Organisation und Planung)

3.3 Webplattform für Sicherheitsinhalte im lokalen Krankenhausnetz

Kurzbeschreibung

*Informationsaustausch ist eine Schlüsselkomponente im Sicherheitsmanagement. Ein sehr nützliches Werkzeug bildet hier eine für alle Mitarbeiter via Webbrowser erreichbare zentrale Webplattform, die im lokalen Krankenhausnetz liegt. Auf ihr sollten alle öffentlichen wichtigen **Dokumente** (Leit- und Richtlinien), aktuelle **Meldungen** (Sicherheitsprobleme), **Termine und Ereignisse** (z. B. anstehende Schulungen und Umfragen) und **Funktionen** (Störungsmeldungen durch Mitarbeiter) angeboten werden.*

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	•
IT-Abteilung	•		
Personal/Nutzer			•

Diese technische Basis der Organisation wird durch die IT aufgesetzt. Die Geschäftsführung sollte unbedingt eingebunden werden und die Plattform unterstützen, aber auch genehmigen. Alle Mitarbeiter sollten zur Nutzung angeregt und motiviert werden.

Umsetzung der Maßnahme

Die Umsetzung dieser Maßnahme ist praktisch immer möglich. Je nach investiertem Aufwand kann eine derartige Plattform unterschiedliche Darstellungsformen haben. Die folgenden Formen (und möglicherweise weitere) sind denkbar; der erwartete Aufwand zur Umsetzung ist aufsteigend gemäß der Reihenfolge:

1. **Einfach informativ/verweisend**: In diesem Fall wird eine Website als zentrale Anlaufstelle für Mitarbeiter eingerichtet, die schlichtweg strukturiert auf die anderen Dienste (z. B. URLs einzelner Dokumente in einer Dateiablage, Zugang Ticketsystem, „Aktuelles"-Website des Krankenhauses) verweist. Die Einrichtung einer Plattform in dieser Form ist in der Regel mit wenig Aufwand verbunden, bringt den Mitarbeitern aber deutlich mehr Übersichtlichkeit.

2. **Teilintegriert**: In dieser Variante gibt es ebenfalls die auf andere Dienste verweisenden Links. Ausgewählte Inhalte und Funktionen werden aber direkt auf der Website integriert. Beispielsweise einzelne Meldungen der „Aktuelles"-Website oder Funktionen zu Umfragen, Kalender, usw.

3. **Vollintegriert**: Bei der Vollintegration gibt es praktisch keine Verweise mehr auf andere Dienste. Nutzer können direkt auf der Seite z. B. ein Störungsticket anlegen, das automatisch generiert wird, alle Dokumente der IT-Sicherheit (und ähnliches) herunterladen, usw. Eine Vollintegration ist üblicherweise am aufwendigsten, bietet Mitarbeitern aber ein für ihre Zwecke optimiertes Portal.

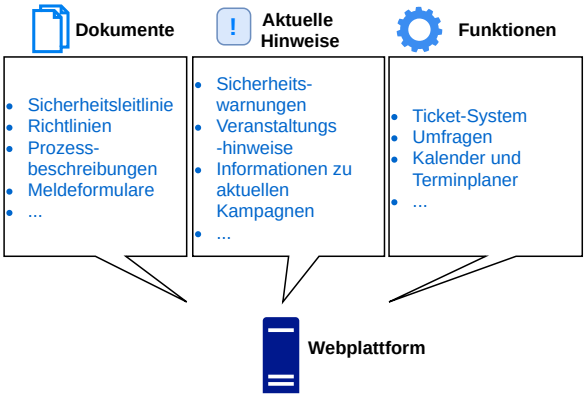


Abbildung 3.3: Beispielelemente einer zentralen Webplattform

Bestehende Kollaborationsplattformen, wie **OwnCloud**[2] oder **Nextcloud**,[3] können für den Anfang als einfach nutzbare Webplattformen intern installiert und für diesen Zweck genutzt werden.

Unabhängig von der Umsetzung müssen einige technische Sicherheitsvorkehrungen getroffen werden, um Missbrauch zu verhindern und Datenschutz zu gewährleisten. Die wichtigsten sind,

- stets auf allen Seiten und Diensten eine TLS-abgesicherte Kommunikation zu nutzen (HTTPS),
- eine Einzelnutzer-Authentifizierung (keine Sammelkennungen) vorzuschalten (im Idealfall über eine netzweite Kennung via z. B. Active-Directory- oder LDAP-Anbindung; vgl. Maßnahme 5.3 Zentralisiertes Nutzermanagement) und
- die Beschränkung der Zugreifbarkeit nur auf das Mitarbeiternetz (vgl. Maßnahme 5.2 Logische Aufteilung des Krankenhausnetzes).

[2] https://owncloud.org/
[3] https://nextcloud.com/

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 1 (Geschäftsführung/Leitung), 13 (Personelle und organisatorische Sicherheit), 15 (Interne Kommunikation)
- **B3S im Krankenhaus** – ANF-MN 67 (Meldepflicht der Mitarbeiter bei Vorfällen)
- **ISO/IEC 27001** – Maßnahmenziele A.5.1 (Vorgaben der Leitung für Informationssicherheit), A.7.2.2 (Informationssicherheitsbewusstsein, -ausbildung und -schulung), A.9 (Zugangssteuerung), A16.1.{2,3} (Meldung von Informationssicherheitsereignissen/Schwächen)
- **BSI IT-Grundschutz-Kompendium** – ISMS.1 (Sicherheitsmanagement)

3.4 Sicherheitsrichtlinien im Krankenhaus

Kurzbeschreibung

*Sicherheitsrichtlinien sind ein wichtiges Mittel des Sicherheitsbeauftragten und der Geschäftsführung, um sichere Konfigurationen von **Systemen** und sicherheitsrelevante **Verhaltensweisen** von Mitarbeitern vorzugeben. In Krankenhäusern bildet der medizinische Betrieb allerdings eine besondere Herausforderung, da Sicherheitsrichtlinien die Abläufe nicht stören oder gar behindern dürfen. Deshalb sind in einigen Fällen Kompromisslösungen notwendig.*

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			•

Vertreter der Ärzteschaft und Pflege sollten bezüglich der Auswirkung von Sicherheitsrichtlinien auf den medizinischen Betrieb befragt werden oder von sich aus Feedback geben.

Umsetzung der Maßnahme

Klassische Sicherheitsrichtlinien sollen das **Verhalten** des Personals bzw. der Nutzer beeinflussen (z. B. Clean-Desk-Policy, Handhabung von Spam- und Phishing-E-Mails oder Home-Office-Richtlinien), können jedoch teilweise auch **technisch forciert** werden (z. B. automatische Bildschirmsperren, Qualität gewählter Passwörter, usw.).

Die Auswahl wichtiger Sicherheitsrichtlinien im Krankenhaus unterscheidet sich dabei nicht wesentlich von anderen Unternehmensformen. Im Krankenhaus ist jedoch die Festlegung von **Geltungsbereichen für Sicherheitskriterien** deutlich wichtiger, damit der medizinische Betrieb nicht negativ beeinflusst wird und Nutzer die Sicherheitsmaßnahmen nicht als Ärgernis empfinden.

Eine Auswahl grundlegender Sicherheitsrichtlinien, die auch im Krankenhaus unbedingt Einsatz finden sollten, sind in den folgenden Abschnitten beschrieben. Weitere können entsprechend den Anforderungen im jeweiligen Krankenhaus zusätzlich umgesetzt werden.

Passwort-Richtlinie

Passwörter müssen im Krankenhaus den gleichen Kriterien und Empfehlungen folgen wie in jeder anderen Umgebung, sei es privat oder geschäftlich. Sie sollten **sehr heterogen** (inklusive Sonderzeichen und Ziffern) und relativ **lang** sein. Das BSI bietet zu diesem Thema eine gute Übersicht an,[4] auch zur Auswahl gut merkbarer Passwörter. Das **Wiederverwenden** gleicher Passwörter für unterschiedliche Dienste muss möglichst **unterbunden** werden.

Die Passwortstärke kann technisch üblicherweise gut forciert werden. Generell ist es – falls anwendbar – zudem sehr empfehlenswert, einen **Passwortmanager** für die Nutzer einzuführen. Der Gültigkeitsbereich der Anforderung muss sich auf das gesamte Krankenhaus erstrecken.

Eine Vorschrift zur regelmäßigen **Änderung von Passwörtern** wurde bis vor kurzem (auf Empfehlung unter anderem vom BSI) oft als Zusatz in die Passwort-Richtlinie aufgenommen. Inzwischen wird das jedoch eher als **kontraproduktiv** angesehen, da dies Nutzer tendenziell dazu verleitet, schwächere Passwörter zu wählen. Generell verdeutlicht dieses Beispiel gut, dass Sicherheit nur durch einen annehmbaren Kompromiss in Verbindung mit Nutzerfreundlichkeit erreicht werden kann.

Individueller Login

Eine mit der Passwort-Richtlinie verbundene Sicherheitsrichtlinie ist die eines **individuellen Logins**. Zugunsten einer **eindeutigen Zuweisbarkeit** von Aufgaben und der damit verbundenen **Rechtevergabe** bzgl. IT-Diensten und IT-Inhalten müssen sogenannte *Gruppen- oder Sammel-Logins* unterbunden werden. Jeder Nutzer muss sich über seine individuelle Kennung authentifizieren können, wenn er sich an einem Rechner anmeldet.

Auch diese Richtlinie sollte weitestgehend krankenhausweit eingesetzt werden. In Einzelfällen können Ausnahmen (z. B. funktionaler Login für ein medizinisches Gerät) definiert werden.

Clean-Desk-Policy

Eine Clean-Desk-Policy sagt in der Regel aus, dass **keine** (vor allem vertraulichen) **Dokumente** und andere Informationsquellen für Dritte einsehbar herumliegen dürfen. Deshalb müssen Schreibtische und auch die Desktop-Ansicht eines Arbeitsplatzrechners insbesondere bei Abwesenheit immer aufgeräumt bzw. leer sein, damit unberechtigte Personen keinen Zugriff auf vertrauliche Informationen haben. Beispielsweise muss die Akte des vorherigen behandelten Patienten immer weggeräumt sein, bevor der nächste Patient das Behandlungszimmer betritt.

Hier kann der Geltungsbereich auch **eingeschränkter** sein. Er muss aber in jedem Fall in Räumen umgesetzt werden, die von unbefugten Personen, Patienten und Gästen möglicherweise betreten werden können. Gesondert abgesicherte Räume mit klar definierten Zu-

[4] https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html

gangsberechtigten können beispielsweise einfach mit dieser Richtlinie umgehen.

Bildschirmsperren

Einen ergänzenden Teil der vorherigen Richtlinie bildet die Richtlinie für automatische Bildschirmsperren. Da ungenutzte und unbeaufsichtigte PCs vor unberechtigtem Zugriff auf das System und die Inhalte geschützt werden müssen, sollten sie mit **passwortgesicherten Bildschirmschonern** ausgestattet sein.

Hier gilt es, für die unterschiedlichen Geltungsbereiche die jeweils passende Konfiguration einzurichten. Beispielsweise sind Bildschirmsperren im **OP-Bereich** nicht nur störend, sondern können auch den medizinischen Betrieb **stark behindern**. In Bereichen mit viel Durchgangsverkehr hingegen, wie zum Beispiel am Empfang, müssen Bildschirmsperren relativ schnell, d. h. in Minuten, automatisch aktiviert werden.

Handhabung von Phishing-E-Mails

Spam- und Phishing-E-Mails zählen nicht nur in einem Krankenhaus zu den größten Einfallstoren für Malware (vgl. Maßnahme 5.5). Entsprechend muss dem Nutzer neben Schulungen und anderen Awareness-Maßnahmen (insbesondere hinsichtlich Phishing-Erkennung) auch mittels Richtlinien die Handhabung von bösartigen E-Mails vorgegeben werden. **Private E-Mails sollten von Nutzern niemals auf einem Arbeitsplatzrechner** abgerufen werden, zumal zentral installierte Filter- und Anti-Viren-Software im Krankenhaus auf diese keinen Zugriff hat.

Bei Unsicherheit oder einer eindeutig erkannten Phishing-Mail sollte sich der Nutzer sofort an die Krankenhaus-IT wenden. Die IT-Abteilung kann die Gefahr einschätzen und entsprechend reagieren, zum Beispiel mit hausinternen E-Mails zur Warnung vor diesen Fällen oder auch, indem sie die Filter des E-Mail-Systems anpasst.

Die Richtlinie betrifft alle E-Mail-Nutzer im Krankenhaus.

Nutzung von Wechseldatenträgern

Ein weiteres Einfallstor für Malware sind fremde Wechseldatenträger, wie externe Festplatten und USB-Sticks. Deren Verwendung sollte im Krankenhaus generell verboten sein. Die Maßnahme kann auf vielen Geräten technisch forciert werden, indem der USB-Zugriff für krankenhausfremde USB-Sticks unterbunden wird. Es gibt entsprechende Lösungen, wie zum Beispiel, nur vom Krankenhaus selbst ausgegebene, verschlüsselte USB-Sticks zuzulassen.

Generell sollten auch hier keine Ausnahmen gemacht werden. Begründete Einzelfall-Ausnahmen können diskutiert und ggf. mit technischen Lösungen unterstützt werden – wie zum Beispiel, für die Verwendung externer Wechseldatenträger einen extra für diese Fälle abgesicherten und vom Krankenhausnetz generell abgetrennten Rechner bereitzustellen.

Vorlagen

Eine Vorlage für interne Sicherheitsrichtlinien liegt diesem Katalog in Anhang A.4 bei.

- **SANS Institut** – Eine Vielzahl an Vorlagen für unterschiedlichste Richtlinien (Englisch), unter https://www.sans.org/security-resources/policies/.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 13 (Personelle und organisatorische Sicherheit), 22 (Schutz vor Schadsoftware), 24 (Identitäts- und Rechtemanagement), 25 (Sichere Authentisierung), 32 (Umgang mit Datenträgern, Austausch von Datenträgern)
- **B3S im Krankenhaus** – Kap. 7.1 (Informationssicherheitsmanagementsystem)
- **ISO/IEC 27001** – Maßnahmenziele A.5 (Informationssicherheitsrichtlinien)

3.5 Identifikation kritischer Systeme im Krankenhaus

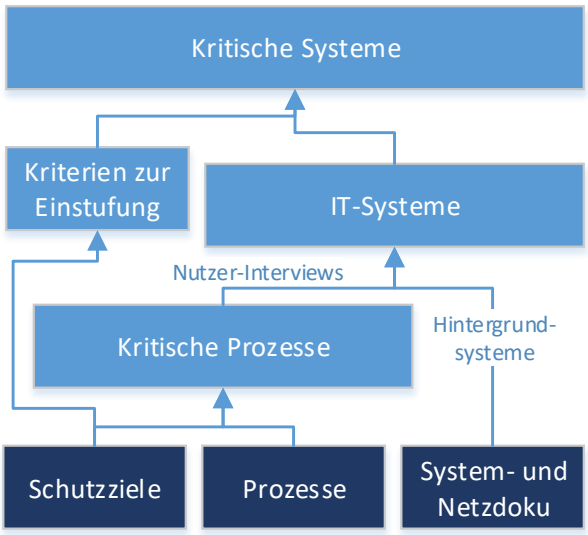


Abbildung 3.4: Voraussetzung und Schritte zur Identifikation kritischer Systeme

Kurzbeschreibung

Eine Dokumentation und Bewertung der Systeme und Schnittstellen im Krankenhaus bildet eine zentrale, essentielle Ausgangsbasis für viele weitere Maßnahmen, wie in 5.2 Logische Aufteilung des Krankenhausnetzes oder auch in 5.5 Schließen von Einfallswegen für und Eindämmung von Malware im Krankenhausnetz. Das BSI bietet eine detaillierte Anleitung für eine geeignete Vorgehensweise mit Hinweisen und Umsetzungshilfen,[a] auf der diese Maßnahmenbeschreibung weitestgehend basiert.

[a] Bundesamt für Sicherheit in der Informationstechnik, *Schutz kritischer Infrastrukturen: Risikoanalyse Krankenhaus-IT*, 2013

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer	•		

Die Bewertung der Kritikalität basiert im Wesentlichen auf den vorab durch die Geschäftsführung definierten Schutzzielen (vgl. 3.1 Rahmenbedingungen für IT-Sicherheitsmanagement). Die Anwender müssen unbedingt bei der Ermittlung der Kritikalität von Prozessen und Systemen mitwirken, da sie die Abläufe ihres Bereichs am besten kennen.

Umsetzung der Maßnahme

Diese Maßnahme setzt voraus, dass bereits **Schutzziele** definiert wurden und die Geschäftsführung hinter diesen steht. Auch müssen **Prozesse** (z. B. Patientenaufnahme, -Behandlung oder -Verpflegung) ebenso wie die Infrastruktur im Haus bekannt sein. Die Vorgehensweise ist wie folgt:

- **Kritische Prozesse** anhand der Schutzziele identifizieren,
- Prozess-**unterstützende IT-Systeme** identifizieren (z. B. mittels Interviews),
- **Kriterien** zur Kritikalitätseinstufung für IT-Systeme definieren,
- **Bewertung** unterstützender IT-Systeme anhand von Kriterien

Vorlagen zur Dokumentation von Prozessen, unterstützenden IT-Systemen und Bedrohungen finden Sie in den Anhängen A.7, A.8 und A.9.

Identifikation kritischer Prozesse

Knappe personelle IT-Ressourcen im Krankenhaus machen eine schrittweise Vorgehensweise notwendig. Das BSI empfiehlt, sich zunächst auf einen generischen Behandlungsprozess eines Patienten zu konzentrieren und diesen von *Aufnahme* bis *Entlassung* in **Teilprozesse** einzuteilen. Die Dokumentation wichtiger Prozesse sollte auch den **Vorgänger-** und **Nachfolgerprozess** sowie **Eingaben** und **Ausgaben** definieren, um zusammenhängende Anwendungen einfacher identifizieren zu können.

Ein Prozess ist spätestens dann **kritisch**, wenn eine Störung darin den Krankenhausbetrieb schwerwiegend beeinträchtigt.

Identifikation unterstützender IT-Systeme

Durch die Identifikation kritischer Prozesse können darauf aufbauend wichtige IT-Systeme identifiziert werden. Am einfachsten funktioniert dies laut BSI, indem die Prozess-Anwender in **Interviews** befragt werden, welche **Anwendungen** (z. B. KIS, PACS, usw.) sie für den jeweiligen Prozess wirklich nutzen (**Anwendersicht**). Der am Anfang der Maßnahme referenzierte Leitfaden stellt dafür einen **Fragenkatalog** als Hilfsmittel bereit.

Die IT-Abteilung muss dann ermitteln, beispielsweise ausgehend von einer Netzdokumentation, welche **Systeme** im Hintergrund die jeweilige Anwendung realisiert. Dazu zählen in der Praxis oft auch zentrale Dateispeicher, Nutzer-Clients, Authentifizierungs- und Virtualisierungssysteme und vor allem auch die Krankenhaus-**Netzinfrastruktur** selbst, sprich Netzkomponenten (Router, Switches, usw.). Insbesondere die Netzinfrastruktur stellt meist einen zentralen, sehr

kritischen Dienst für fast alle Anwendungen im Krankenhaus dar.

Kriterien zur Einstufung

Die Kriterien zur Einstufung der Kritikalität eines IT-Systems müssen dahingehend bewertet werden, wie sich eine **Störung** oder ein Ausfall dieser auf die Unterstützung davon abhängiger **Prozesse** auswirkt. Gleichzeitig muss berücksichtigt werden, welchen Schutzbedarf die auf den Systemen liegenden oder bearbeiteten **Daten** haben. Beispielsweise sind medizinische Daten besonders schützenswert, genauso wie andere personenbezogene Daten.

Zur Abstufung sollten die Unternehmens- und Schutzziele herangezogen werden:

- Verfügbarkeit: Wieviel Ausfallzeit eines Systems ist tolerierbar?
- Integrität: Wie wirkt sich eine Kompromittierung der Daten aus?
- Vertraulichkeit: Wie wirkt sich ein Ausspähen der Daten durch Unberechtigte aus?

Das BSI empfiehlt eine Einteilung in normale, hohe und sehr hohe Kritikalität.

Bewertung von IT-Systemen

Zunächst sollten prozessstützende **Anwendungen** gemäß den festgelegten Kriterien eingestuft werden, die von den Anwendern direkt genutzt werden. Das sind klassischerweise das KIS, PACS und andere. Das BSI schlägt vor, eine Tabelle mit folgenden Inhalten zu führen:

- Organisationseinheit
- Prozess
- IT-Unterstützung (ein System kann mehrere Prozesse unterstützen)
- Maximal zulässige Ausfallzeit der IT-Systeme
- Kritikalität

Schließlich sollten alle IT-Systeme, welche die zuvor eingestuften Anwendungen realisieren, gruppiert dokumentiert werden. So müssen zum Beispiel alle Systeme bekannt sein, von denen das KIS abhängig ist. Dazu zählen jedoch nicht nur unmittelbar notwendige Systeme zur Realisierung, sondern insbesondere auch die Netzinfrastruktur. Diese Vorgehensweise ist ebenfalls erforderlich für eine stark differenzierte Netzsegmentierung (vgl. 5.2 Logische Aufteilung des Krankenhausnetzes). Systeme, die miteinander kommunizieren müssen, um eine Anwendung bzw. einen Dienst zu realisieren, müssen in der Regel in dasselbe Sub-Netz gelegt werden. Systeme, die nicht direkt miteinander kommunizieren müssen, sollten hingegen in getrennten Netzen liegen.

Kontinuierliche Verbesserung

Bei dieser Maßnahme handelt es sich nicht um eine Maßnahme mit Endergebnis. **Änderungen** in der **Prozess-**, **Infrastruktur-** oder **Systemlandschaft** müssen stets berücksichtigt werden, damit die in dieser Maßnahme entstehende und gepflegte Dokumentation aktuell bleibt.

Je nach Art der Änderung kann im entsprechenden vorher beschriebenen Schritt wieder eingestiegen werden, darauf **aufbauende Schritte** müssen jedoch immer erneut durchgeführt werden.

Tool-Unterstützung

Es empfiehlt sich, die Dokumentation der Prozesse und Systeme durch ein bereits dafür entwickeltes Tool zu unterstützen. Diese Tools bieten oftmals weitere nützliche Funktionalität an und orientieren sich am Inhalt des BSI-Grundschutzkompendiums. Sie helfen, notwendige Maßnahmen für eine BSI-Zertifizierung zu berücksichtigen und zu strukturieren. Eine Übersicht über verfügbare Tools wird ebenfalls vom BSI angeboten.[5]

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 4 (Prozess-/Anwendungsverantwortlicher), 5 (Risikomanagement), 9 (Asset-Management), 19 (Netz- und Systemmanagement)
- **B3S im Krankenhaus** – insb. ANF-RM 10, ANF-RM 11, ANF-RM 12, ANF-RM 13, Kap. 4.3 (IT-Systemlandschaft), Kap. 5.2.1 (Kernprozesse), Kap. 5.2.2 (techn. Unterstützungsprozesse), Kap. 5.2.3 (kritische Anwendersysteme)
- **ISO/IEC 27001** – Maßnahmenziele A.8.1.1 (Inventarisierung der Werte), ISO/IEC 27005 Risikomanagement
- **BSI-Standards** – 200-3 Risikomanagement

[5] https://www.bsi.bund.de/DE/Themen/ITGrundschutz/GSTOOL/AndereTools/anderetools_node.html

3.6 Reaktion auf Sicherheitsvorfälle im Krankenhaus ■

Kurzbeschreibung

*Bisherige organisatorische Maßnahmen bilden die Grundlage zur Definition eines Sicherheitsverständnisses im Krankenhaus über Richtlinien. Die Verletzung einer Sicherheitsrichtlinie wird als **Sicherheitsvorfall** bezeichnet;[a] entsprechend bilden Sicherheitsrichtlinien und Leitfäden die Grundlage für einen Prozess zur Behandlung von Sicherheitsvorfällen.*

[a] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			•

Die Geschäftsführung muss deutlich hinter dem Prozess stehen, welcher von der IT-Abteilung und den Bearbeitern von Sicherheitsvorfällen geplant und umgesetzt wird. Das Personal muss erkannte Sicherheitsvorfälle oder Probleme melden.

Umsetzung der Maßnahme

Die Umsetzung der Maßnahme teilt sich in die Planungsphase und Durchführungsphase auf.

Planungsphase

In der **Planungsphase** wird die Grundlage für eine koordinierte Reaktion auf Vorfälle gelegt: Der Anwendungsbereich wird definiert; Verantwortlichkeiten, Vorgehensweisen und Kommunikationswege werden festgelegt.

Hinsichtlich des **Anwendungsbereichs** muss jeder Anwender im Krankenhaus genau wissen, was ein Sicherheitsvorfall ist, was also gemeldet werden muss. Dabei helfen die in den vorherigen Abschnitten definierten Sicherheitsrichtlinien und -Leitfäden. Hier kann das Verständnis der Nutzer vor allem mit einprägsamen meldewürdigen Beispielen im Rahmen von Schulungen und Awareness-Maßnahmen erhöht werden (vgl. Maßnahmen 4.2 Security-Awareness-Kampagnen und geeignete Medien ■ sowie 4.3 Durchführung von Übungen und Planspielen ■). Einige einfache Verständnisbeispiele sind:

- Patient Bob kann eine offen liegengelassene Patientenakte von Alice einsehen (Verletzung der Vertraulichkeit).
- Das Krankenhaus-Informationssystem oder ein anderer im Betrieb wichtiger Dienst ist ausgefallen (Verletzung der Verfügbarkeit).
- Ein Unbekannter wird dabei beobachtet, wie er versucht, auf ein PC-System bei der Visite zuzugreifen (potenzielle Verletzung der Integrität, aber auch der Vertraulichkeit).
- Arzt Dr. Charlie bekommt auf sein geschäftliches E-Mail-Konto gefährliche Phishing-Mails und erkennt diese (mögliches Einfallstor für Malware).

Inhalte der Schulungen sollten auch die Art und Weise der Beschreibung von beobachteten Sicherheitsvorfällen und eine unmittelbare Beweissicherung durch den Beobachter (z. B. über Fotos, Zeugen, etc.) sein. Alles sollte in einer Richtlinie zur Behandlung von Sicherheitsvorfällen zusammengefasst sein.

Definierte **Zuständigkeiten** sind grundsätzlich wichtig, um Vorfälle schnell bearbeiten zu können und den Betrieb möglichst zügig wiederherzustellen. Zentrale zu besetzende Rollen im Krankenhaus sind beispielsweise:

- Ein *Incident Response Process Manager*, der für die Prozessgestaltung verantwortlich ist.
- Mehrere *Incident Handler*, welche Sicherheitsvorfälle behandeln. Je nach Personal-Ressourcen kann diese Rolle auch in 1^{st},2^{nd},3^{rd}-Level-Supporter aufgeteilt werden. Oft fehlt in Kliniken dafür aber die notwendige Personalstärke. Ein Incident Handler ist als Handlungsverantwortlicher eines zugewiesenen Vorfalls anzusehen.
- Ein *Computer Incident Security Response Team* (CSIRT) zur schnellen Behandlung Vorfällen. Dem Team sollten alle Incident Handler, der IRP-Manager und weitere versierte Mitarbeiter angehören.
- Ein *Major Incident Team*, welches die Behandlung von Major Incidents (schwerwiegende Vorfälle) koordiniert und durchführt.

Eine koordinierte, definierte **Vorgehensweise** bei der Bearbeitung von Sicherheitsvorfällen ist ebenfalls eine grundlegende Basis für eine schnelle Bearbeitung. Dabei gibt es wichtige Voraussetzungen, die vorab geklärt werden müssen:

- Das CSIRT muss vorab definiert haben, was ein Sicherheitsereignis (sicherheitsrelevante Situation) und was ein Sicherheitsvorfall (ein oder mehrere Ereignisse plus entstandener Schaden) ist.
- Wer entscheidet, was konkret ein Sicherheitsvorfall ist?
- Auch sollten Minor Incidents von Major Incidents unterschieden werden.

Eine typische Vorgehensweise[6] bei der Behandlung ist:

1. Feststellung der **Relevanz**
2. Durchführung von **Sofortmaßnahmen** (v. a. Eindämmung, Untersuchung, Behebung und Wiederherstellung)
3. **Dokumentation** des Vorfalls (siehe Anhang A.3)
4. Ausübung der **Meldepflicht**
5. **Beweissicherung**
6. **Ursachenanalyse**

Bei der Planung hinsichtlich der **Kommunikationswege** (d. h. wer meldet was an wen?) gibt es einige Aspekte, die berücksichtigt werden müssen. Für die Aufnahme von Sicherheitsvorfällen sollte eine zentrale Stelle eingerichtet werden, von der aus das weitere Vorgehen im Einzelfall koordiniert werden kann. Dieses kann technisch unterstützt werden durch web-basierte Ticket-Systeme, wie das frei nutzbare System Bugzilla für kleinere und OTRS für große Umgebungen, oder via zentraler telefonischer Aufnahme und nachgeschaltetem Ticket-System. Beides hat Vor- und Nachteile: Ticket-Systeme können die Koordination vor allem in großen Kliniken stark erleichtern. Auch kann man den Nutzern über Ticket-Systeme den Bearbeitungsstatus des Vorfalls immer bereitstellen. Ticket-Systeme können aber auch ein Hemmnis für Nutzer darstellen und manche überfordern. Die Variante über das Telefon erfordert wiederum deutlich mehr manuellen Aufwand für den die jeweiligen Anrufe entgegennehmenden Mitarbeiter, jedoch ist die Qualität der Meldungen durch das Nachfragen höher. Es ist jedoch empfehlenswert, in größeren Häusern mit mehr als 100 Mitarbeitern ein Ticket-System einzuführen, da der manuelle Aufwand andernfalls zu hoch wird.

Des Weiteren sind hier bei der Kommunikation vor allem Kontakte und Wege bezüglich verpflichtender Meldungen an behördliche Stellen zu beachten. Das BSI bietet dazu eine FAQ-Seite,[7] ein Meldeformular wird von der Bundesnetzagentur[8] angeboten.

Durchführungsphase

In der **Durchführungsphase** wird der Prozess praktisch umgesetzt. Erfahrungen, die im Prozess gesammelt werden, sollten erneut in die Planungsphase einfließen, um kommende Durchführungsphasen zu optimieren. Das kann den definierten Anwendungsbereich und Zuständigkeiten, Vorgehensweisen, insbesondere auch Systeme zur technischen Unterstützung und auch Kritikpunkte durch Nutzer betreffen. Empfehlenswert ist auch die Definition einer Richtlinie für Sicherheitsvorfälle. Eine entsprechende Vorlage ist in Anhang A.5 zu finden.

Besondere Herausforderungen im Betrieb

Eine Problematik, die in Unternehmen ebenso wie in Krankenhäusern auftritt, ist die Verfügbarkeit des bereits oft ohnehin am Limit arbeitenden IT-Personals für die Bearbeitung von Vorfällen. Hier bedeutet ein **krankheitsbedingter Ausfall** eines Mitarbeiters in der IT oftmals bereits eine starke Beeinträchtigung des Betriebs, insbesondere bei der Bearbeitung von Sicherheitsvorfällen. In manchen Krankenhäusern hat sich dafür als Teillösung die bedarfsabhängige Einbeziehung von **Dienstleistern** etabliert. Manche bieten eine Rufbereitschaft an, welche in derartigen Fällen hilfreich ist.

Ein Aspekt, der häufig von den Verantwortlichen bei der Behandlung von Sicherheitsvorfällen nicht ausreichend berücksichtigt wird, ist der des **Nutzer-Feedbacks**. Von Vorfällen betroffene Mitarbeiter (v. a. des medizinischen Betriebs) sollten immer über den aktuellen Stand der Behandlung eines Vorfalls oder einer Störung auf dem Laufenden gehalten werden. Einerseits haben Nutzer somit das beruhigende Gefühl, dass die Bearbeitung im Gange ist, und andererseits können sie besser abschätzen, wann Dienste oder Systeme für sie wieder nutzbar sind. Bei schwerwiegenderen Vorfällen mit vielen Betroffenen (z. B. KIS-Ausfall) sollte die in Maßnahme 3.3 Webplattform für Sicherheitsinhalte im lokalen Krankenhausnetz ■ empfohlene Web-Plattform (oder ähnliches) für Meldungen genutzt werden. Bei Einzelfällen bieten Ticket-Systeme oft entsprechende Funktionalität.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 6 (Notfallmanagement), 8 (Behandlung von IT-Sicherheitsvorfällen), 15 (Interne Kommunikation)
- **B3S im Krankenhaus** – Kap. 7.9 (Vorfallerkennung und Behandlung), Anforderungen ANF-MN 72-77
- **ISO/IEC 27001** – A.16 (Handhabung von Informationssicherheitsvorfällen)
- **BSI IT-Grundschutz-Kompendium** – DER.1 (Detektion von sicherheitsrelevanten Ereignissen), DER.2.1 (Behandlung von Sicherheitsvorfällen), DER.2.3 (Bereinigung weitreichender Sicherheitsvorfälle)
- **NIST SP 800-62** Computer Security Incident Handling Guide

[6] Brenner u. a., „Praxisbuch ISO/IEC 27001“, 2. Auflage, Hanser Verlag, S.118

[7] https://www.bsi.bund.de/DE/Themen/KRITIS/IT-SiG/FAQ/FAQ_zur_Meldepflicht/faq_meldepflicht_node.html

[8] https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/MitteilungSicherheitsverletzung/Mitteilungeinersicherheitsverletzung-node.html

3.7 Erstellung von Notfallkonzepten und Wiederanlaufplänen ■

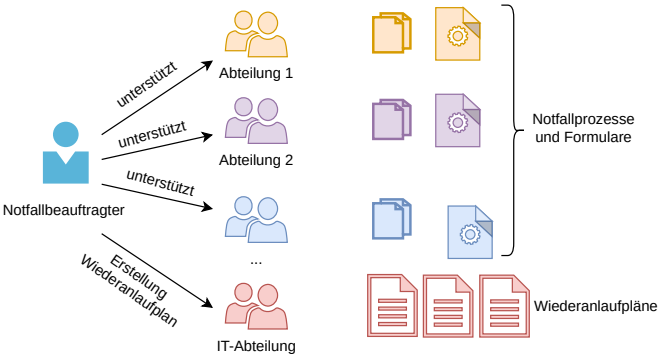


Abbildung 3.5: Erstellung von Notfallkonzepten und Wiederanlaufplänen

Kurzbeschreibung

Wie in jeder anderen Organisation können auch im Krankenhaus große Teile der IT-Infrastruktur ausfallen, beispielsweise durch Hardware- und Softwaredefekte, ein fehlerhaftes Update, Stromausfall oder Malware. Da in einem Krankenhaus jedoch besonders kritische Prozesse des medizinischen Betriebs stark von der IT abhängig sind und nicht bis zur Wiederherstellung des Normalbetriebs ausfallen dürfen, müssen Krankenhäuser Notfallpläne erstellen, in denen dargestellt wird, wie der medizinische Betrieb auch ohne IT-Infrastruktur weiterlaufen und der Wiederanlauf möglichst strukturiert erfolgen kann.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung	•	•	
IT-Abteilung	•		
Notfallbeauftragter	•		
Personal/Nutzer	•		

Bei der Erstellung von Notfallprozessen und Wiederanlaufplänen sind alle Parteien direkt involviert. Die Koordination muss vom Sicherheitsbeauftragten oder einem zugeordneten Notfallbeauftragten ausgehen.

Umsetzung der Maßnahme

Als Grundlage für die Vorgehensweise bei der Notfallplanung ist immer eine Übersicht über die wichtigsten **Prozesse**, unterstützende **IT-Dienste** (vergleiche Maßnahme 3.5 Identifikation kritischer Systeme im Krankenhaus ■) und jeweils eingebundenes Personal vorausgesetzt. Das **Hauptziel** ist die Aufrechterhaltung des medizinischen Betriebs.

Empfehlenswert ist bei der Erstellung ein **priorisierter Ansatz**, bei dem der Notfallbeauftragte in Absprache mit der Geschäftsführung immer eine **Auswahl der wichtigsten Prozesse** vornimmt, für die Notfall-Prozesse erstellt werden; z. B. in der Größenordnung 3-8, je nach Größe des Hauses. Es sollte darauf geachtet werden, dass das für den jeweiligen Prozess **zuständige Personal** sich **nicht überschneidet**, damit die Gruppen möglichst parallel arbeiten können.

Einerseits müssen **Notfall-Prozesse** und **-Konzepte** (d. h. ohne IT-Unterstützung) erarbeitet werden, um den Betrieb aufrechtzuerhalten, andererseits sollte ein von der IT-Abteilung erstellter **Wiederanlaufplan** als hilfreiche Unterstützung für die möglichst zügige Wiederherstellung des Normalbetriebs vorliegen. Für beide Seiten – die Aufrechterhaltung des Betriebs sowie die Wiederherstellung von IT-Diensten – sind **Übungen** notwendig, um die Notfallkonzepte zu überprüfen, ggf. zu verbessern und und praktisch zu vertiefen (siehe auch Maßnahme 4.3 Durchführung von Übungen und Planspielen ■).

Ein möglicher Ansatz ist, die **Koordination** durch den **Notfallbeauftragten** oder den Informationssicherheitsbeauftragen mit **mehreren Gruppen gleichzeitig** durchzuführen. Das heißt: Zentral koordiniert erstellen mehrere Abteilungen, wie z. B. Verwaltung, Empfang, Radiologie, Kardiologie und Labor, Notfall-Prozesse und -Konzepte für den Fall eines IT-Ausfalls. Gleichzeitig erarbeitet die IT-Abteilung einen Wiederanlaufplan.

Es ist empfehlenswert, beschriebene **Notfall-Prozesse** sowie **Wiederanlaufpläne** gesammelt und in gedruckter Form aufzubewahren, auf die das Krankenhauspersonal in kürzester Zeit Zugriff hat.

IT-unabhängige Notfall-Prozesse

Bei der Erstellung von **Notfall-Prozessen**, welche im Falle eines IT-Ausfalls greifen, ist es offensichtlich, dass das jeweils **ausführende Personal** selbst den **Kernbeitrag** leisten muss. Dieses weiß am besten, welche Handlungen, Schrittfolgen, Dokumentationen und IT-Systeme notwendig sind, beispielsweise in der Patientenaufnahme oder in der -behandlung.

Die einzelnen Gruppen, vorrangig bestehend aus dem jeweils zuständigen Personal für einen Prozess, müssen sich dann darüber bewusst werden, **wo welcher Dienst und welches System im Normalbetrieb** (z. B. KIS, LIS, PACS, Dateiablagen, Drucker, Client-PCs, mobile Geräte, usw.) für welchen **Zweck** (z. B. Dateneinsicht, Dokumentation, Organisation, Kommunikation, usw.) eingesetzt wird. Darauf aufbauend müssen dann für jeden Prozess Konzepte erarbeitet werden, wie diese IT-gestützten Aktivitäten **ersetzt** werden können. So eignen sich im Notfall beispielsweise bereits ausgedruckt und griffbereit in den Behandlungsräumen vorliegende Formulare für die normalerweise über das KIS

durchgeführte Dokumentation der Behandlung von Patienten.

Dabei können sich die jeweiligen Gruppen auf Prozessdefinitionen des Normalbetriebs stützen, sofern diese vorhanden sind, und – ausgehend von einzelnen Aktivitäten – darin eine entsprechende **Notfallaktivität** erstellen:

Beispielsweise anstatt „**Prozess 27 Aktivität 13:** Dokumentation des Patienten-Gesundheitszustands in KIS Model XYZ" die Notfallaktivität „**Notfallprozess 27 Aktivität 13:** Dokumentation des Patienten-Gesundheitszustands in Formular ABC-7-a". In einer davon abhängigen Beispiel-Aktivität muss dann auf entsprechende Inputs und Outputs referenziert werden, z. B. ***Notfallprozess 27 Aktivität 19:*** *Auf Basis der Formulare ABC-7-a, DEF-3-b, GHI-1-a Arztbrief für Patient erstellen.* Hier ist zu erkennen, dass **Schnittstellen zwischen den Prozessen** erarbeitet werden müssen. Deshalb ist es notwendig, dass sich Anwender der jeweiligen Prozesse untereinander abstimmen.

Die Notfallprozesse sollten regelmäßig überprüft werden. Sowohl, wenn sich in den Prozessen des Normalbetriebs etwas ändert, als auch zu festgelegten regelmäßigen Zeitpunkten, z. B. alle sechs Monate. Ähnliches gilt für Übungen, welche ebenfalls regelmäßig stattfinden sollten, damit das Krankenhaus-Personal im Notfall unmittelbar handlungsfähig ist. Neben Übungen bietet es sich an, Notfall-Konzepte bei zentralen Sicherheitsbelehrungen oder in ähnlichen Veranstaltungen durchzugehen.

Griffbereite Formulare

Im Notfall muss ein Großteil von prozessunterstützenden IT-Systemen durch **Formulare** ersetzt werden, insbesondere zur Dokumentation des medizinischen Betriebs (z. B. zur Patienten-Dokumentation, Patienten-Entlassung, usw.). Hier müssen folgende Aspekte bedacht werden:

- Die Formulare müssen vorgedruckt, **unmittelbar griffbereit** und in **ausreichender Stückzahl** vorhanden sein.
- Den Formularen müssen ausreichend **Schreibstifte beigelegt** sein, um sie absolut zeitnah einsetzen zu können.
- Die Formulare müssen je nach Typ mit einer eindeutigen **ID** versehen sein, damit das Personal sie schnell identifizieren kann.
- Die Formulare müssen in **Notfall-Prozessdefinitionen** klar **referenziert** werden (vgl. vorheriger Abschnitt).
- Zur Ordnung und Übersichtlichkeit sollten **Ablagefächer** für die jeweiligen Dokumenttypen bereitstehen..
- Es müssen **Abhängigkeiten und Transport** bedacht werden, je nachdem, wo ein Dokument benötigt wird (z. B. ausgefüllte Formulare ABC-7-a werden in Abteilungen A1, B2, C1, usw. benötigt).

Es muss auch darauf geachtet werden, welche Formulare in **mehreren Prozessen** benötigt werden, damit nicht zahlreiche individuelle Dokumente für den gleichen Zweck entstehen, sondern eine Vorlage, die für den gleichen Zweck in verschiedenen Prozessen verwendet werden kann.

Einschränkung des Betriebs

Je nach Größenordnung eines IT-Ausfalls ist eine reibungslose Aufrechterhaltung des *kompletten* medizinischen Betriebs nicht immer möglich. Entsprechend ist in der Praxis eine **Einschränkung des medizinischen Betriebs** auf eine definierte Menge an Notfall-Prozessen teilweise sinnvoll. Dafür ist ein kontrolliertes Aussetzen von Prozessen mit **geringerer Priorität**, wie zum Beispiel aufschiebbare chirurgische Eingriffe, nicht auszuschließen, damit stets der Überblick und die Kontrolle des Betriebs erhalten bleiben.

Überleitung zum Normalbetrieb

Für eine funktionierende Überleitung in den Normalbetrieb muss insbesondere darauf geachtet werden, dass Informationen und Dokumente, die während des Notfallbetriebs generiert wurden, nachträglich entsprechend in die IT-Systeme, wie KIS, LIS, usw., eingepflegt werden. Die Original-Dokumente sollten jedoch noch eine Weile aufgehoben werden, falls bei ihrer Digitalisierung Fehler gemacht oder Dokumente gar übersehen wurden.

Wiederanlaufplan erstellen

Die Erstellung eines Wiederanlaufplans erfolgt durch die IT-Abteilung, ggf. auch in Absprache mit Prozessnutzern hinsichtlich der Priorität von IT-Systemen. Diese ist auch bei der Identifikation wichtiger Systeme (vgl. Maßnahme 3.5 Identifikation kritischer Systeme im Krankenhaus ■) eine entsprechend zu dokumentierende Kerninformation.

Beim Wiederanlaufplan sind **Abhängigkeiten** zwischen Systemen zu berücksichtigen. Das fängt bei relativ eindeutigen Zusammenhängen an, wie der Stromversorgung, USVs, Netzersatzanlagen (NEA), wird jedoch dann bereits für Komponenten der Netzinfrastruktur (Switches, Router, Firewalls, usw.) komplizierter und weiter verstärkt auf System- und Dienstebene (z. B. *Dienst X läuft auf VMs A, B, C, D, welche über Hypervisors auf Systemen H, G realisiert werden*).

Auch müssen diese Pläne unter Berücksichtigung von Datensicherungen (vgl. Maßnahme 6.4 Automatisierte Datensicherung zur effektiven Wiederherstel-

lung ■) erstellt werden, welche im Notfall bei einer Kompromittierung eines Systems das Rückgrat der Wiederherstellung darstellen. Daher sind entsprechende notwendige Informationen in einem Wiederanlaufplan mindestens die Folgenden:

- Für **Dienste:**
  - Generell: Zweck, Hersteller, Produkt, zuständige Dienstleister (+Kontakt), Dienstverantwortlicher
  - Zugang: Registrierungsinformationen, Zugangsdaten (Benutzername, Passwort), IP-Adresse, MAC-Adressen
  - Anforderungen: Notwendige Leistung (RAM, CPU, usw.), zwingend benötigte Schnittstellen (z. B. USB)
  - Abhängigkeiten: Host-System, Referenz auf andere notwendige Dienste (z. B. SQL-Server), Datensicherungsort
- Für **Systeme:**
  - Generell: Hostname, Zweck, Typ (virtuell, physisch), Hersteller, Produkt, zuständige Dienstleister (+Kontakt), Systemverantwortlicher, Ort (z. B. *im Serverraum, Rack 4, Höheneinheit 17*)
  - Zugang: Registrierungsinformationen, Zugangsdaten (Benutzername, Passwort), IP-Adresse, MAC-Adressen
  - Spezifikation: Leistung (RAM, CPU, usw.)
  - Abhängigkeiten: Hypervisor-System (falls Typ *virtuell*), Datensicherungsort

Aufgrund der höchst schützenswerten Informationen muss das **Wiederherstellungshandbuch** mit den Wiederherstellungsplänen entsprechend geschützt und nur berechtigten Nutzern zugänglich gemacht werden. Und auch hier sind, wie bei Notfall-Prozessen, sowohl **Übungen** als auch **Revisionszeiträume** notwendig.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 6 (Notfallmanagement), 7 (Betriebliches Kontinuitätsmanagement), 8 (Behandlung von IT-Sicherheitsvorfällen), 16 (Externe Informationsversorgung und Kommunikation)
- **B3S im Krankenhaus** – Kap. 7.2.3 (Prozess- /Anwendungsverantwortlicher), Kap. 7.4 (Betriebliches Kontinuitätsmanagement)
- **ISO/IEC 27001** – A.17 (Informationssicherheitsaspekte beim Business Continuity Management)
- **ISO/IEC 27031** – Leitfaden für die Bereitschaft von Informations- und Kommunikationstechnologien für Business Continuity
- **BSI IT-Grundschutz-Kompendium** – DER.4 (Notfallmanagement)

Kapitel 4

Mitarbeiter-Awareness

Die Schaffung von Awareness bei den Mitarbeitern ist ein Teil des organisatorischen Informationssicherheitsmanagements. Aufgrund der Relevanz der Thematik im Krankenhaus sind in diesem Katalog Awareness-Maßnahmen jedoch in diesem separaten Kapitel beschrieben. Dabei sind die Maßnahmen in einer Art und Weise angeordnet, dass sie Ihnen, dem Leser, übersichtlich auf wenigen Seiten generelle Gestaltungskonzepte und viele Möglichkeiten zur Schaffung von Awareness nahebringen können. Entsprechend wird vermittelt,

- wie Awareness-Schaffung generell für IT-Sicherheit im Krankenhaus strukturiert in Phasen gestaltet werden kann,
- welche Medien in welchen Phasen der Awareness-Schaffung eingesetzt werden können,
- wie aufwändigere und detailliertere Methoden, wie zum Beispiel Übungen und Spiele, durchgeführt werden können
- und wie Mitarbeiter-Awareness auch getestet werden kann.

Auf Basis der Maßnahmen ist es zudem empfehlenswert, einen Plan zur Verbesserung der Mitarbeiterawareness anzufertigen. Eine Vorlage dazu können Sie in Anhang A.6 finden. Wie bei generellen organisatorischen Maßnahmen richten sich auch diese Maßnahmen vor allem an die Geschäftsführung und die Entscheidungsträger im Krankenhaus.

4.1 Konzeption und Präsentation von Awareness-Maßnahmen ■

Kurzbeschreibung

Mitarbeiter-Awareness ist einer der essenziellsten Aspekte bei der Absicherung eines Krankenhauses. Viele sicherheitsrelevante Vorfälle und Probleme entstehen durch unbeabsichtigtes Fehlverhalten und fehlende Awareness. In dieser Maßnahme wird generell beschrieben, wie Awareness-Maßnahmen und Inhalte geeignet für ihre Zielgruppe aufbereitet sein sollen, damit sie möglichst wirksam sind.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			•

Geeignete Awareness-Inhalte müssen insbesondere durch die Verantwortlichen für Awareness- und Schulungsmaßnahmen ausgewählt und umgesetzt werden. In diesem Kontext wird angenommen, dass die IT-Abteilung als Kompetenzträger im Bereich IT-Sicherheit derartige Maßnahmen übernimmt.

Umsetzung der Maßnahme

Generell gibt es vier wichtige Dimensionen bei Awareness-Programmen, die berücksichtigt werden müssen, damit eine Kampagne erfolgreich ist: der **Beweggrund**, das **Klima**, die **Gestaltung** und der **Inhalt** des Awareness-Transfers.[1]

Beweggrund für Awareness-Maßnahmen

Awareness-Maßnahmen im Krankenhaus können nicht nur Sicherheitsvorfälle vermeiden und somit Kliniken sicherer machen, sondern sie bereiten das Personal auch auf ein **korrektes Verhalten bei eingetretenen Sicherheitsvorfällen** vor. Dies wirkt sich im Betrieb positiv auf die Effizienz und die Sicherheit vor **Ausfällen** aus.

Klima des Awareness-Transfers

Eine Awareness-Kampagne muss auf die Charakteristika der Umgebung angepasst werden. Im Krankenhaus beispielsweise müssen dessen **Ziele**, die **Zielgruppe (Ärzte, Pflege, Administration, usw.)** der jeweiligen Awareness-Maßnahme und andere Aspekte berücksichtigt und dazu passend gestaltet werden. Die Zielgruppen von Awareness-Kampagnen müssen sich mit den darin angesprochenen Problematiken und Vorgaben **identifizieren** können. Dies wird am besten erreicht, indem **aktuelle** und **zielgruppen-relevante Probleme** thematisiert werden. Eine etablierte schrittweise Vorgehensweise[2] für Kampagnen zur Awareness-schaffung ist Folgende:

- Schaffung von **Aufmerksamkeit** (z. B. E-Mails zu akuten Sicherheitsproblemen)
- Wissen **transferieren** (z. B. Angebot detaillierter Informationen über Intra-Webportal)
- Wissen **verstärken** (z. B. Themenaufgreifende Newsletter, Intra-Web-Artikel)

Nähere Informationen zur Durchführung einer Kampagne gibt es auch in Maßnahme 4.2 Security-Awareness-Kampagnen und geeignete Medien ■.

Gestaltung des Awareness-Transfers

Die Gestaltung kann durch unterschiedliche Medien und Maßnahmen umgesetzt werden. Dabei ist es wichtig, dass zeitgemäße und vor allem für ein Krankenhaus angemessene Methoden angewandt werden. Zum Beispiel nehmen „Vor-Lesungen" im wörtlichen Sinne viel Zeit in Anspruch und vermitteln Inhalte relativ mühsam. Deutlich einprägsamer sind auf den Punkt gebrachte **Illustrationen**, **Videos**, **Give-Aways**, **Flyer**, **interaktive Websites** und **Spiele**. In diesem Katalog ist die Gestaltung unter Verwendung unterschiedlicher Medien in den folgenden Maßnahmen detaillierter beschrieben.

Auch muss darauf geachtet werden, wann Awareness-Schaffung stattfindet. Viele in diesem Bereich tätige Autoren von Veröffentlichungen empfehlen **kontinuierliche Maßnahmen in kurzen Abständen**. So sollte ein fest vorgesehener, zeitlich begrenzter Punkt in wöchentlich oder monatlich ohnehin stattfindenden Besprechungen und Versammlungen dafür eingeplant werden.

Einen weiteren Unterschied kann das *Wer* ausmachen. Durch die gelegentliche Präsentation von Schulungsmaterial durch **externe Gäste**, die sich mit Nutzer-Awareness beschäftigen, kann der Thematik bei den Nutzern eine noch höhere Akzeptanz verliehen werden.

Inhalte für Awareness-Maßnahmen

Die Wahl der Inhalte für Awareness-Kampagnen ist überaus wichtig, um den gewünschten Effekt zu erzielen. Einige Richtlinien bietet folgende Liste:

[1] Ghazvini, Arash, and Zarina Shukur. „Awareness training transfer and information security content development for healthcare industry". International Journal of Advanced Computer Science and Applications (ijacsa) 7.5 (2016).

[2] *Fox, Dirk, and Sven Kaun. „Security Awareness-Kampagnen". Proc. BSI-Kongress. 2005.*

- Inhalte müssen **fallspezifisch und abgegrenzt** sein. Schulungen oder Maßnahmen, die das gesamte Spektrum von Security-Awareness auf einmal behandeln wollen, führen oft dazu, dass die Zuhörer überfordert werden und sich keine Verbesserung einstellt.
- Inhalte sollten einen **Bezug zu aktuellen Problemen** haben. So können akute Missstände gezielt beschrieben und behoben werden (z. B. anonymisierte Vorfälle oder auch akute Vorfälle aus anderen Kliniken in den Medien).
- Inhalte müssen möglichst **einfach formuliert und dargestellt** werden. Beispielsweise durch geeignete Illustrationen und universell verständliche Symbolik.
- Es sollten Beispiele und Analogien aus dem **privaten Alltag** verwendet werden. Beispielsweise kann Nutzern das Risiko durch den bildhaften Vergleich eines nicht-gesperrten Bildschirms mit der offenen Haustür daheim und dem in beiden Fällen möglichen unerlaubten Zugriff verdeutlicht werden. Auf diese Weise können sich Nutzer besser mit derartigen Sachverhalten **identifizieren**.
- Inhalte müssen **variieren und angepasst** werden. Die Präsentation der immer gleichen Folien zur Security-Awareness lässt Nutzer diesbezüglich schnell abstumpfen.

Wie bereits beschrieben, kann der Inhalt für Schulungen auch sehr gut auf der Basis von Nachrichten- oder Zeitschriftenartikeln gestaltet werden. Etwa durch das Heranziehen aktueller öffentlich gewordener Vorfälle aus anderen (über-)regionalen Krankenhäusern. Komplettiert mit einer anschließenden Präventionstechnik schafft eine derartige Präsentation das wichtige Verständnis bei den Nutzern.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 13 (Personelle und organisatorische Sicherheit)
- Weder **B3S im Krankenhaus** noch **ISO/IEC 27001** geben konkrete Hinweise zur Gestaltung von Awareness-Maßnahmen. Jedoch sind Awareness und die Schulung von Mitarbeitern in verschiedenen Anforderungen ein wichtiges Thema (vgl. *ISO/IEC 27001* Anforderung A.7.2.2, *B3S im Krankenhaus* insb. Anforderungen ANF-MN 3, ANF-MN 18, ANF-MN 65, ANF-MN 70, ANF-MN 71).
- **BSI IT-Grundschutz-Kompendium** – ORP.3 (Sensibilisierung und Schulung), Umsetzungshinweise zu Baustein ORP.3

4.2 Security-Awareness-Kampagnen und geeignete Medien

Kurzbeschreibung

Zur Erhöhung der Sicherheitsawareness des Personals eignen sich verschiedene Medien zur Präsentation vielfältiger Inhalte und in unterschiedlichen Stadien einer Kampagne. In dieser Maßnahme wird ein Überblick gegeben, welche Medien genutzt werden können und welche Art von Inhalten dafür jeweils besonders geeignet ist.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			•

Die Schaffung von Sicherheitsawareness beim Personal ist vor allem die Aufgabe des Informationssicherheitsbeauftragten. Derartige umfassende Maßnahmen müssen üblicherweise von der Geschäftsführung abgesegnet werden und können auch auf Anregungen von Nutzern aufbauen.

Umsetzung der Maßnahme

In Maßnahme 4.1 Konzeption und Präsentation von Awareness-Maßnahmen wird eine schrittweise Vorgehensweise erklärt, wie bei den Nutzern Awareness am besten geschaffen werden kann. Diese ist demnach: *1)* **Aufmerksamkeit schaffen**, *2)* **Wissen transferieren** und *3)* **Wissen verstärken**.[3] Im Folgenden werden geeignete Medien dementsprechend gruppiert.

Aufmerksamkeit schaffen

„Aufmerksamkeit schaffen" bezieht sich in erster Linie auf die **Informierung des Krankenhaus-Personals** über die Veranstaltung einer Awareness-Kampagne. Dem Personal sollten hier organisatorische Aspekte bekannt gemacht werden. Dazu zählen Termine zur Durchführung von Hauptmaßnahmen und **Verweise** auf detaillierte Informationen (z. B. auf einer zentralen **Webplattform**, vgl. 3.3 Webplattform für Sicherheitsinhalte im lokalen Krankenhausnetz).

Zur Schaffung von Aufmerksamkeit für Awareness-Kampagnen eignen sich insbesondere **Flyer**, **Plakate** und breite Informationskanäle wie **E-Mail**. Auch können derartige Informationen über **Vorgesetzte** (z. B. Chefarzt zu Oberärzten zu Ärzteschaft, Pflegeleitung und Pflegepersonal) mündlich vermittelt werden.

Wissen transferieren

In dieser Phase wird das Awareness-Wissen an das gesamte Personal vermittelt. Insbesondere hier sollte sich an die Prinzipien aus Maßnahme 4.1 Konzeption und Präsentation von Awareness-Maßnahmen gehalten werden, beispielsweise die Vermittlung fokussierter und alltagsnaher Themen. Hier eignen sich klassische **Vorträge** oder auch **Seminare**, um einer größeren Gruppe von Mitarbeitern Inhalte zu vermitteln. Jedoch auch **Spiele** oder die Durchführung von **Übungen** oder **Szenarien** sind sehr hilfreich, um gelerntes Wissen besser zu behalten.

Hier bieten sich zum Beispiel Quiz-**Spiele** an, die ähnlich wie der Fragenkatalog einer Führerschein-Theorieprüfung gestaltet, aber dem Kontext des Krankenhaus-Betriebs angepasst sind. Die Inhalte sollten sich auf den Krankenhaus-Alltag beziehen. Beispiel:

„Was ist zu tun, wenn Sie Ihren Rechner verlassen?"

a) „Nicht länger als 10 Minuten abwesend sein"

b) „Den Bildschirm sperren"

c) „Das USB-Kabel der Tastatur abziehen"

In diesem Fall ist Antwort *b)* korrekt. Solche Spiele können in einer Gruppe im Rahmen von Seminaren oder auch auf oben erwähnter zentraler Webplattform im Intranet für jeden Nutzer angeboten werden. Auch gibt es bereits Spiele, welche dem Sicherheitsbeauftragten selbst dabei helfen, neue Ideen und Vorgehensweisen zur Verbesserung der IT-Sicherheit zu entwickeln, beispielsweise das Web-Spiel „Targeted Attack"[4], das „Enter Game"[5] oder „CyberCIEGE"[6], die zwar keinen direkten Krankenhausbezug haben, deren Kernaussagen aber übertragbar sind.

Übungen und Szenarien werden im Detail in Maßnahme 4.3 Durchführung von Übungen und Planspielen näher erörtert.

Wissen verstärken

In dieser Phase soll das Wissen, das den Mitarbeitern in der letzten Phase vermittelt wurde, verstärkt und aufgefrischt werden. Zeitsparende Medien für das Krankenhauspersonal sind beispielsweise **E-Mails** zu aktuellen Fällen (z. B. Erinnerung an Verhaltensregeln bei SPAM- und Phishing-E-Mails), die Erstellung und das Verteilen von **Postern und Plakaten** mit Informationen auf einen Blick zu einem kleinen, umschlossenen Themenbereich (z. B. Verhalten am Arbeitsplatz,

[3] *Fox, Dirk, and Sven Kaun. „Security Awareness-Kampagnen". Proc. BSI-Kongress. 2005.*

[4] http://targetedattacks.trendmicro.com/index.html

[5] https://entergame.ch/de/

[6] https://nps.edu/web/c3o/cyberciege

Verhalten bei der Visite, Erkennungsmerkmale von Phishing-E-Mails, „Was sind schützenswerte Informationen“, u.s.w.). Es bietet sich jedoch auch an, erworbenes theoretisches Wissen (z. B. Verhalten im IT-Ausfall) im Rahmen von **Übungen** anzuwenden und regelmäßig zu trainieren.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 13 (Personelle und organisatorische Sicherheit)
- **B3S im Krankenhaus** – Kap. 7.8 (Personelle und organisatorische Sicherheit)
- **ISO/IEC 27001** – A.7.2.2 (Informationssicherheitsbewusstsein, -ausbildung und -schulung)
- **BSI IT-Grundschutz-Kompendium** – ORP.2 (Personal)

4.3 Durchführung von Übungen und Planspielen

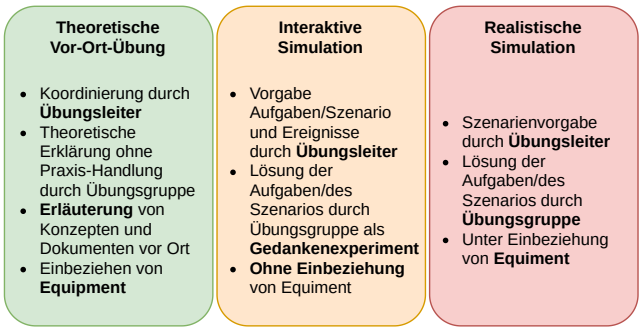


Abbildung 4.1: Arten von Übungen und ihre Inhalte

Kurzbeschreibung

Übungen und Planspiele sind wichtige Instrumente, um Notfallkonzepte (vgl. Maßnahme 3.7 Erstellung von Notfallkonzepten und Wiederanlaufplänen ■) zu üben, zu verinnerlichen und zu verbessern. Theoretische Konzepte, z. B. bei Serverausfällen, Stromausfall oder einem Ransomware-Befall, bringen relativ wenig, wenn das Personal das Wissen nicht sofort abrufen und nicht nach definierten Prozessen handeln kann.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	•
IT-Abteilung	•		
Notfallbeauftragter	•		
Personal/Nutzer			•

Für die Planung und Durchführung von Planspielen sind der Informationssicherheitsbeauftragte, je nach Fall zusammen mit dem Notfallbeauftragten, und die IT-Abteilung zuständig. Da jedoch bei der Umsetzung im Alltag wichtiges Personal gebunden wird, sollte die Geschäftsführung genauso einbezogen werden und die Genehmigung dazu erteilen. Das gesamte Personal sollte auf Basis eines gestaffelten Auswahlverfahrens an solchen Übungen teilnehmen und mögliche Kritik zur Verbesserung von Prozessen und Konzepten einbringen.

Umsetzung der Maßnahme

Im Krankenhaus ist es üblicherweise nicht möglich, eine groß angelegte Kollektiv-Übung mit allen Mitarbeitern durchzuführen; der Betrieb muss schließlich stets aufrechterhalten werden. Der Zweck, dass das Personal im Notfall direkt weiß, was zu tun ist, ohne sich in Prozessdokumentationen einlesen zu müssen, kann auch in **kleineren Gruppen**, welche regelmäßig **durchwechseln**, umgesetzt werden (insbesondere bei Änderungen im Konzept oder im Personal).

Insbesondere für Notfallübungen hat die WHO ein Übersichtsdokument bereitgestellt, welches als Ausgangsbasis für diese Maßnahme gilt.[7]

Arten und Phasen von Übungen

In dieser Maßnahme werden drei denkbare Arten von Übungen berücksichtigt: (1) **theoretische Vor-Ort-Übung** (Vorführung durch Übungsleiter mit Equipment), (2) **interaktive Simulation** (realistische Ereignisreaktion durch Personal ohne Equipment, erzählend) und (3) **realistische Simulation** (realistische Ereignisreaktion durch Personal mit Equipment, visuell). Jede Methode wird dabei von einem Übungsleiter geleitet und im **tatsächlichen Umfeld** (z. B. in Verwaltungsräumen, Behandlungsräumen, auf den Stationen bei der Visite, in der Radiologie, usw.) besprochen und/oder durchgeführt. Die Umsetzung einer Übung ist in vier Phasen aufgeteilt:

- **Vorbereitung**: Hier wird zunächst geschaut, welche Notfallpläne und Maßnahmen es gibt, für welche davon eine Übung notwendig ist und was zur Durchführung benötigt wird (z. B. Personal, Einrichtungen, Zeit, Budget). Danach erfolgen die Festlegung des Übungsumfangs, die Ankündigung bei der Geschäftsführung und dem Personal und unter Umständen auch die Miteinbeziehung von Dienstleistern.
- **Planung**: Hier werden das Team zur Durchführung und die Übungsziele festgelegt. Außerdem werden Szenarien (z. B. Dienst-Ausfall) und darin auftretende Ereignisse sowie erwartete angemessene Reaktionen des Übungspersonals erarbeitet. Die Ereignisse werden in eine sinnvolle Reihenfolge für das Szenario gebracht und als Drehbuch zusammengefasst. Zuletzt werden Kriterien zur Auswertung (z. B. Reaktionszeit) erarbeitet.
- **Durchführung**: Hier muss zunächst die Vorbereitung des Schauplatzes, z. B. eines Behandlungszimmers, eingeplant und umgesetzt werden, gefolgt von der eigentlichen Durchführung und Überwachung der Übung, sowie letztlich die Wiederherstellung des Schauplatzes.
- **Nachbereitung**: Hier wird zunächst eine Nachbesprechung mit den Testpersonen inklusive Be-

[7] https://iris.wpro.who.int/bitstream/handle/10665.1/5502/9789290614791_eng.pdf

wertung, Kritik und möglichen Verbesserungsvorschlägen (beiderseits) vorgenommen. Die Ergebnisse werden dann als Bericht zusammengefasst und auf dessen Basis nachfolgende Aktivitäten (z. B. Verbesserung Konzepte und Formulare, weitere Schulung zum Thema XY) definiert.

Das Dokument der WHO bietet für IT-Ausfall-Übungen entsprechende generelle **Checklisten** und **Dokumentvorlagen** zur Organisation aller Phasen.

Prozessübergreifende Übungen

Die meisten Prozesse weisen **Schnittstellen** zu anderen Prozessen auf, beispielsweise folgt auf den Prozess der Patientenanmeldung die Patientenbehandlung. Diese Schnittstellen sind besonders fehleranfällig und werden unter Umständen in Übungen vergessen. Entsprechend ist darauf zu achten, dass sie in den Übungen zumindest berücksichtigt werden.

Geeignete Szenarien

Eine denkbare Auswahl an Szenarien umfasst mindestens die Folgenden:

- Testen von **IT-Notfällen** (einzelne Geräte, Gesamt- bzw. Teil-Netz, einzelne bzw. viele IT-Dienste, Ransomware/unbrauchbare Dateien)
- Testen von **Wiederherstellungsplänen** (Einspielung von Backups, Neu-Installation von IT-Systemen, z. B. Clients für die Verwaltung oder Visite oder für Server und Dienste)
- **Nutzer-Awareness** (sichere Dienstnutzung, Erkennung von Phishing-E-Mails, Vorgehen bei Malware-Infektion, Umgang mit Fremden in internen Bereichen)

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 13 (Personelle und organisatorische Sicherheit)
- **B3S im Krankenhaus** – Kap. 7.8 (Personelle und organisatorische Sicherheit)
- **ISO/IEC 27001** – A.7.2.2 (Informationssicherheitsbewusstsein, -ausbildung und -schulung)
- **BSI IT-Grundschutz-Kompendium** – ORP.2 (Personal)

4.4 Einfache und kostengünstige interne Penetrationstests

Kurzbeschreibung

Penetrationstests sind ein bewährtes Mittel, um Schwachstellen im eigenen Sicherheitskonzept zu finden. Vorgehensweisen echter Angriffe werden dazu insofern angewendet, dass Schwachstellen aufgedeckt, aber nicht ausgenutzt, sondern geschlossen werden. In dieser Maßnahme werden ausgewählte einfache Mittel für interne Penetrationstests vorgeschlagen, die unabhängig vom verfügbaren Budget eines Krankenhauses einsetzbar sind. Die hier genannten Techniken zielen vor allem auf Schwächen in der Nutzer-Awareness ab.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			•

Penetrationstests müssen unbedingt in allen Details mit der Geschäftsführung abgestimmt werden, da sie auch zu negativen Resultaten führen können; im Extremfall sogar zu unzufriedenen Mitarbeitern und einem Misstrauen gegenüber der IT und der Geschäftsführung. Die Nutzer sollten unbedingt darüber informiert werden, dass stichprobenartige Penetrationstests durchgeführt werden.

Umsetzung der Maßnahme

Das Ziel von Awareness-Penetrationstests ist es in erster Linie, die Awareness bei den Anwendern selbst zu steigern. Das geschieht entweder passiv durch das Bewusstsein über das Stattfinden der Tests oder durch das Entdecken einer Schwachstelle und dem erfolgreichen Schließen derselbigen.

Allgemeines

Bei der Organisation sollten einige Aspekte beachtet werden. Mit Rückendeckung der Geschäftsführung sollte den Mitarbeitern im Krankenhaus die Durchführung von Penetrationstests **angekündigt** werden. Außerdem ist es wichtig, den Nutzern direkt zu verdeutlichen, dass es **keine Sanktionen** gibt, wenn sie durch Tests bei Fehlverhalten (z. B. Öffnen einer Phishing-E-Mail) ertappt werden. Über die Ergebnisse kann anonymisiert auch das Personal informiert werden, um Trends zu zeigen und die Thematik „Sicherheit“ im ganzen Haus bewusster zu machen. Auch ist von Bedeutung, die Tests **nicht vorhersehbar** zu gestalten und Regelmäßigkeiten im zeitlichen Verlauf (z. B. nicht jeden Montag um 9:00 Uhr) und im Inhalt (z. B. nicht immer dieselbe Phishing-Mail versenden) zu **vermeiden**. Auch ist es wichtig, nicht immer alle Mitarbeiter, sondern eine zufällige **Stichprobe** zu testen. Denn ein Penetrationstest ist schnell erkannt, wenn die gleiche E-Mail auch im Eingangsordner des Büronachbarn auftaucht.

Simuliertes Phishing

E-Mail und Webbrowsing gehören sicherlich zu den größten Einfallstoren für Malware wie Ransomware. Durch Tests in diesem Bereich können Nutzer besonders viel **Erfahrung** im Umgang damit aufbauen. Betreiber eigener E-Mail-Server können besonders einfach E-Mails hinsichtlich eines ausgedachten Absenders, Betreffs oder E-Mail-Körpers fälschen. So ist es auch sinnvoll, als **Absender vermeintlich kompromittierte Konten** aus dem Krankenhaus zu verwenden, z. B. die E-Mail-Adresse eines miteinbezogeneng echten oder fiktiven Mitarbeiters. Inhalte für den **Betreff** oder **E-Mail-Körper** können auf Basis echter Phishing-Mails zusammengestellt werden oder realitätsnah selbstgeneriert sein. Dabei sollten englische, grammatikalisch fehlerbehaftete deutsche (Standard-SPAM) Texte als auch solche in korrektem Deutsch eingesetzt werden. Letztere sind oft nur bei ausgefeiltem Phishing zu finden, Nutzer müssen jedoch auch diese erkennen können. Unter diesem Aspekt sollte eine abwechslungsreiche Ausgefeiltheit des Inhalts erfolgen: Mit dem Ansprechen fremder Personen in internen Bereichen, dem Verhindern von Tailgating und die strikte Weigerung, interne Informationen herauszugeben.

Zum Fälschen von **URLs** in E-Mails kann der lokale **DNS-Server** im Krankenhaus-Netz genutzt werden, um auf ausgedachte, jedoch augenscheinlich externe Websites zuzugreifen. Durch **Umleiten** der DNS-Anfragen auf einen **lokalen Webserver** kann beispielsweise durch einfaches Zählen des Zugriffs auf diese Websites anonym festgestellt werden, wie viele Nutzer auf eine URL in einer E-Mail geklickt haben.

Im Web finden sich **Software-Werkzeuge**, um Phishing-Penetrationstests durchzuführen und auszuwerten. Eine Open-Source-Variante ist Gophish[8], die beispielsweise bei der Erstellung und dem Versand von Phishing-Mails und anschließender Auswertung hilft.

Zutritt zu Bereichen, Zugriff auf Informationen

Eine weitere einfache Möglichkeit, die Awareness von Mitarbeitern zu überprüfen, sind sicherheitskritische Verhaltensweisen im Alltag. Beispielsweise durch eine dem Personal fremde Person (jedoch in Absprache mit der Geschäftsführung), die augenscheinlich versucht,

[8] https://getgophish.com/

sich Zugang zu Räumen (z. B. durch Warten auf autorisiertes Personal bzw. „Tailgating“), Geräten oder Dokumenten zu verschaffen, oder die sich bereits in internen Bereichen (z. B. Gängen vor der Verwaltung) bewegt.

Auch können simulierte Telefonate (nicht aus dem Krankenhaus-Telefonnetz) zum Penetrationstesten angewendet werden, beispielsweise durch Anrufe am Empfang, in der Verwaltung oder von ausgewähltem medizinischen Personal, verbunden mit dem Versuch, an sensible Informationen wie Patienten- und Personaldaten, interne Informationen über die Krankenhausstruktur und Pläne zu gelangen. Auch ist das Telefon prädestiniert, dass sich Angreifer und Penetrationstester als andere Personen ausgeben, beispielsweise als ein Oberarzt oder als Mitarbeiter der Geschäftsführung.

Die Reaktionen des Personals auf diese Penetrationstests sollten entsprechend den herausgegebenen Richtlinien des Krankenhauses erfolgen, beispielsweise fremde Personen in internen Bereichen ansprechen, Tailgating verhindern und auf keinen Fall interne Informationen herausgeben.

Weitere Möglichkeiten

Vielen Nutzern ist oft nicht bewusst, dass vermeintlich einfache Speichermedien wie **USB-Sticks** ebenfalls alleine durch Einstecken in einen PC Malware verbreiten können. Angreifer platzieren diese in größerer Zahl potenziell auf dem Grundstück des Krankenhauses, wodurch die Wahrscheinlichkeit, dass ein Mitarbeiter einen findet und einsteckt, relativ hoch ist. Das Erstellen eines präparierten USB-Sticks ist jedoch nicht so einfach – einzelne Dienstleister bieten aber einen derartigen Penetrationstest an.

Schwachstellenbehandlung

Erkannte Schwachstellen in der Sicherheitsawareness der Mitarbeiter müssen geeignet geschlossen werden. Strafen bei Fehlverhalten sollten möglichst vermieden werden, vielmehr muss der Grund (z. B. fehlendes Wissen, Unachtsamkeit, usw.) für das Fehlverhalten ermittelt werden. Einige Lücken können dann individuell oder als breit angesetzte Kampagne (z. B. mit Postern, Videos, internen oder externen Seminaren) geschlossen werden.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 13 (Personelle und organisatorische Sicherheit)
- **B3S im Krankenhaus** – Kap. 7.8 (Personelle und organisatorische Sicherheit), 7.10 (Überprüfungen im laufenden Betrieb)
- **ISO/IEC 27001** – A.18.2.2 (Einhaltung von Sicherheitsrichtlinien und -standards)
- **BSI IT-Grundschutz-Kompendium** – ORP.2 (Personal)

Kapitel 5

Netzsicherheit

Als Netzsicherheitsmaßnahmen werden in diesem Katalog Maßnahmen bezeichnet, die entweder Komponenten oder die Struktur des Krankenhausnetzes betreffen, oder aber zentral implementiert werden und zur Absicherung des gesamten Netzes beitragen. Entsprechend bilden solche Maßnahmen eher „Quick Wins“, können also mit relativ wenig Aufwand sehr viel bewirken und sind daher, wenn möglich, dezentralen Maßnahmen hinsichtlich des Aufwands vorzuziehen. Die ausgewählten Maßnahmen sind nach Dringlichkeit geordnet:

- Zunächst sollte der Übergang zum Internet gesichert und eine grobe Zonenstruktur angelegt werden.
- Das interne Krankenhaus-Netz kann dann in feingranularere Zonen eingeteilt werden, um Vorfälle zu vermeiden oder mindestens zu begrenzen.
- Grundsätzlich ist ein zentralisiertes Nutzermanagement einzurichten sowie
- eine zentrale Überwachung des Netzes, um Probleme, (Malware-) Infektionen und Angriffe zu erkennen.
- Außerdem ist es essenziell, klassische Einfallswege für Angriffe und Malware im Krankenhaus zu schließen.
- Aufgrund der Relevanz des WLAN-Dienstes im digitalisierten Krankenhaus wird auch dessen Absicherung angesprochen.

Die hier beschriebenen Maßnahmen sind überwiegend technischer Natur und richten sich vor allem an die IT-Abteilung im Krankenhaus.

5.1 Absicherung des Netzzugangs und generelle Netz-Zonen

Kurzbeschreibung

In einem Krankenhausnetz gibt es üblicherweise einen zentralen Netzausgang ins Internet. Dieser und dahinterstehende Dienste müssen durch ein geeignetes Grundkonzept und vor allem auch Einzelmaßnahmen gegen typische Angriffe abgesichert werden.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			•
IT-Abteilung	•		
Personal/Nutzer			

Die Absicherung des Netzausgangs und die Realisierung des generellen Netz-Zonen-Konzepts müssen durch die IT-Abteilung in Abstimmung mit der Geschäftsleitung umgesetzt werden.

Umsetzung der Maßnahme

Bei der Absicherung des Netzausgangs müssen folgende Aspekte berücksichtigt werden:

- Welche Dienste müssen aus dem Internet (z. B. für Telearbeit) erreichbar sein?
- Welche Dienste müssen miteinander kommunizieren können?
- Welche Funktionen muss der Router zum Internet bereitstellen können?
- Wie können kompromittierte Systeme einfach eingedämmt werden?

Es hat sich bewährt, ein grobes Zonenkonzept und eine Trennung in das **interne LAN**, ein **Management-Netz** zur zentralen Sammlung und Auswertung von Monitoring-Informationen aller Dienste und Systeme, das **externe Netz** (d. h. Internet), sowie eine dazwischenliegende, sogenannte **demilitarisierte Zone** (DMZ) umzusetzen. Dabei sollte beachtet werden, dass jede Zone zur besseren Handhabbarkeit ein eigenes IP-Netz darstellt. Für das Management-Netz sowie die DMZ reichen oft kleinere $/24$-Netze mit jeweils 254 nutzbaren IPv4-Adressen. Für das Krankenhaus-LAN hingegen mit allen Clients und lokalen Diensten sollte ein größeres $/16$ Netz mit 65534 nutzbaren IPv4-Adressen vorgesehen werden. Wie in Maßnahme 5.2 Logische Aufteilung des Krankenhausnetzes beschrieben, kann das Krankenhaus-LAN für eine bessere Trennung von Diensten weiter segmentiert werden.

Im Internet öffentlich erreichbare IT-Dienste des Krankenhauses stellen eine signifikante Angriffsmöglichkeit für Angreifer dar. Um durch einen kompromittierten öffentlichen IT-Dienst nicht die Sicherheit des gesamten Krankenhaus-LAN zu gefährden, werden genau diese in die DMZ gelegt. Die DMZ ist jeweils durch einen NAT-Router sowie eine Firewall sowohl vom internen Krankenhaus-LAN als auch vom externen Internet getrennt. Das Management-Netz liegt dabei im Krankenhaus-LAN, ist jedoch ebenfalls davon getrennt.

Bei der Absicherung des eigentlichen **Netzausgangs** müssen ebenfalls einige Gefahren berücksichtigt werden, die den Krankenhausbetrieb beeinträchtigen oder kompromittieren können:

Verfügbarkeit des Netzes: Als Krankenhaus-Betreiber sollte man sich nicht auf eine einzige Internet-Anbindung und einen einzigen Internet-Provider verlassen. Es muss eine zweite getrennte Leitung eines anderen Anbieters existieren, welche zumindest temporär (bei Ausfall der Hauptleitung) den Krankenhausbetrieb aufrecht erhalten kann. Dazu muss der Router zwischen DMZ und Internet einen **Fall-Back-Port** unterstützen. Der Router schaltet also bei Ausfall der Hauptleitung dann automatisch auf die Fall-Back-Leitung des zweiten Anbieters. Um die Ausfallsicherheit zu erhöhen, ist es zudem ratsam, zwischen DMZ und Internet auch einen Fall-Back-Router zu haben, welcher einspringt, sobald ein Router ausfällt (z. B. wegen Software-Updates, siehe unten).

Schließen trivialer Schwachstellen: Praktisch für alle Router zwischen den beschriebenen Netzen gilt, dass vor allem triviale Angriffe präventiv verhindert werden müssen. Sehr oft werden Router allein aufgrund ihrer Standard-Konfiguration kompromittiert. Einstellungen betreffend der voreingestellten **IP-Adressen**, **Suchdomains**, **Benutzernamen** und **Passwörter** müssen unbedingt geändert werden. Andernfalls ist es für Angreifer in der Regel sehr leicht, den Router (auch aus dem Internet) zu kompromittieren. Default-IP-Adressen und URLs erlauben dem Angreifer die schnelle Identifikation des Routers im Netz und ermöglichen auch komplexere, sehr wirksame Angriffe wie Cross-Site-Request-Forgery (CSRF).[1] Auch bei den Nutzernamen sollten Standard-Einträge („root“, „Administrator“, „admin“) deaktiviert und individuelle angelegt werden.

Zugriff auf die Konfigurationsoberfläche einschränken: Der Zugriff auf die Konfigurationsoberfläche eines Routers aus dem Internet muss zudem verboten werden. Entweder muss dies durch den Router selbst unterstützt werden oder aber über entsprechende Firewall-Regeln auf das lokale Netz, am besten auf ein bestimmtes Gateway im Netz, beschränkt werden. Durch die Zugriffsbeschränkung auf ein einzelnes Gate-

[1] https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF)

way werden auch Manipulationsversuche aus dem lokalen Netz deutlich erschwert.

Unnötige Dienste und Port-Weiterleitungen: Manche Router bieten von sich aus bereits Dienste und Port-Weiterleitungen in den Default-Einstellungen an. So sollte **Universal Plug-and-Play** (UPnP) bei Routern deaktiviert werden, sofern es nicht benötigt wird. Unterstützt der Router die Deaktivierung der Funktion nicht, dann hilft hier ebenfalls eine entsprechende Firewall-Regel. Port-Weiterleitungen am Router müssen regelmäßig auf ihre Funktion und Notwendigkeit geprüft werden. Alle nicht mehr benötigten Weiterleitungen stellen ein potenziell gravierendes Sicherheitsproblem dar und müssen geschlossen werden.

Automatische Softwareupdates: Vor allem veraltete Software und ihre (oft öffentlich in der CVE-Datenbank o. ä. dokumentierten) Schwachstellen sind ein Grund für kompromittierte Systeme. Bei öffentlich erreichbaren Diensten und Systemen, vor allem auch den Routern zwischen DMZ und Internet, sollte daher die automatische Update-Funktion aktiviert sein. Die redundanten Router dürfen dabei nicht gleichzeitig aktualisiert werden, damit, falls die neue Softwareversion fehlerhaft ist, nicht beide gleichzeitig außer Betrieb gesetzt werden.

Zentrale Überwachung: Der Netzausgang ist die am besten geeignete zentrale Stelle des Krankenhausnetzes, um ein Netzüberwachungssystem zu installieren (siehe Maßnahme 5.4 Zentralisierte Überwachung ■). So können unberechtigte und auffällige Zugriffe von außen sowie auffälliger Netzverkehr aus dem LAN (z. B. durch Malware) erkannt werden. Dazu sollte der Router die Port-Spiegelung („Mirror-Port“) unterstützen, um den Verkehr am Netzausgangsport auf einen anderen Port zu einem Intrusion-Detection-System zu spiegeln. Dies ist auch beim Fall-Back-Router anzuwenden.

Sicheres VPN: VPN spielt auch für Krankenhäuser eine große Rolle, insbesondere in der immer mehr aufkommenden Tele-Arbeit („Home-Office“). Viele Router bieten bereits einen VPN-Server an, der einfach zu konfigurieren ist und ad-hoc funktioniert. Es sollte lediglich darauf geachtet werden, dass sichere Protokolle verwendet werden. Das vormals beliebte PPTP (Point-To-Point Tunneling Protocol) gilt als nicht mehr sicher und sollte auf keinen Fall mehr dafür verwendet werden. Ebenfalls verbreitete Alternativen, wie OpenVPN, IPsec oder Wireguard, sind zu bevorzugen.

Testen der Konfiguration: Ein weiterer wichtiger Aspekt ist das Testen der Konfiguration. In Abstimmung mit der IT-Leitung (unter Umständen auch mit der Geschäftsleitung) sollte die Konfiguration der Router von außen (z. B. von einem anderen Standort über das Internet) getestet werden. Dazu zählen **Port-Scans** (welche Ports sind nach außen hin offen und welche Dienste laufen dahinter, z. B. mit Tools wie *nmap*) oder Schwachstellenscans (frei nutzbare Systeme wie *OpenVAS* können bekannte Schwachstellen in Software detektieren). Freie Linux-Distributionen, wie *Parrot OS* oder *Kali Linux* bieten einige Software-Tools zur Identifikation von Schwachstellen in Systemen.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 11 (Robuste/resiliente Architektur), 19 (Netz- und Systemmanagement), 31 (Protokollierung und Auswertung)
- **B3S im Krankenhaus** – Kap. 7.13.1 (Netz- und Systemmanagement (Netztrennung und Segmentierung)), Kap. 7.13.2 (Absicherung Fernzugriffe), Kap. 7.13.3 (Härtung und sichere Basiskonfiguration der System und Anwendungen), Kap. 7.13.7 (Sichere Authentisierung)
- **ISO/IEC 27001** – Maßnahmenziele A.13.1.3 (Trennung von Netzen)
- **BSI IT-Grundschutz-Kompendium** – NET.3.1 (Router und Switches), BSI TR-03148 (Sichere Breitband Router)

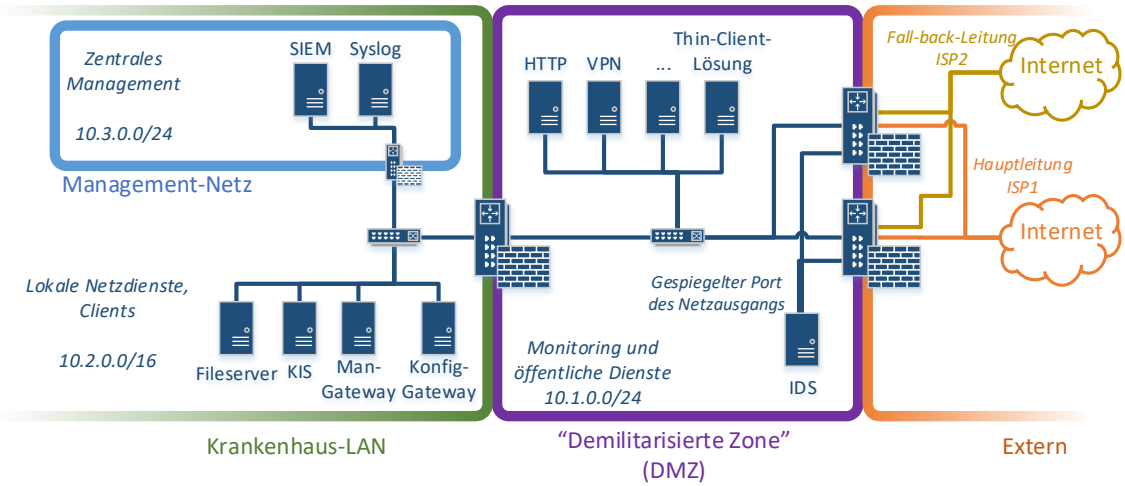


Abbildung 5.1: Generelles Netz-Zonen-Konzept

5.2 Logische Aufteilung des Krankenhausnetzes ■

Kurzbeschreibung

Eine zur Maßnahme 5.1 Absicherung des Netzzugangs und generelle Netz-Zonen ■ weiterführende Aufteilung eines (Krankenhaus-) Netzes wird auch als Netzsegmentierung bezeichnet. Sie teilt das interne Netz in weitere Sub-Netze ein, um unerlaubten Dienst-Zugriff (z. B. auch durch infizierte Hosts und Krypto-Trojaner) zu unterbinden. Die Maßnahmenbeschreibung soll bei der Umsetzung dieser komplexen Aufgabe unterstützen und Verantwortlichen geeignete Vorgehensweisen aufzeigen.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	•
IT-Abteilung	•		
Personal/Nutzer			•

Eine Netzsegmentierung schneidet massiv in die Abläufe eines Krankenhauses ein und kann bei mangelhafter Umsetzung den Betrieb stark beeinträchtigen (z. B. Nicht-Verfügbarkeit wichtiger Dienste). Die Geschäftsführung muss in die Planung einbezogen werden und das Vorgehen genehmigen. Nutzer sollten abgefragt werden, ob es durch die Netzsegmentierung zu Einschränkungen jeglicher Art gekommen ist (Fehlkonfiguration).

Umsetzung der Maßnahme

Maßnahme 5.1 Absicherung des Netzzugangs und generelle Netz-Zonen ■ beschreibt eine grundlegende grobe Netzsegmentierung und trennt die Krankenhaus-Infrastruktur in ein **internes LAN**, ein **Managementnetz**, **öffentlich erreichbare Dienste** (DMZ) und ein **externes Netz**. Weitere Netzsegmentierung betrifft vor allem die Einteilung des Krankenhaus-**LAN**, u. U. auch Krankenhaus-**MAN/WAN** (bei mehreren Standorten).

Die Maßnahme wird anhand eines Beispiels beschrieben, das in der dieser Maßnahme angehängten Abbildung illustriert wird.

Ausgangsbasis für Netzsegmentierung

Um Netzsegmentierung effektiv gestalten zu können, muss in der Praxis Maßnahme 3.5 Identifikation kritischer Systeme im Krankenhaus ■ in der beschriebenen oder einer anderen effektiven Art und Weise umgesetzt worden sein. So oder so sollten für eine strukturierte Netzsegmentierung die folgenden Informationen bekannt sein:

1. kritische Prozesse und sie unterstützende **Anwendungen** (z. B. KIS, LIS, PACS, usw.),
2. **Hintergrund-Systeme** der Anwendungen sowie ihre Kommunikation untereinander.

Die folgenden Schritte können zu einer ersten oder auch ausgebauten Segmentierung des Krankenhaus-LAN genutzt werden. Zur Segmentierung empfiehlt es sich, **tagged VLANs** zu nutzen, da diese deutlich flexibler sind als port-basierte Varianten und einfacher als eine umfangreiche IP-basierte Trennung von Netzen umzusetzen ist.

Subnetz und Gateways für zentrale unterst. Dienste

Zentrale unterstützende Dienste sind beispielsweise ein Verzeichnissystem (LDAP, Active Directory) und zentrale Fileserver (Samba, NFS, usw.), die von Anwendungen für unterschiedliche Zwecke genutzt werden. Diese sollten von klassischen Nutzer-Clients nicht alle gleichartig erreichbar sein und in einem eigenen Subnetz liegen.

Falls diese Dienste doch von Clients aus erreichbar sein müssen, bietet es sich an, **Zugriffs-Gateways** einzurichten, welche sich in jeweils **beiden Subnetzen** der Dienste bzw. Clients befinden. Der Zugriff kann von technischer Seite über einen SSH-Tunnel (auch passwortlos mit Public-Key-Authentifizierung und entsprechend restriktiv konfiguriert) oder auch über VPN erfolgen.

Einrichtung von Subnetzen für Anwendungen

Anwendungen bezeichnen hier zentrale Nutzerdienste, um einen Prozess (z. B. Patientenaufnahme) zu unterstützen. Zunächst sollte damit angefangen werden, Teil-Systeme, die direkt zur Umsetzung der jeweiligen Anwendungen installiert sind, in ein Subnetz zu legen. Im Beispiel in der dieser Maßnahme angehängten Illustration setzt sich das KIS aus mehreren Teilsystemen (orange) zusammen. Auch gibt es monolithische Dienste, wie im Beispiel das Laborinformationssystem (LIS), das grundsätzlich einfacher zu behandeln ist.

Subnetze gemäß Kommunikationsbeziehungen

Systeme, welche nun mit den jeweiligen zentralen Anwendungen kommunizieren, können nun ebenfalls in ein gemeinsames Subnetz mit **Schnittstellen-Systemen** gelegt werden. Das sind im Falle des KIS beispielsweise einerseits konkrete Clients (z. B. für **Visite** oder in **Behandlungszimmern**). Diese müssen jedoch nicht mit allen KIS-Teilsystemen kommunizieren können, sondern nur zu **KIS-Zugangspunkten** (z. B. mit dem jeweiligen System mit Webservice).

Auf der anderen Seite müssen üblicherweise **medizinische Geräte** über entsprechende Schnittstellen mit

dem KIS kommunizieren. Diese müssen aber auch nicht mit allen KIS-Systemen oder den KIS-Zugriffspunkten kommunizieren, sondern nur mit entsprechenden Systemen, welche HL7-konforme Schnittstellen anbieten. Folglich gehören medizinische Geräte und KIS-Schnittstellen-Systeme in gleiche Subnetze.

Im Beispiel des monolithischen Dienstes **LIS** ist eine derartige genaue Differenzierung nicht möglich. Jedoch sollten beispielsweise **Laborgeräte** und **zugreifende Clients** voneinander **getrennt** werden. Das heißt, das LIS kommt in zwei (oder mehr) Subnetze, damit Laborgeräte nicht direkt von Clients aus angesprochen werden können.

Subnetze für Abteilungen

Zudem ist eine weitere Aufteilung des Netzes nach **Abteilung** bzw. Organisationbereich hilfreich. So kann der unerlaubte abteilungsübergreifende Zugriff auf Systeme unterbunden werden. Im Beispiel wird dies für zwei unterschiedliche Verwaltungsabteilungen demonstriert. Diese haben dann beispielsweise jeweils ein eigenes Subnetz und ein darin befindliches Gateway, das etwaigen Zugriff auf benötigte zentrale Dienste von den Clients aus ermöglicht.

Eine weitere sehr effektive Maßnahme, beispielsweise zur Eindämmung von Computer-Viren, -Würmern oder Malware im Allgemeinen, ist die **Unterbindung** von **Client-zu-Client-Kommunikation** im selben Subnetz (vgl. Verwaltungssubnetz 1 und 2). Dies ist beispielsweise durch den zusätzlichen Einsatz einer Firewall und entsprechende Konfiguration möglich. Genutzte Gateways sollten jedoch davon ausgeschlossen (gleichzeitig aber anderweitig gehärtet) sein.

Hinweise zur Segmentierung

- **Fernwartung-Gateways medizinischer Geräte** sollten ebenfalls in einem eigenen Subnetz mit den jeweiligen medizinischen Geräten sein. So wird verhindert, dass Fernwartung-Gateways zur Kompromittierung des Netzes genutzt werden.
- Das **Management-Gateway** zur zentralen Speicherung von Log-Dateien usw. muss von allen Geräten aus erreichbar sein.
- **Monitoring** und **Pen-Tests** sollten zur Absicherung der Wirksamkeit der Netzsegmentierung eingesetzt werden.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 19 (Netz- und Systemmanagement), 20 (Absicherung Fernzugriffe), 31 (Protokollierung und Auswertung)
- **B3S im Krankenhaus** – Kap. 7.13.1 (Netz- und Systemmanagement (Netztrennung und Segmentierung))
- **ISO/IEC 27001** – A.12.2 (Schutz vor Schadsoftware), A.13.1.3 (Trennung von Netzwerken)
- **BSI IT-Grundschutz-Kompendium** – NET.1.1 Netzarchitektur und -design

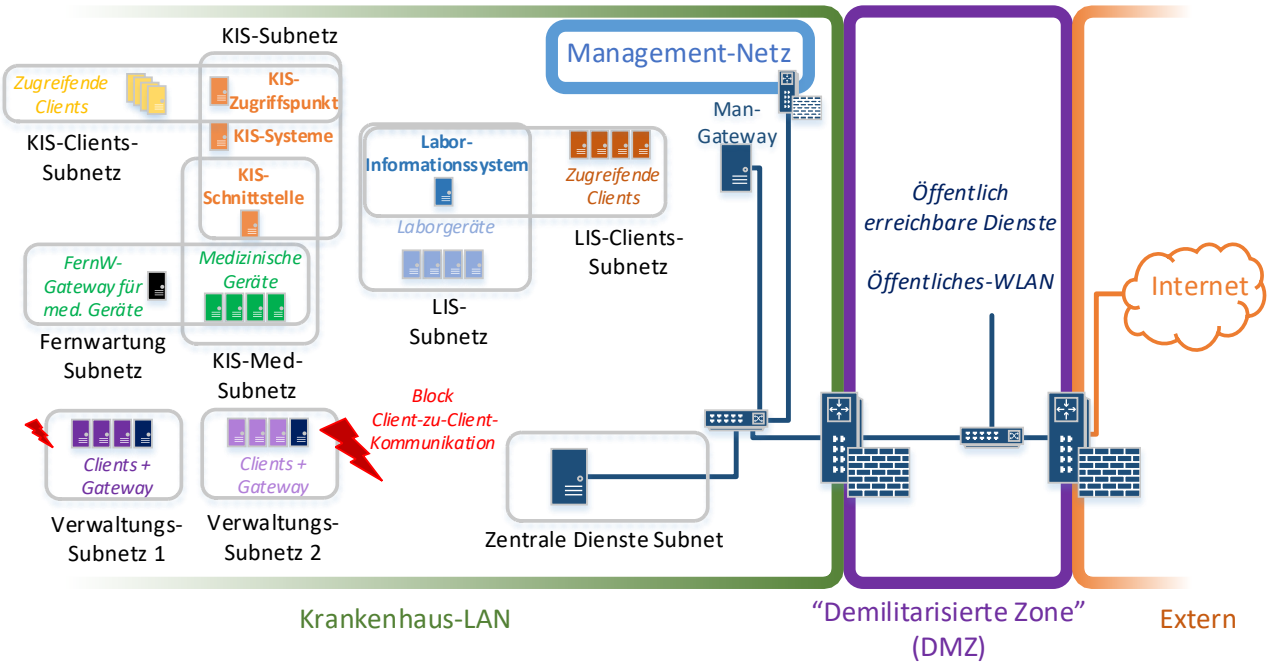


Abbildung 5.2: Beispiel Netzsegmentierung

5.3 Zentralisiertes Nutzermanagement

Kurzbeschreibung

*Ein zentralisiertes Nutzermanagement ist eine der wichtigsten Maßnahmen, um eine sinnvolle **Zugangskontrolle** im Netz aufrechtzuerhalten, unabhängig von der Größe des jeweiligen Krankenhauses. Es erlaubt eine zuverlässige Verwaltung von Identitäten und Rechten, spart den Verantwortlichen sehr viel Zeit im Gegensatz zu einem dezentralen Nutzermanagement und ermöglicht es erst, den Überblick über IT-Nutzer im Krankenhaus zu behalten.*

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			

Für die Umsetzung eines zentralisierten Nutzermanagements ist die IT-Abteilung zuständig. Da diese Umsetzung relativ weitreichende Konsequenzen hat (betrifft in der Regel die meisten IT-Systeme), sollte die Geschäftsführung diese Maßnahme genehmigen.

Umsetzung der Maßnahme

Zur Umsetzung dieser Maßnahme sind einfache und ausgereifte Ansätze in der Praxis auf **zwei Implementierungen** beschränkt: Einerseits das Aufsetzen eines Lightweight Directory Access Protocol (**LDAP**)-basierten (teilweise Open-Source-Systeme) oder eines Active Directory (AD)-basierten Directory-Servers, der vorwiegend in stark Windows-lastigen Umgebungen zu finden ist.

Generelle Funktionsweise

Generell muss zwischen einer **dezentralisierten** Nutzerverwaltung (d. h. Nutzer werden auf jedem Gerät verwaltet) und einer **zentralisierten** Nutzerverwaltung (d. h. Nutzer im Netz werden an einem Punkt/System verwaltet) unterschieden werden. Ersteres erfordert sehr viel Aufwand und ist nach Möglichkeit zu vermeiden, weshalb Letzteres klar zu bevorzugen ist.

Bei einer **zentralisierten** Nutzerverwaltung werden Nutzerkonten auf einem System im Netz angelegt, modifiziert und wieder gelöscht. Das erspart Administratoren nicht nur sehr viel Zeit, sondern trägt auch essenziell zur Sicherheit bei, da die IT-Abteilung den Überblick über Nutzer und ihre jeweiligen Berechtigungen behält. So ist die Wahrscheinlichkeit geringer, dass beispielsweise bei Ausscheiden eines Mitarbeiters aktive Kennungen auf Systemen vergessen werden und bestehen bleiben.

Jedoch erfolgt auch die Authentifizierung bei einer zentralisierten Verwaltung unterschiedlich: Anstatt individuell und lokal auf jedem System, erfolgt stattdessen eine **Authentifizierung** via Abfrage über das Netz bei dem jeweiligen Directory-Server.

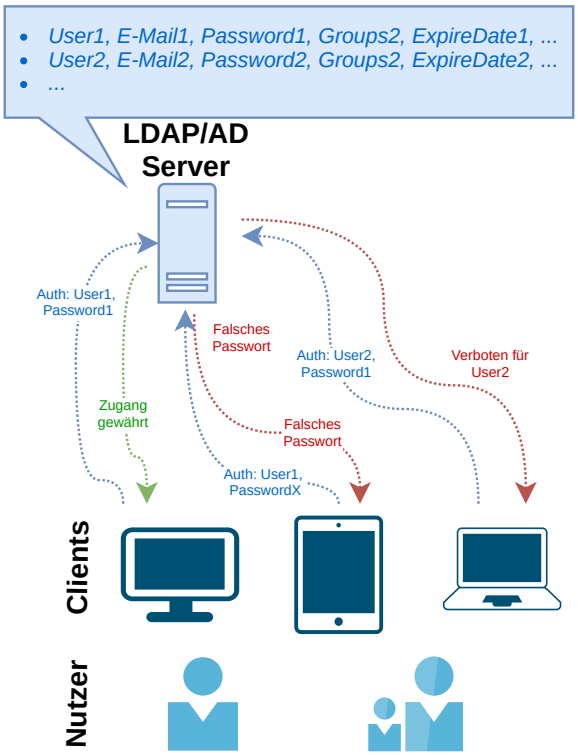


Abbildung 5.3: Zentrale Nutzerverwaltung und Authentifizierung (vereinfacht dargestellt)

Autorisierung über Gruppen

In einem Directory-Dienst kann die **Autorisierung** (d. h. „*Wer darf was nutzen?*“) an einem Dienst (z. B. KIS, Dateiablage) oder die eines Clients (z. B. med. Client, PC in Verwaltung) anhand unterschiedlicher Attribute eines Nutzers erfolgen. Geeignet sind generell **Gruppen**zugehörigkeiten von Nutzern (in LDAP bspw. *OrganizationalUnits* bzw. *ou*), durch welche beispielsweise auch das Krankenhausnetz unterteilt werden kann. Es könnten Gruppen angelegt werden für

- **Stationen** (z. B. Chirurgie, Kardiologie, Innere Medizin, Radiologie),
- **Verwaltungsabteilungen** (z. B. Geschäftsführung, Buchhaltung, Prozesse, Personal, Beschaffung) oder
- **Technikabteilungen** (z. B. IT-Abteilung, Haustechnik, Netze, Server, Clients).

Je nach Umgebung sind durchaus auch andere Gruppen oder feingranularere Strukturen denkbar. Nutzer können dann einer oder mehreren Gruppen zugewiesen werden, durch welche ihre jeweilige Berechtigung ausgedrückt wird. Beispielsweise dürfen sich auf einem Rechner des Personalmanagements im Verwaltungsgebäude des Krankenhauses nur Personen anmelden, die der Gruppe **Personal** (sowie u. U. noch weiteren, wie z. B. *Buchhaltung*) im Directory-Server zugewiesen sind.

Sicherheitsvorkehrungen

Soweit möglich, sollten sich Nutzer selbst auch ausschließlich über eine Authentifizierung und Autorisierung via Directory-Server an einem System anmelden können. Doppelte Mechanismen (z. B. Authentifizierung lokal oder via Directory-Server) müssen weitestgehend vermieden werden, da sie ansonsten eine überaus unübersichtliche Umgebung schaffen, in der Fehler potenziell häufiger vorkommen als in einer **eindeutigen, zentralisierten Lösung**.

Jedoch sind einzelne Ausnahmen sinnvoll, insbesondere im Krankenhausbetrieb, in dem medizinische Prozesse stark von der IT-Infrastruktur abhängen. Deshalb sollte eine Anmeldung für Nutzer und eine Verwaltung von Rechnern durch die IT auch dann noch möglich sein, wenn der Directory-Server **nicht mehr verfügbar** ist. Das kann durch zahlreiche Ereignisse passieren, beispielsweise durch einen Hardware-Defekt, Software-Fehler, eine Kompromittierung, einen Stromausfall, einen Teil-Netz-Ausfall, falsch konfigurierte Netzkomponenten wie Switches oder Router, und viele mehr. Für diese Fälle sind folgende Ausnahmen sinnvoll:

- Die Bereitstellung eines **redundanten Directory-Servers**, im Falle eines Software- oder Hardware-Defekts des primären Servers (hier ist beispielsweise das Redundanzkonzept aus Maßnahme 7.2 Patchen zentraler Dienste mit geringer Auswirkung auf den Krankenhausbetrieb ■ anwendbar).
- Die Einrichtung eines **Notfallnutzers** auf allen lokalen Systemen bei bestehender Notwendigkeit. Ist der Directory-Server gar nicht mehr erreichbar, kann so eine Anmeldung unabhängig von der Netzinfrastruktur erfolgen. Die Zugangsdaten sollte jedoch pro Abteilung nur eine zentrale, vertrauenswürdige Person (z. B. Oberärzte, Abteilungsleiter) kennen und einsetzen können.
- Die Einrichtung eines **Administrator-Nutzers** auf jedem lokalen System. Dieser Nutzer dient der IT-Abteilung zur Aufrechterhaltung der Verwaltbarkeit von IT-Systemen, auch ohne Directory-Dienst. Die Zugangsdaten sollten hier nur der IT-Abteilung bekannt sein.

Daneben sollte grundsätzlich bei der Konfiguration und Einrichtung eines Directory-Servers sichergestellt werden, dass die Kommunikation mit den Clients ausschließlich **verschlüsselt** (z. B. über TLS) geschieht.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 11 (Robuste/resiliente Architektur), 14 (Ordnungsgemäße Systemadministration), 24 (Identitäts- und Rechtemanagement)
- **B3S im Krankenhaus** – Kap. 7.13.6 (Identitäts- und Rechtemanagement), Kap. 7.13.7 (Sichere Authentisierung), Kap. 7.13.8 (Kryptographische Absicherung)
- **ISO/IEC 27001** – A.9 (Zugangssteuerung)
- **BSI IT-Grundschutz-Kompendium** – APP.2.1 (Allgemeiner Verzeichnisdienst), APP.2.3 (OpenLDAP), APP.3.1 (Webanwendungen), ORP.4 (Identitäts- und Berechtigungsmanagement)

5.4 Zentralisierte Überwachung ■

Abbildung 5.4: Ausbaustufenkonzept Netzüberwachung

Kurzbeschreibung

*Eine zentrale Überwachung ist ein wichtiger Teil des Netzmanagements und kann unterschiedlichste Facetten haben. Dazu gehören die Überwachung des **Netzverkehrs**, die zentrale **Auswertung von Logs**, die Überwachung zentraler **Dienste und Dienst-Inhalte** oder auch aktive **Scans**. Das Ziel ist eine Überwachung von Einfallswegen, wie E-Mail, und die frühzeitige Erkennung von Angriffen.*

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			

Die Umsetzung muss durch die IT-Abteilung vorgenommen werden; insbesondere die Überwachung von Nutzerinhalten (z. B. Web-Inhalte, E-Mails, usw.) sollte mit der Geschäftsführung, der Datenschutzstelle und der Personalvertretung abgestimmt werden.

Umsetzung der Maßnahme

Die Netzüberwachung muss unabhängig von Größe und Ausreifung in jedem Krankenhaus geeignet umgesetzt werden. Einige Maßnahmen können sehr schnell bei sehr breiter Abdeckung umgesetzt, andere können darauf aufbauend installiert werden. Die folgende Auflistung ist dementsprechend von grundlegenden bis hin zu fortgeschrittenen Maßnahmen geordnet.

Network Intrusion Detection System

Ein Network Intrusion Detection System (NIDS) ist eine meist zentral im Netz bzw. am Netzausgang sowie an internen Zonenübergängen installierte Anwendung zur Detektion von **auffälligem** oder durch **Malware im Netz** generiertem Netzverkehr. Die Einrichtung ist daher mit vergleichsweise wenig Aufwand bei gleichzeitig großer Abdeckung verbunden und somit auch für Krankenhäuser mit wenigen Personal-Ressourcen geeignet.

Ein geeigneter Installations-Ort ist nah am Router zwischen internem Netz und Internet, angeschlossen an einem **gespiegelten Port** (Port-Mirror) des Netzausgangs (Fall-Back-Router müssen gleichermaßen mit dem NIDS verbunden sein). So wird jeglicher ins Krankenhaus-Netz eingehender und ausgehender Netzverkehr überwacht. Je nach Größe eines Krankenhaus-Netzes muss darauf geachtet werden, dass das NIDS **Multi-Threading** unterstützt.

Ein NIDS arbeitet dabei in der Regel mindestens signaturbasiert (vergleichbar mit einem Virenscanner auf PCs) oder auch mit einem speziellen Satz an Regeln zur Erkennung von Anomalien im Netzverkehr. Hier muss auf ein NIDS mit aktiver Community oder einem zuverlässigen Hersteller geachtet werden, die bzw. der stets aktuelle **Signatur-Updates** zur Verfügung stellt.

Dabei gibt es auch etablierte Open-Source NIDS, wie **Suricata** oder **Zeek**. Ersteres ist vergleichsweise nutzerfreundlich, Letzteres bietet im Gegensatz zu Suricata auch Anomalie-Detektion. GUIs müssen bei beiden über Drittpakete installiert werden.

Zentrales Logging

Das zentrale Sammeln von Logs ist eine fundamentale (wenn auch aufwendigere) Maßnahme zur Ursachenfindung bei IT-Problemen. Jedoch einmal umgesetzt, **spart es viel Zeit**, da im Problemfall nicht auf jeden Dienst und jedes System einzeln zugegriffen werden muss, sondern alles an einem Ort im Netz liegt. Bereits ab wenigen Dutzend Systemen ist zentrales Logging – auch im Hinblick auf ein tendenziell wachsendes Netz – sehr empfehlenswert.

Der zentrale **Log-Server** sollte im Management-Netz (vgl. Maßnahme 5.1 Absicherung des Netzzugangs und generelle Netz-Zonen ■) liegen, der Netzverkehr zwischen Diensten bzw. Rechnern und dem Log-Server muss an der Firewall freigeschaltet bzw. weitergeleitet (NAT-Port-Forward) werden. Nebenbei unterstützen ebenfalls viele Netzkomponenten, wie Switches und Router, eine Logging-Funktionalität. Ein Workaround für Netzkomponenten ohne Remote-Syslog-Funktionalität bietet ein regelmäßiges Kopieren der jeweiligen Log-Datei(en) über SSH auf den zentralen Log-Server. Der Log-Server muss vor allem sehr viel (einfach erweiterbare) Speicherkapazität bereitstellen; Laufwerke mit Log-Daten sollten generell verschlüsselt werden (z. B. mit LUKS oder BitLocker).

Verwendbare Log-Software ist ebenfalls zahlreich verfügbar. Ein einfaches System ist *syslog-ng*, das *rsyslog* ersetzt hat. Es ist jedoch empfehlenswert, auf mehr **Funktionalität** zu achten: Eine **(Web-)GUI** mit Such- und Filterfunktion erleichtert die Arbeit enorm. Zudem

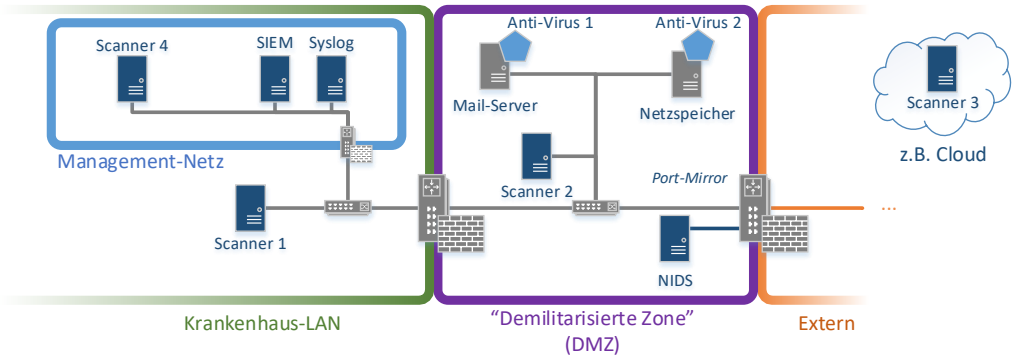


Abbildung 5.5: Gesamtkonzept Netzüberwachung

muss sowohl ein Client als auch ein Server eine **sichere Kommunikation** (Authentifizierung, Autorisierung, Verschlüsselung) via TLS oder ähnlichem unterstützen, denn Log-Daten sind sehr schützenswerte Informationen. Auch müssen **Zeitstempel** einheitlich und präzise sein (z. B. DIN ISO 8601 oder RFC 3336-konform). Gängige Log-Software erfüllt viele dieser Anforderungen.

Überwachung von Dienstinhalten

Ähnlich wie eine Überwachung des Netzverkehrs ist es ebenfalls möglich und sinnvoll, zentrale Dienste, wie vor allem eine **Dateiablage** im Netz (z. B. klassische CIFS- oder NFS-basierte NAS-Systeme, jedoch auch modernere „Cloud Computing"-Systeme wie OwnCloud, NextCloud, usw.) oder auch **E-Mail** hinsichtlich Malware zu überwachen. Dabei darf dennoch die Privatsphäre der Datei- und Mail-Inhaber nicht unberücksichtigt bleiben – die Maßnahmen müssen sich auf die Detektion von Malware durch geeignete Anti-Viren-Software beschränken. Betroffene Dateien sollten in eine (üblicherweise von der Anti-Viren-Software selbst) kontrollierte *Quarantäne* verlegt und betroffene Nutzer (z. B. per E-Mail) benachrichtigt werden.

Aktives Scannen

Eigenes aktives Scannen des Netzes ist eine zuverlässige Maßnahme der Netzüberwachung, um Schwachstellen im Netz aufzudecken. Klassische, bereits hilfreiche Methoden sind **Dienst- und Port-Scans** (z. B. mit nmap) und Schwachstellen-Scans (z. B. OpenVAS) in den einzelnen Netzsegmenten (**LAN**, **DMZ**, von **Extern**), welche zu unterschiedlichen Ergebnissen führen. Das Scannen ausgehend vom Krankenhaus-LAN (z. B. über ein über WLAN eingebundenes Gerät) gibt die Nutzer-Sicht zurück – d. h. welche Systeme und Dienste kann ein Nutzer erreichen. Die Sicht aus der DMZ zeigt, was z. B. ein Angreifer ausgehend von einem kompromittierten Rechner in der DMZ sehen kann. Das Scannen von außen (z. B. über einen gemieteten Host bzw. Cloud-Dienst oder einen vertrauenswürdigen Web-Dienst) gegen den externen Router zeigt die Sicht auf alle aus dem Netz erreichbaren Dienste. Um einen Nutzen aus **Dienst- und Port-Scans** zu ziehen, muss ein **Soll-Zustand** definiert sein: Welche Systeme dürfen in der DMZ sein, welche Ports bzw. Dienste dürfen darauf erreichbar sein? In computerlesbarem Format abgelegt (z. B. in einer MySQL-Datenbank) können Skripte Ergebnisse von Port-Scans mit dem Soll-Zustand abgleichen. Bei einer Verletzung des Soll-Zustands (z. B. unbekannter Port ist offen) sollte eine Meldung (z. B. per E-Mail) an einen Verantwortlichen des IT-Teams erfolgen.

Security Incident and Event Management System (SIEM)

Der Übergang von einem zentralem Logging zu einem SIEM-System ist nicht immer klar getrennt. SIEM-Systeme sind hauptsächlich auf Security-Informationen spezialisiert und bedienen sich in der Regel den Daten eines zentralen Log-Servers. Vor allem bei großen Krankenhäusern mit einer deutlich größeren Zahl an Systemen, Diensten und Nutzern ist ein SIEM-System sehr empfehlenswert, da es üblicherweise **fortgeschrittenere Daten-Auswertungen**, **-Visualisierungen** und **Berichtsfunktionen** bereitstellt. Die meisten SIEM-Systeme sind nicht-freie bzw. Open-Source-Lösungen. Eine Ausnahme bildet **OSSIM**.[2]

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 22 (Schutz vor Schadsoftware), 23 (Firewall, Intrusion Detection), 31 (Protokollierung und Auswertung)
- **B3S im Krankenhaus** – Kap. 7.13.5 (Intrusion Detection/Prevention)
- **ISO/IEC 27001** – Maßnahmenziele A.12.2 (Schutz vor Schadsoftware), A.12.4 (Protokollierung und Überwachung)
- **BSI IT-Grundschutz-Kompendium** – NET.1.2 (Netzmanagement)
- **BSI-Leitfaden** zur Einführung von Intrusion-Detection-Systemen[a]

[a] https://www.bsi.bund.de/DE/Publikationen/Studien/IDS02/gr_index_htm.html

[2] https://www.alienvault.com/products/ossim

5.5 Schließen von Einfallswegen für und Eindämmung von Malware im Krankenhausnetz

Kurzbeschreibung

*In einem Krankenhaus-Netz gibt es, wie auch in üblichen Netzen anderer Branchen, Dienste, welche oft als klassische (und die üblichsten) Einfallswege für Malware, wie Krypto-Trojaner, Computer-Würmer oder -Viren, dienen. Dazu zählen in erster Linie E-Mail oder auch Web-Browsing. Auch ist eine Verbreitung durch einmal infizierte Hosts im LAN in einer homogenen Umgebung (bzgl. Dienste, Betriebssysteme, usw.) relativ wahrscheinlich. Die Maßnahme **fokussiert sich auf diese primären Einfallswege**, sie kann aber auch auf einen anderen Dienst (z. B. Datei-Ablage, Cloud-Dienste, usw.) problemlos erweitert werden. Aufgrund ihrer zentralen Implementierung handelt es sich um eine Netz-Maßnahme.*

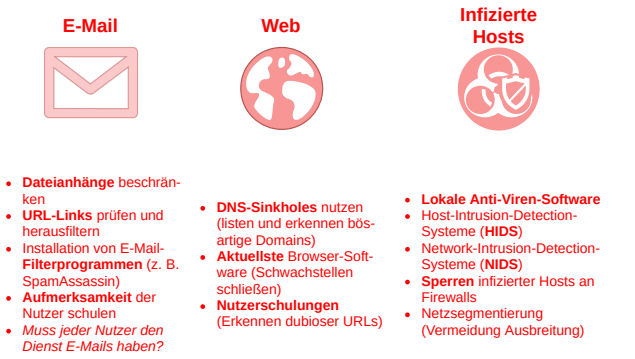


Abbildung 5.6: Abwehr und Eindämmung von Malware

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			•

Aufgrund der möglicherweise einschränkenden Wirkung der Maßnahme sollte sie durch die Geschäftsführung abgesegnet sein. Ebenfalls sollten grobe Anforderungen der Nutzergruppen (z. B. Verwaltung, medizinisches Personal), vor allem an die eingeschränkten Dienste, abgefragt und die Art der Nutzung (vgl. Abschnitt *Umsetzung der Maßnahme*) erörtert werden.

Umsetzung der Maßnahme

Malware verbreitet sich durch E-Mail und Web-Browsing über unbedarfte Handlungen von Nutzern, infizierte Dateien, veraltete Software (z. B. Web-Browser) und darin enthaltene Schwachstellen. Um die Sicherheit zu erhöhen und eine Infektions- und Ausbreitungsgefahr zu verringern, sollten Inhalte vorgefiltert und potenzielle Gefahren (gefährliche Dateien oder infizierte Hosts) **geblockt** werden.

Filter in E-Mails

Über E-Mail gibt es grob zwei Hauptwege, um sich mit Malware zu infizieren: Einerseits über direkt **angehängte Dateien** (insbesondere ausführbare Dateien, aber auch anwendungsspezifische Quelldateien, z. B. zur Tabellenkalkulation), andererseits über **in E-Mails enthaltene URLs**, welche beim Öffnen Schadsoftware nachladen. Zusätzlich stellt oft in E-Mail ausgeführtes **Javascript** ein Sicherheitsproblem dar, die meisten E-Mail-Clients verbieten das jedoch.
Wird der E-Mail-Dienst im eigenen Krankenhaus betrieben, kann der Inhalt praktisch beliebig kontrolliert werden. Eine extremere Variante ist hier, (fast) jegliche Anhänge an E-Mails zu verbieten und URLs und Inline-HTML und - Script in E-Mails zu entfernen. Das schränkt jedoch die Nutzbarkeit von E-Mails und somit unter Umständen den Betrieb stark ein, weshalb eine **Kompromissfindung mit den Nutzern** notwendig ist. Anfangs können aber zunächst (relativ) ungefährliche Dateien wie Textdateien, PDFs oder Bilddateien (PNG, JPG, …) erlaubt werden und im Einzelfall weitere hinzugefügt werden. Auch kann eine Gruppe vertrauenswürdiger E-Mail-Adressen definiert werden, welchen das Senden von Anhängen erlaubt ist. Zu beachten ist jedoch, dass eine Kompromittierung einer *vertrauenswürdigen E-Mail-Adresse* dann höchst problematisch ist.

Die technische Umsetzung der Maßnahme erfolgt je nach gewünschtem Funktionsumfang entweder über ein kommerzielles Produkt (oft mit mehr Funktionen) oder über freie Produkte wie **SpamAssassin**, welches sich auf Clients (insbesondere für kleinere Krankenhäuser) oder auch zentral auf dem eigenen Mailserver (in der Regel für Krankenhäuser mit eigener Infrastruktur) installieren lässt. Es gibt auch weitere Anti-Spam-Anwendungen für die Verwendung von *SpamAssassin*.[3]

Sperren bösartiger Websites im Web

Ein ähnliches Prinzip, wie es auch für E-Mail-Filter existiert, ist ebenfalls für generelles Web-Browsing möglich. Um zu verhindern, dass Nutzer, beispielsweise über nicht-gefilterte **bösartige URLs in Mails**, über **Links in vermeintlich vertrauenswürdigen Web-Sites** oder auch über automatisch in vielen Web-Sites integrierte **Werbeinhalte** („Malvertising“) ungewollt Malware auf ihren Client laden, können einerseits Browser-Erweiterungen auf jedem Client installiert werden. Andererseits gibt es auch **zentral installierte Filter**, wel-

[3] https://cwiki.apache.org/confluence/display/SPAMASSASSIN/StartUsing

che folglich das gesamte Krankenhaus-Netz abdecken und deutlich weniger Aufwand bedeuten.

Zentrale Ansätze basieren oft auf einem **Blacklisting-Verfahren** bekannter bösartiger bzw. verdächtiger DNS-Einträge (z. B. *example.com*), einem sogenannten DNS-Sinkhole. Aufgerufene Web-Sites und Werbung in Web-Sites werden am Laden gehindert, indem der Rechnername nicht aufgelöst wird. Auch bestehen derartige Black-Lists alternativ direkt aus bösartigen oder auffälligen IP-Adressen, wobei hier jedoch auch False-Positives auftreten können.

Ein kostenloses DNS-Sinkhole ist z. B. **unbound**,[4] ein DNS-Server mit Blacklisting-Listen. Diese können direkt aus dem Web heruntergeladen werden. Einen vergleichbaren Dienst stellt **Pi-Hole**[5] dar, wenn auch eher für kleine Netze. Beide sind einfach zu installieren.

Für sicheren, vertrauenswürdigen Austausch von Informationen über E-Mail bietet es sich darüber hinaus an, E-Mails beispielsweise mit **Pretty Good Privacy** (PGP) zu verschlüsseln und zu signieren.

Web-Browsing über eine VM als Sandbox

Ein DNS-Sinkhole kann faktisch jedoch nicht alle bösartigen Web-Sites kennen. Eine weitere Maßnahme ist, über eine **abgeschottete virtuelle Maschine** zu surfen. Diese ist praktisch komplett vom internen Netz über VLAN und entsprechende Firewall-Regeln abgeschottet und kann ausschließlich auf HTTP und HTTPS-Seiten im Internet zugreifen. Das heißt, das System hat Zugriff auf das Internet, jedoch keinerlei Zugriff auf andere Systeme im Krankenhausnetz. Beispielsweise in Linux kann über eine SSH-gesicherte Verbindung und **X-Forwarding** dann auf jedem anderen Client der Webbrowser der dedizierten Sandbox aufgerufen werden. Auf dem ausführenden Client wird ausschließlich die UI übertragen, Daten bleiben in der abgeschotteten VM.

Aktuelle Software und starke Passwörter

Malware verbreitet sich auch oft über Schwachstellen in verwalteter Software: So erfolgt laut Aussage des FBI beispielsweise die initiale Verbreitung von Ransomware zu 70 bis 80 Prozent über *Remote Desktop Zugriffe*.[6] Solche Lücken können durch aktuellste Software auf Clients und Servern sowie ausreichend starke Passwörter zumindest verringert werden.

Sperren infizierter Hosts

Es gibt trotz Schließung bekannter Einfallstore keine Garantie, dass Malware nicht doch in ein Krankenhaus-Netz gelangt. In dem Fall sollte eine schnelle/automatisierte **Eindämmung** von Malware im Netz vorgenommen werden. Als Basis dazu dient ein **Network** bzw. **Host Intrusion Detection System**, welches Malware detektiert (vgl. Maßnahmen 5.4 Zentralisierte Überwachung ■ und 6.2 Überwachung von Endgeräten ■). Deren Meldungen müssen (zentral) ausgewertet und entsprechende Maßnahmen ergriffen werden, insbesondere ein **Blockieren des Rechners am Internetausgang** (um die Möglichkeit des Nachladens weiterer Malware zu unterbinden), oder gar eine generelle Blockade des Netzzugriffs des betroffenen Systems.

In herkömmlichen Netzen ist ein Sperren über eine IP-Adresse üblicherweise nur am jeweiligen nächsten Router möglich, was unbedingt genutzt werden sollte, um beispielsweise **kompromittierten Besucher-Geräten** den Zugriff auf Krankenhaus-Dienste zu verbieten. Gleiches gilt für kompromittierte Geräte im Krankenhaus-LAN, denen nicht die Möglichkeit zur Kommunikation mit beispielsweise dem Management-Netz als auch der DMZ erlaubt werden soll (vgl. Maßnahme 5.1 Absicherung des Netzzugangs und generelle Netz-Zonen ■). Gesperrten Nutzern sollte zudem eine Benachrichtigung über ihre Sperrung angezeigt werden (z. B. durch Umleitung von Web-Anfragen auf eine Informationsseite). Außerdem sollte, sofern die Infrastruktur bereitsteht, automatisch ein Ticket oder zumindest eine Meldung über eine Sperrung an die verantwortliche Stelle in der IT-Abteilung gehen.

Solche Funktionalität wird bereits durch kommerzielle Komplettsysteme unterschiedlicher Hersteller unterstützt. Umsetzbar ist das Ganze aber auch im kleineren Rahmen, z. B. durch eine skriptbasierte Auswertung von NIDS-Meldungen und der automatischen Installation einer Firewall-Regel an den Netz-Grenzen und mindestens am zentralen Netzausgang. Die **Sperrung direkt am Client**, nur für gemanagte Clients und über sichere Fernwartungsprotokolle wie SSH, kann mit einer dort installierten Paketfilter-Software erfolgen (z. B. iptables, Windows-Firewall[7]).

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 23 (Firewall, Intrusion Detection), 25 (Sichere Authentisierung), 30 (Patch- und Änderungsmanagement)
- **B3S im Krankenhaus** – Kap. 5.2.2.1 (Informationtechnik (IT)), Kap. 6.5.1 IT 8 (Security (Firewall, DMZ, VPN, Malware-Schutz, Spamabwehr usw.))
- **ISO/IEC 27001** – Maßnahmenziele A.9.1.2 (Zugang zu Netzen und Netzwerkdiensten), A.12.2 (Schutz vor Schadsoftware)
- **BSI IT-Grundschutz-Kompendium** – OPS.1.1.4 (Schutz vor Schadprogrammen)

[4] https://nlnetlabs.nl/projects/unbound/about/

[5] https://pi-hole.net

[6] https://www.bleepingcomputer.com/news/security/fbi-says-140-million-paid-to-ransomware-offers-defense-tips/

[7] https://docs.microsoft.com/en-us/powershell/module/netsecurity/new-netfirewallrule?view=win10-ps

5.6 Sicheres WLAN für Personal und Patienten

Kurzbeschreibung

Wireless LAN (WLAN) hat inzwischen auch in Krankenhäusern große Bedeutung erlangt, die im Zuge der Digitalisierung noch weiter zunehmen wird. Einerseits ist WLAN und der darüber bereitgestellte Internetzugang ein wichtiger Dienst für Patienten, andererseits dient WLAN als Grundlage für viele Digitalisierungsvorhaben im Krankenhaus – von Messaging-Diensten bis zur Visite.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			
IT-Abteilung	•		
Personal/Nutzer			

Die Hauptverantwortung bei der Absicherung des Krankenhaus-WLAN liegt bei der IT-Abteilung. Diese muss geeignete, d. h. nutzerfreundliche als auch sichere Maßnahmen umsetzen.

Umsetzung der Maßnahme

Das grundlegendste Design-Kriterium dieser Maßnahme ist die **Trennung von WLANs** auf Basis ihrer Verwendung. Das Patienten-WLAN sollte unbedingt von internen WLANs getrennt werden. Die erste Trennung sollte auf Basis der SSID geschehen, bereits darauf aufbauend müssen je nach Netztyp weitere Maßnahmen ergriffen werden. Zunächst werden jedoch die in der Praxis relevanten Schwachstellen und Gefahren für WLAN zusammengefasst.

Offenkundige Schwachstellen und Gefahren

Einige **Schwachstellen** im WLAN sind inzwischen bereits seit längerem bekannt: Komplett **offene Hot-Spots** müssen unbedingt vermieden werden, da sonst praktisch jeder den Netzverkehr von jedem anderen Nutzer mitlesen und potenziell kritische Informationen abhören kann. Gleiches gilt de facto für **WEP-Verschlüsselung**, welche in wenigen Minuten mit frei verfügbaren Tools aus dem Internet geknackt werden können.

Jedoch ist nicht nur WEP, sondern ebenfalls WPA und WPA2 unter bestimmten Umständen anfällig für Manipulation und eine Kompromittierung. Im Web sind inzwischen nicht nur Anleitungen, sondern auch Tools frei verfügbar, die praktisch für Jedermann das Knacken von WPA- und WPA2-abgesicherten WLANs unter bestimmten Umständen trivial umsetzbar machen. Dabei werden üblicherweise zu schwache „WLAN-Passwörter“ (d. h. ***Pre-Shared-Key***-Authentifizierung) ausgenutzt, welche auf Basis von abgehörten verschlüsselten Netzpaketen auf jedem Client lokal hergeleitet werden können.

Eine andere Problematik, die mit einem reinen **Pre-Shared Key**-Authentifizierungsverfahren auftritt, sind sogenannte **Rogue-Access-Points**. In diesem Fall installieren Angreifer einen „bösartigen Access-Point“, welcher dieselbe SSID ausstrahlt, wie der angegriffene AP. Den meisten Nutzern fällt dieser AP nicht als böswillig auf und sie verbinden sich damit, was dazu führen kann, dass ein Angreifer den Netzverkehr komplett abgreifen kann.

Selbst für das im Allgemeinen als sicher geltende WPA2 ist zudem vor wenigen Jahren eine schwere **Schwachstelle in der Implementierung** einiger Geräte bekannt geworden, welche in Verbindung mit einem Rogue-Access-Point ausnutzbar ist (vgl. KRACK-Angriff[8]). Zur Absicherung dagegen ist unbedingt auf **aktuelle Soft- und Firmware** von Clients und Access-Points zu achten.

Auch ist WLAN nicht besonders gut gegen **Störangriffe** gewappnet, sei es direkt über Störungen des Funks (d. h. klassische Störsender) oder protokollbedingt. WPA und WPA2 unterstützen sogenannte Deauthentication Frames, welche (auch ohne im WLAN angemeldet zu sein) von beliebigen Clients gesendet werden können, um alle Geräte vom jeweiligen Access-Point kurzfristig beliebig oft abzumelden. Entsprechend darf WLAN **nicht als Verbindungsmedium** für wirklich **kritische Dienste** genutzt werden.

Unabhängig von Angriffen muss auch darauf geachtet werden, dass der **notwendige Daten-Durchsatz** für Dienste im Krankenhaus verfügbar ist. Vor allem, wenn das Netz mit Patienten und Gästen geteilt wird, muss hier achtgegeben werden.

Oft wird auch Whitelisting von MAC-Adressen als Sicherheitsmaßnahme eingesetzt, beispielsweise durch eine klassische nachgelagerte Anmeldung (Nutzer und Passwort oder Token-basiert) und Freischaltung über eine Intranet-Website. Dieses bietet in der Realität jedoch keinen echten Schutz, da MAC-Adressen von authentifizierten Geräten auf einfachste Weise abgehört und auf Clients gefälscht werden können.

Sicheres internes WLAN

Ein internes WLAN unterscheidet sich vom Patienten-WLAN dadurch, dass darüber der Zugriff auf ausgewählte **interne Dienste** möglich ist. Eine entsprechende Absicherung ist daher obligatorisch, vor allem hinsichtlich Verschlüsselung, Integritätsschutz und Authentifizierung.

[8] https://www.krackattacks.com/

Zur Absicherung der Funkverbindung sollte in jedem Fall wenigstens WPA2 eingesetzt werden. Dieses wird in der Praxis durch alle moderneren Access-Points und Clients ohne Probleme unterstützt. Hier spielt jedoch auch der eingesetzte Authentifizierungsmechanismus eine wichtige Rolle, da – wie im vorherigen Abschnitt beschrieben – eine Pre-Shared-Key (PSK)-Methode anfällig für einige Schwachstellen ist. Entsprechend sollte hier (wenn möglich) eine **zertifikatsbasierte** Authentifizierung über **802.1X** umgesetzt werden. Diese verhindert bereits einige Problematiken vom PSK-Verfahren.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 21 (Härtung und sichere Basiskonfiguration der Systeme und Anwendungen)
- **B3S im Krankenhaus** – 7.13.1 (Netz- und Systemmanagement), 7.13.7 (Sichere Authentisierung), 7.13.8 (Kryptographische Absicherung)
- **ISO/IEC 27001** – A.10.1 (Kryptographische Maßnahmen), A.13.1.3 (Trennung von Netzwerken)
- **BSI IT-Grundschutz-Kompendium** – NET.2.1 (WLAN-Betrieb), NET.1.1 (Netzarchitektur und -design)

Kompromiss im Patienten-WLAN

Wie bereits auch in Maßnahme 5.2 Logische Aufteilung des Krankenhausnetzes beschrieben, muss das Patienten-WLAN von internen Diensten und anderen Geräten aller Art **getrennt sein**. Optional können öffentliche Krankenhaus-Dienste bzw. Dienste in der DMZ darüber erreichbar sein. Auch muss eine Client-zu-Client-Kommunikation unterbunden werden (was einige WLAN-Router/APs unterstützen). Durch die allgemeine Trennung wird auch verhindert, dass sich Malware von unsicheren Patienten-Geräten auf das Krankenhaus-Netz überträgt.

Beim Patienten-WLAN ist hingegen ein 802.1X-Verfahren voraussichtlich kaum erfolgreich, da bei Patienten die Akzeptanz einer komplizierteren zertifikatsbasierten Authentifizierung verständlicherweise gering ausfallen würde. Da aus dem Patienten-WLAN in der Regel nur Zugang zum Internet und ausgewählten öffentlichen Diensten möglich ist, ist eine **WPA2 PSK**-Lösung in diesem Fall ein entsprechend vertretbarer Kompromiss. Neue Geräte unterstützen zudem auch bereits den Nachfolger-Standard WPA3, welcher bei gegebener Kompatibilität vorzuziehen ist. Jedoch muss hierbei im mindesten auf ein **starkes** „WLAN-Passwort“ geachtet werden. Das BSI empfiehlt hier ein Passwort mit einer Mindestlänge von 20 Zeichen, das sich aus Ziffern, Buchstaben und Sonderzeichen zusammensetzt. Das hervorgehobene Ziel ist zunächst, die Vertraulichkeit und Integrität des Netzverkehrs für Patienten sicherzustellen, die über ein offenes oder WEP-abgesichertes WLAN nicht gegeben sind. Weitere Maßnahmen, wie Token und MAC-Filter-basierter Zugang, können zudem darauf aufgesetzt werden, auch wenn dieser, wie beschrieben, kaum zur Sicherheit beiträgt.

Wenn WLAN für interne Dienste, Patienten und Gäste genutzt wird, sollte darauf geachtet werden, dass für **interne Anwendungen** und Dienste **genug Daten-Durchsatz** erzielbar ist und nicht z. B. Video-Streaming von Patienten und Gästen eingeschränkt wird. Dafür stellen viele Router Quality of Service (QoS) Steuerungsfunktionen bereit, worüber der Durchsatz für Netze oder einzelne Dienste (z. B. Videostreaming direkt) eingeschränkt werden kann.

Kapitel 6

Sicherheit von medizinischen Großgeräten und Endgeräten

Als Gegenstück zu Netzsicherheitsmaßnahmen (vgl. vorheriges Kapitel) können solche für Endgeräte angesehen werden. Diese können selten zentral implementiert werden, sondern sind direkt am Gerät vorzunehmen. Die Absicherung eines ganzen Netzes mit derartigen Maßnahmen muss entsprechend (meistens mehrfach) an vielen Clients vorgenommen werden, wodurch sie deutlich zeitaufwendiger sind. Dennoch sind sie oft notwendig, da sie gemeinsam mit und komplementär zu Netzsicherheitsmaßnahmen mehr Sicherheit bieten. In diesem Abschnitt werden auch die im Krankenhausnetz typischen medizinischen Geräte angesprochen.

- Zunächst wird gezeigt, wie die Komplexität in großen Netzen heruntergebrochen werden kann, um somit mehr Sicherheit zu gewinnen.
- Danach wird die Überwachung und Kontrolle der Endgeräte behandelt, um Probleme zu erkennen, zu beheben und zu vermeiden.
- Eine durch ihre Relevanz herausstechende Maßnahme ist hier die Datensicherung (Backup), die deshalb extra angesprochen wird.
- Schließlich werden noch einige wichtige Herausforderungen bezüglich Geräten des medizinischen Betriebs behandelt.

Die beschriebenen Maßnahmen richten sich vor allem an die IT-Abteilung und sind grundlegend technischer Natur.

6.1 Handhabbarkeit von Arbeitsplatzrechnern und Rechnern des medizinischen Betriebs

Kurzbeschreibung

Endgeräte bzw. Clients machen in Krankenhäusern und in anderen Organisationen oft einen sehr großen Teil der gesamten Infrastruktur aus. Darüber hinaus sind sie deutlich schwieriger zu managen als beispielsweise zentrale Dienste oder als die vor Nutzern „versteckte" IT-Infrastruktur. In dieser Maßnahme werden verschiedene Ansätze beschrieben, um Endgeräte einfacher und folglich zuverlässiger zu managen. Zudem kann die IT-Abteilung dadurch eingesparte Zeit besser einsetzen – beispielsweise zur Bearbeitung von akuten Sicherheitsvorfällen.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			

Das generelle Endgeräte-Konzept sollte mit der Geschäftsführung abgestimmt werden. Dazu zählen auch Ausnahmen, welche im Haus zugelassen und von den Nutzern benötigt werden (zum Beispiel bzgl. Patchmanagement, Softwareversionen, usw.).

Umsetzung der Maßnahme

Die beschriebenen Maßnahmen richten sich an handelsübliche Client-PCs, wie sie in der Verwaltung oder bei der Visite und in Behandlungsräumen von Krankenhäusern vorkommen. Nicht managebare medizinische Geräte (z. B. Ultraschallgeräte) werden in Maßnahme 6.8 Absicherung nicht managebarer Geräte angesprochen.

Desktop-Virtualisierung und Thin-Clients

Virtualisierung ist aus heutigen IT-Infrastrukturen nicht wegzudenken – im Serverbereich hat sie sich bereits seit längerem durchgesetzt. Jedoch sind auch Virtualisierung und Zentralisierung im Client-Bereich möglich und bieten viele Vorteile. Es können zahlreiche Lösungen unter dem Suchbegriff „Virtual Desktop Infrastructure" oder „Desktop-Virtualisierung" und „Thin Clients" gefunden werden. Das Prinzip dahinter ist, dass Desktop-Umgebungen und Anwenderapplikationen zentral eingerichtet und verwaltet werden. Über Clients (oft auch *Thin Clients*) können die Anwendungen über eine Netzverbindung zum zentralen Rechenzentrum genutzt werden. So können zum Beispiel Patch-Management, Applikations- und Versionsverwaltung der Clients dann weitestgehend **zentral gemanagt** werden. Die Maßnahme ist zudem oftmals Voraussetzung für eine einfache und sichere Umsetzung von **Telearbeit**.

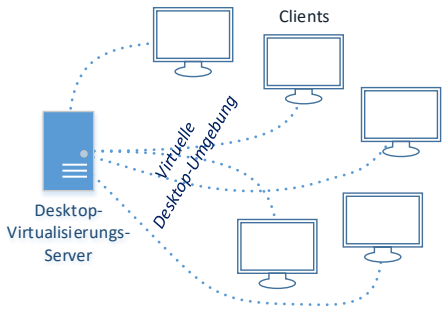


Abbildung 6.1: Desktop-Virtualisierung

Als *schnelle Variante* lässt sich etwas Ähnliches über SSH mit X-Forwarding (in praktisch jedem Linux-System vorhanden) und einer geeigneten Nutzerverwaltung am Host-System bauen. Im Web finden sich dazu einige Anleitungen.

Zu beachten ist, dass die **Qualität der Dienstnutzung** stark von der Netzinfrastruktur abhängt. Diese muss leistungsfähig genug sein, um den Dienst zu tragen.

Eine weitere Problematik ist, dass die **Client-Firmware** (d. h. BIOS, UEFI) und darunterliegende Client-**Betriebssysteme** nicht abgedeckt sind. Um zumindest letzteres abzudecken, eignet sich eine automatisierte Installation von Betriebssystem-Updates (unter Umständen in Verbindung mit einem netzweiten Patch- und Update-Service, wie *WSUS* für Windows).

Homogenität der Geräte und Betriebssysteme

Eine weitere Möglichkeit, um die Handhabbarbeit von Endgeräten zu erleichtern, ist generell das Achten auf Homogenität bei Geräten und Client-Betriebssystemen. So kann nicht nur die Installation und Wartung von Software im Haus weitgehend standardisiert werden. Das heißt, sobald einmal eine Lösung zur Einrichtung einer Software auf einem Client gefunden wurde, kann diese Lösung auch auf allen (oder zumindest den meisten) gleichartigen Systemen umgesetzt werden.

Darüber hinaus ist es ebenfalls einfacher, passende Hardware-**Ersatzteile**, wie beispielsweise Netzteile, Batterien und Akkumulatoren, Kabel, PCI-Module, usw., vorrätig zu halten.

Deployment-Werkzeuge

Für die Einrichtung und Administration nicht nur von Clients existieren einige Automatisierungs-Werkzeuge wie **Puppet**, **Ansible** oder, mit besonderem Fokus auf Windows, auch **OPSI**.[1] Diese unterstützen in der Regel eine beliebige Gruppierung von Geräten (z. B. *Clients-Visite*, *Clients-Administration*, *Clients-Behandlungszimmer*, usw.). Darauf aufbauend können sie, ausgehend von einem zentralen Server, über das Netz Clients je nach Gruppenzugehörigkeit einheitlich konfigurieren oder Programme installieren und Sequenzen von Befehlen ausführen (und vieles mehr). Teilweise wird, wie beispielsweise bei Ansible, außer einem laufenden SSH-Server auf dem Client kein weiterer vorinstallierter Agent benötigt.

So können von Malware befallene Systeme ohne den üblicherweise damit verbundenen manuellen Aufwand automatisiert neu aufgesetzt und frisch installiert werden.

Software-Stack-Vorlagen

Eine Alternative zu Deployment-Werkzeugen kann in bestimmten Bereichen auch die Vorbereitung von bereits fertigen Abbildern virtueller Maschinen sein. Die auch als *Cloud Images* bezeichneten Dateien enthalten zweckgebunden die bereits vorinstallierte und direkt an beliebigen Endgeräten einsatzbereite notwendige Software und Anwendungen, im Krankenhaus zum Beispiel für Clients am Empfang, auf einer Station oder für die Visite.

Die Abbilder werden dann direkt auf den Clients mit einem vorinstalliertem Hypervisor (z. B. Virtualbox, KVM) ausgeführt. Auch hier wird, wie bei Thin Clients, auf Virtualisierung gesetzt, jedoch mit dem Unterschied, dass die Virtualisierung in diesem Fall lokal und soweit unabhängig von einer Netzanbindung stattfindet.

System-Updates können dann einfach durch die zentrale Konfiguration und den Austausch der jeweilig eingesetzten Cloud-Images auf den Endgeräten durchgeführt werden. Eine entsprechend hervorzuhebende Empfehlung beim Einsatz dieser Teil-Maßnahme ist auch der Einsatz der im nächsten Abschnitt beschriebenen Teil-Maßnahme.

Trennung von Betriebssystem und Nutzerdaten

Die Trennung von Betriebssystem und Nutzerdaten sollte generell beachtet werden. Jedoch können auch hier unterschiedliche Lösungen mit verschiedenen Vorteilen angewendet werden. Zum einen die lokale Trennung durch geeignete **Partitionierung** der Platten, zum anderen, ebenfalls lokal, die Trennung durch **unterschiedliche Datenträger bzw. Festplatten**. So kann die Neu-Installation von Betriebssystemen besser getrennt werden.

Eine noch geeignetere, jedoch netzabhängige Variante ist die Verwaltung von Nutzerdaten über ein **Netzlaufwerk**. Lokale Platten der Endgeräte enthalten dann nur noch das Betriebssystem (was auch im Fall von Diebstahl eines Endgeräts Vorteile bringt). Bei erfolgreichem Login am Rechner wird dann das Netzlaufwerk des jeweiligen Nutzers automatisch eingebunden.

In Verbindung mit der vorherigen Teil-Maßnahme kann das Cloud Image als Betriebssystem angesehen werden, in das Daten aus dem jeweiligen Nutzerlaufwerk eingebunden werden.

Hier sei darauf hingewiesen, dass Nutzerdaten in den beschriebenen Fällen auch gut zu sichern sind und im Gegensatz zu austauschbaren Systeminformationen unbedingt gesichert werden sollten (vgl. Maßnahme 6.4 Automatisierte Datensicherung zur effektiven Wiederherstellung).

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 19 (Netz- und Systemmanagement), 21 (Härtung und sichere Basiskonfiguration der Systeme und Anwendungen), 22 (Schutz vor Schadsoftware), 30 (Patch- und Änderungsmanagement)
- **ISO/IEC 27001** – A.14 (Anschaffung, Entwicklung und Instandhalten von Systemen)
- **BSI IT-Grundschutz-Kompendium** – SYS.1.5 (Virtualisierung)

[1] https://www.opsi.org/

6.2 Überwachung von Endgeräten ■

Kurzbeschreibung

Ein Network Intrusion Detection System ist wichtig zur Überwachung des Netzes. Entsprechende Gegenstücke gibt es auch auf Host-Ebene mit ergänzenden Detektions- und Schutzmaßnahmen. Diese Maßnahme fokussiert auf Clients. Entsprechendes für Server wird in Maßnahme 7.3 Überwachung von Serversystemen ■ vorgenommen.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			
IT-Abteilung	•		
Personal/Nutzer			

Die Überwachung von Endgeräten muss durch die IT-Abteilung vorgenommen werden.

Umsetzung der Maßnahme

Der Vorteil von host-basierten Systemen besteht neben mehr Möglichkeiten der Detektion auch darin, dass vor allem geeignetere **Gegenmaßnahmen** möglich sind. Der Nachteil ist die dezentrale Installation auf allen dadurch geschützten Systemen und dem entsprechend dazu proportionalen **Mehraufwand**. Folgenden Aspekten sollte bei der Überwachung von Clients eine besondere Rolle zukommen.

Erkennung von Malware

Eine Standard-Maßnahme zum Schutz von Clients ist der Einsatz von **Anti-Viren-Software** (AV-Software), welche bekannte Schadsoftware erkennen und ihre Ausführung verhindern kann. Auf dem Markt existieren viele kostenlose sowie kostenpflichtige AV-Programme, welche einen vergleichbaren Funktionsumfang bieten. Im Web lassen sich Vergleiche gängigster AV-Programme finden.

Erkennung eines Einbruchs

Neben AV-Software hat sich zur Überwachung von Endgeräten noch eine weitere Klasse von Programmen etabliert, sogenannte *Host Instrusion Prevention Systems* (HIDS). Diese Systeme detektieren üblicherweise nicht nur Schadsoftware (ein AV-Programm kann als Teil eines HIDS angesehen werden), sondern sie überwachen zusätzlich andere Aspekte, wie **Datenintegrität** und Auffälligkeiten in **Log-Dateien**, und melden Probleme an einen Administrator.

Relativ umfangreiche Funktionalität wird dabei zum Beispiel durch die **zentralisierte** Open-Source-Lösung *OSSEC*[2] (für Windows und Unix-Systeme) bereitgestellt. Es muss entsprechend ein OSSEC-Server (mit Web-UI) installiert werden, welcher alle Daten von OSSEC-Agenten sammelt. Die Agenten werden dabei auf jedem zu überwachenden Gerät installiert. Es ergänzt etwaige AV-Software beispielsweise um eine Datei-**Integritätsprüfung** (d. h. es meldet die Manipulation überwachter Dateien), überwacht **Log-Dateien** und meldet auffällige Einträge. Auch ist es in der Lage, bestimmte **Rootkits** zu detektieren, und es kann auch **aktive Gegenmaßnahmen** selbst durchführen.

Zur Unterstützung der Durchsicht von Log-Dateien nach verdächtigen Einträgen existieren darüber hinaus entsprechende Programme. Generell ist es ratsam, einen zentralisierten Logserver (vgl. Maßnahme 5.4 Zentralisierte Überwachung ■) für Log-Dateien zu installieren.

Überwachung von medizinischen Geräten

Die Überwachung von medizinischen Geräten ist von *interner* Seite üblicherweise nicht gegeben. Die Möglichkeit einer Installation entsprechender Software auf den Geräten besteht nicht. Aber es ist möglich, insbesondere die **Netzschnittstelle** derartiger Systeme genauer zu überwachen (vgl. dazu auch die Perspektive der **aktiven Absicherung** in Maßnahme 6.8 Absicherung nicht managebarer Geräte ■■).

So kann zum Beispiel ein separates NIDS, wie Suricata, genutzt werden, um ein Teilnetz mit medizinischen Geräten zu überwachen. Switches, an denen medizinische Geräte angeschlossen sind, unterstützen in der Regel Port-Mirroring, über die beispielsweise eine kleine Appliance den gespiegelten Netzverkehr überwacht.

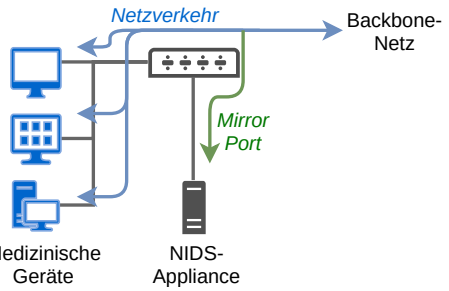


Abbildung 6.2: Überwachung mit externer Appliance

[2] https://www.ossec.net/

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 22 (Schutz vor Schadsoftware), 31 (Protokollierung und Auswertung)
- **B3S im Krankenhaus** – Kap. 7.9 (Vorfallerkennung und Überwachung)
- **ISO/IEC 27001** – A.12.2 (Schutz vor Schadsoftware), A.12.4 (Protokollierung und Überwachung)
- **BSI IT-Grundschutz-Kompendium** – OPS.1.1.4 (Schutz vor Schadprogrammen), SYS.2.1 (Allgemeiner Client)

6.3 Kontrolle und Einschränkung von Software-Anwendungen ■

Kurzbeschreibung

Im Krankenhaus sind Rechner des medizinischen Betriebs und in der Verwaltung in der Regel handelsübliche PC. Sie unterscheiden sich lediglich durch die darauf zur Zweckerfüllung genutzte Software. Eine Einschränkung der auf den Rechnern von Nutzern ausführbaren Programme auf unbedingt notwendige kann Manipulation, Schwachstellen und die Einführung von Malware in einigen Fällen verhindern, in denen andere Maßnahmen, wie ein Virenschutz oder Mail-Filter, nicht angeschlagen haben.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			
IT-Abteilung	•		
Personal/Nutzer			•

Für die Umsetzung ist die IT-Abteilung zuständig. Durch eine Befragung der Nutzer im Betrieb nach unbedingt notwendigen Anwendungen kann die Maßnahme jedoch enorm geschärft werden.

Umsetzung der Maßnahme

Die Einschränkung von Software-Anwendungen auf Client-PCs kann aus zwei Richtungen angegangen werden. Einerseits mit einem **Whitelisting**-Verfahren, in dem nur *erlaubte* Anwendungen definiert sind, und andererseits mit einem **Blacklisting**-Verfahren, worin *explizit verbotene* Anwendungen und Berechtigungen beschrieben werden.

Beide Arten sind im Krankenhaus nicht so einfach umzusetzen; eine Fehlkonfiguration kann den Betrieb dabei bereits signifikant einschränken, da die PCs nicht mehr zweckmäßig genutzt werden können. Bei unzureichend strikten Richtlinien hingegen bleiben Schwachstellen offen. Da diese Maßnahme weniger zur Basisabsicherung als vielmehr zu den fortgeschrittenen (und zeitaufwendigen) Maßnahmen gehört, ist ein liberaler, jedoch schrittweise verbessernder Ansatz in der Praxis vorzuziehen.

Hilfreiche Vorarbeiten

Um alle notwendigen Systeme abzudecken, ist es oft hilfreich, eine Gruppierung von Client-PCs nach Zweck vorzunehmen. Beispielsweise werden in der **Visite**, in **Behandlungsräumen**, in der **Radiologie**, in den **jeweiligen Verwaltungsabteilungen** usw. jeweils ähnliche Anwendungen benötigt. Jede dieser Gruppen braucht dann einen entsprechenden eigenen Satz an Richtlinien. Dieser Satz an Richtlinien kann – einmal erstellt – für Systeme mit dem gleichen Zweck wiederverwendet werden.

Die im Folgenden beschriebenen Vorgehensweisen funktionieren in der Praxis nur, wenn Nutzer **keine lokalen Administrator**-Konten haben. Ansonsten sind diese Maßnahmen umgehbar.

Sinnvolles Whitelisting

Insbesondere beim Whitelisting-Ansatz sollte zuerst bei den Nutzern **abgefragt** werden, welche Anwendungen benötigt werden. Auch darf nicht vergessen werden, notwendige Systemprogramme (z. B. explorer.exe) freizuschalten, damit Nutzer nicht *ausgesperrt* sind. Generell ist ein Whitelisting-Ansatz potenziell sicherer, da er neue Gefahren (z. B. Malware) allgemein automatisch abdeckt.

Sinnvolles Blacklisting

Für das Blacklisting-Verfahren gibt es einige wenige Policies, um bereits deutlich mehr Sicherheit leisten zu können. Ein simpler Ansatz ist, den Nutzern das Ausführen aller Anwendungen in **allen Verzeichnissen** zu verbieten, in denen sie **Schreibrechte** besitzen. Das ist üblicherweise das persönliche **Nutzerverzeichnis** (Home-Verzeichnis), es können aber auch **Temporäre Verzeichnisse** sein. Auch sollten Anwendungen auf Wechseldatenträgern (z. B. USB-Sticks) generell zur Ausführung verboten werden (vgl. Maßnahme 6.5 Schnittstellen und sichere mobile Datenträger im Krankenhaus ■). Darauf aufbauend können schrittweise nicht benötigte Anwendungen identifiziert und blockiert werden.

Auf diese Weise kann die Ausführung von Programmen, die versehentlich via Web, Mail oder USB-Stick heruntergeladen werden, verhindert werden. Lediglich bereits auf Systemen installierte Programme bleiben ausführbar.

Geeignete Software

Unter allen gängigen Betriebssystemen gibt es Dienste zum Black- oder -Whitelisting von Anwendungen. Bei Windows ist in der Regel die Anwendung **AppLocker**[3] (*secpol.msc*) dafür nutzbar. Eine noch mächtigere Variante für Linux ist **AppArmor**, unter der deutlich feingranularere Berechtigungen beschrieben werden können.

Grenzen und Hinweise

Ebenfalls gefährliche interpretierte Dateien mit enthaltenen Makro-Programmen (z. B. für Tabellen- oder Dokumenteditoren) oder auch *Archivbomben* können übli-

[3] https://docs.microsoft.com/de-de/windows/configuration/lock-down-windows-10-applocker

cherweise nicht durch diese Maßnahmen reguliert werden.

Generell bietet sich für unterschiedliche Gruppen jedoch auch ein Mischansatz an. Beispielsweise in Gruppen, wo benötigte **Anwendungen** relativ klar und **fix** sind, ist ein **Whitelisting**-Ansatz umsetzbar. In Gruppen von PCs mit relativ **hoher Dynamik** bietet hingegen ein **Blacklisting**-Ansatz einen guten Kompromiss zwischen Aufwand und Nutzen.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 14 (Ordnungsgemäße Systemadministration), 21 (Härtung und sichere Basiskonfiguration der Systeme und Anwendungen)
- **B3S im Krankenhaus** – Kap. 7.13.4 (Schutz vor Schadsoftware)
- **ISO/IEC 27001** – A.12.2 (Schutz vor Schadsoftware)
- **BSI IT-Grundschutz-Kompendium** – OPS.1.1.4 (Schutz vor Schadprogrammen), SYS.2.1 (Allgemeiner Client)

6.4 Automatisierte Datensicherung zur effektiven Wiederherstellung ■

Kurzbeschreibung

Datensicherung (Backup) ist eine der obligatorischsten Maßnahmen, um den Betrieb, auch im Krankenhaus, aufrechtzuerhalten bzw. wiederherzustellen. Im Falle einer Kompromittierung, einer Misskonfiguration oder eines Software- bzw. Hardware-Defekts können lange Ausfallzeiten vermieden werden, indem ein zuvor lauffähiger Stand wieder eingespielt wird. Inbesondere gegen sogenannte Kryptotrojaner gelten Backups als einfachste Variante zur Bereinigung der IT-Infrastruktur.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			
IT-Abteilung	•		
Personal/Nutzer			

Von einer Datensicherung bekommt ein Nutzer im Idealfall nichts mit. Für die Umsetzung ist die IT-Abteilung verantwortlich. Diese sollte auch am besten wissen, wo Nutzer ihre Daten halten (zentral vs. dezentral) und welche Daten gesichert werden müssen.

Umsetzung der Maßnahme

Der Komplex „Backup“ umfasst mehrere Aspekte, bei denen Besonderheiten zu berücksichtigen sind. Das sind mindestens eine geeignete **Backup-Infrastruktur** im Hintergrund, Betriebskonzepte, die zur **Vereinfachung** bzw. Erschwerung der Umsetzung beitragen, **Backup-Konzepte** hinsichtlich dem Umfang berücksichtigter Daten, Häufigkeit und Art der Backup-Implementierung sowie **Datenschutzaspekte**. Alle Aspekte werden in einer Backup-Richtlinie zusammengefasst, welche auf Basis der Vorlage aus Anhang A.4 erstellt werden kann.

Backup-Infrastruktur

Eine geeignete Backup-Infrastruktur sollte verschiedene Anforderungen erfüllen, um Datenverlust trotz Datensicherung zu vermeiden.

Zum einen sollten Sicherungen an einem **geografisch entfernten Standort** (z. B. einem anderen Gebäude oder mindestens einem anderen gesicherten Raum) gehalten werden. So wird verhindert, dass bei größeren Katastrophen, wie Diebstahl, einem Wassereinbruch oder einem Gebäudebrand, Produktivdaten und Sicherungen gleichermaßen verloren gehen können. Falls kein anderer Standort möglich ist, wäre unter Umständen auch die Nutzung eines vertrauenswürdigen Cloud-Dienstes denkbar. Dafür muss jedoch im Einzelfall die rechtliche Situation geprüft werden (vgl. Abschnitt *Datenschutzkonformität* unten).

Auch sollte eine geeignete Netzinfrastruktur einen **ausreichenden Datendurchsatz** bereitstellen können. Dieser befindet sich üblicherweise mindestens im Gigabit-Bereich (d. h. in der Regel Gigabit-Ethernet), um die oft im Krankenhaus eingesetzte Vielzahl an Systemen handhaben und gleichzeitig das Netz für den Produktivbetrieb nutzen zu können.

Zur Speicherung der Sicherungen sollten entsprechende Server mit geeigneten Funktionen ausgerüstet sein. Einerseits sollte ein Server einfach durch **Speichermodule**, wie Festplatten, **erweiterbar** sein. Außerdem muss der Datenverlust durch Festplattenausfall verhindert werden. Am einfachsten geht das über ein **RAID-System** (z. B. RAID5 oder RAID6). RAID5 verkraftet dabei den Ausfall einer Festplatte und RAID6 den von zweien; RAID6 ist jedoch etwas weniger effizient in der Speicherausnutzung. Dabei sollte darauf geachtet werden, dass immer ein Vorrat an Festplatten für Erweiterungen und Ersatz in ausreichender Menge verfügbar ist.

Vereinfachende Faktoren

Als stark vereinfachenden Faktor, auch bei der Umsetzung eines Daten-Sicherungsdienstes, ist unter anderem die in Maßnahme 6.1 Handhabbarkeit von Arbeitsplatzrechnern und Rechnern des medizinischen Betriebs ■ beschriebene *Trennung von Betriebssystem und Nutzerdaten* hilfreich (Letzteres idealerweise auf Netzlaufwerken). Insbesondere wird dadurch, zumindest bei häufigen **gleichzeitig** startenden Backup-Jobs, die Netzlast reduziert (auch wenn sie generell wegen der Umsetzung als Netzlaufwerk höher als üblich ausfällt); Dienste und Anwendungen im Betrieb werden folglich weniger beeinflusst.

Auch kann die generelle Nutzung von Netzlaufwerken **Inkompatibilitäten kompensieren** – beispielsweise bei mobilen Geräten (z. B. für die Visite). Hier spart man sich dann die Suche nach geeigneten Backup-Tools für diese speziellen mobilen Geräte.

Häufigkeit, Umfang und Art

Bei der Ausführung der Datensicherung spielen unterschiedliche Aspekt eine Rolle, dazu zählt auch, **wie oft**, **wie** und auf **welchen Daten** sie durchgeführt wird.

Bei der Menge und Bedeutung der Daten, die im Krankenhaus generiert werden, ist eine möglichst aktuelle Version der Daten notwendig. Daher ist es sinnvoll, bereits **stündlich** eine komplette **automatische** Datensicherung durchzuführen. Damit die Netzlast dabei nicht zu hoch und der Betrieb durch stündliche Backups nicht beeinträchtigt wird, sollte unbedingt auf eine *Vollsicherung* verzichtet und eine **inkrementelle Sicherung** (unter Umständen mit Erkennung veränderter

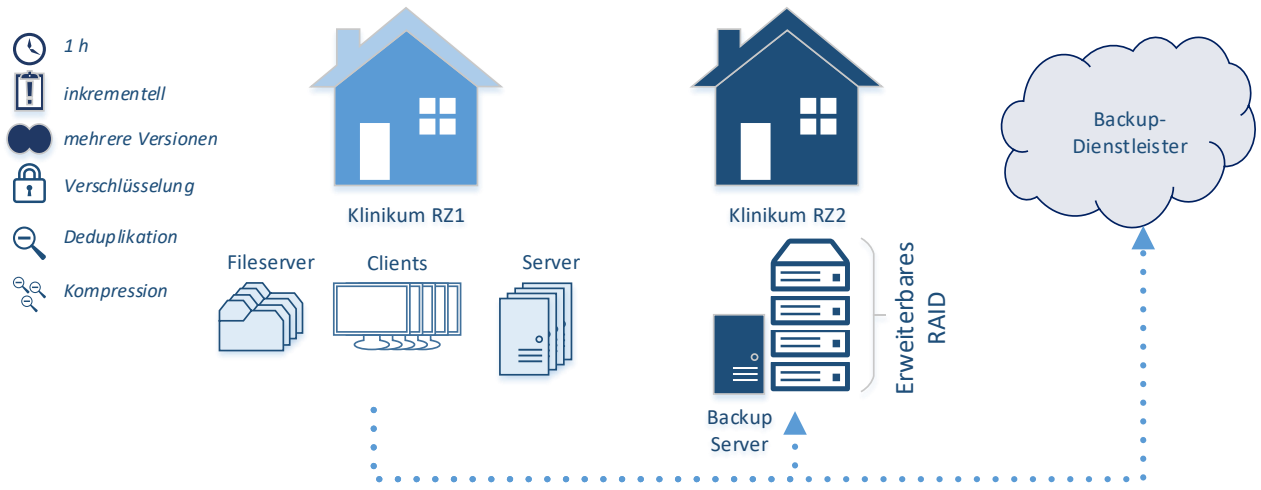


Abbildung 6.3: Datensicherungsinfrastruktur im Krankenhaus

Daten, abhängig vom Dateisystem) bevorzugt werden. Dabei ist es außerdem wichtig, **mehrere Zeitpunkte** im Backup zu halten. Beispielsweise könnte das letzte durchgeführte Backup unbemerkt von Malware befallen sein, sodass ein noch früheres, integeres Backup eingespielt werden muss.

Bei der Frage, was gesichert werden soll, kann unter Umständen eine Differenzierung helfen. Normalerweise sollten aus Gründen der Platzeffizienz nur **Nutzerdaten** gespeichert werden, da Betriebssystemdaten üblicherweise einfach zu rekonstruieren sind. Jedoch kann es bei sehr kritischen Systemen auch sinnvoll sein, ein **komplettes Systemabbild** zu sichern; beispielsweise, um bei einer Wiederherstellung eines Systems eine aufwendige, zeitintensive Konfigurierung zu vermeiden und Dienste möglichst schnell durch direktes Einspielen wieder nutzbar zu machen.

Auch sollte darauf geachtet werden, dass Sicherungsdateien **verschlüsselt**, **dedupliziert** und **komprimiert** werden, was durch das Backup-Tool unterstützt werden muss. Die Verschlüsselung dient der Vertraulichkeit der Daten. Eine Deduplikation verhindert die Speicherung redundanter Daten und die Komprimierung verkleinert die gespeicherten Inhalte, sodass eine sehr viel effizientere Speicherung stattfindet.

Ein Beispiel für ein geeignetes Tool zur Datensicherung ist **Borg**[4], welches als Backup-Tool praktisch alle der genannten Kriterien erfüllen und sogar abgesichert über eine SSH remote Inhalte sichern kann. Ein anderes modernes Tool ist **restic**,[5] das **append-only Backups** unterstützt und das Löschen bestehender Sicherungspunkte verhindert, sodass Mal- und Ransomware die Manipulation gesicherter Daten verboten wird.

Datenschutzkomformität

Bei einer Datensicherung ist darüber hinaus die Beachtung von Datenschutz- und gesetzlichen Bestimmungen wichtig. Einerseits ist eine funktionierende Datensicherung eine Grundvoraussetzung des Datenschutzes, um Datenverlust zu vermeiden. Vor allem aber Konzepte, wie das *Recht auf Vergessenwerden* im Datenschutz, sind eine Herausforderung für die Datensicherung. Üblicherweise müssen, sobald ein Patient es einfordert, alle persönlichen Daten über ihn unverzüglich gelöscht werden, auch aus den Sicherungsdateien. Da dies jedoch mit einem enormen, teilweise nicht vertretbaren Aufwand in Sicherungsdateien verbunden ist, verweisen viele zugängliche rechtliche Einschätzungen auch darauf, dass eine Löschung erst bei Wiederherstellung unter Umständen akzeptabel ist. Hier ist eine offizielle Abklärung mit dem Datenschutzbeauftragten sinnvoll.

In Bayern sind sich auch viele Krankenhäuser nicht sicher, ob eine unterstützende Cloud-Lösung zur Speicherung von Patienten-Daten rechtens ist. Allgemein wird dies zumindest im Bayerischen Krankenhausgesetz (BayKrG) Artikel 27 (Datenschutz)[6] nicht explizit ausgeschlossen, wodurch eine Prüfung in Einzelfällen möglich ist.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 29 (Datensicherung, Datenwiederherstellung und Archivierung)
- **B3S im Krankenhaus** – Kap 7.13.11 (Datensicherung, Datenwiederherstellung und Archivierung)
- **ISO/IEC 27001** – A.12.3 (Datensicherung)
- **BSI IT-Grundschutz-Kompendium** – CON.3 (Datensicherungskonzept)

[4] https://www.borgbackup.org/
[5] https://restic.net/
[6] https://www.gesetze-bayern.de/Content/Document/BayKrG-27

6.5 Schnittstellen und sichere mobile Datenträger im Krankenhaus

Kurzbeschreibung

Im Krankenhaus spielt der Austausch von Daten eine große Rolle. Nicht nur das Personal, sondern auch Patienten verwenden immer öfter USB-Sticks und externe Festplatten, um Dokumente und eigene Gesundheitsdaten klinikums- und abteilungsübergreifend auszutauschen. Gleichzeitig gelten mobile Datenträger als häufiger Einfallsweg von Malware in ein (Krankenhaus-) Netz. Ein Kompromiss zwischen einer sicheren und gleichzeitig benutzerfreundlichen Lösung ist daher notwendig.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			•
IT-Abteilung	•		
Personal/Nutzer			•

Die Geschäftsführung sollte bei der Maßnahmenumsetzung nicht vergessen und auch als Nutzer behandelt werden. Genauso sollte vorab bei Nutzern, Ärzten, Pflege und in der Verwaltung erfragt werden, welche Anwendungsfälle zum Einsatz von mobilen Datenträgern, wie USB-Sticks, notwendig sind (z. B. Patient bringt USB-Stick mit MRT-/Röntgen-Aufnahme).

Umsetzung der Maßnahme

Generell zielt diese Maßnahme auf die folgenden Kernergebnisse ab:

- Nur **berechtigte Personen** sollen mobile Datenträger verwenden dürfen.
- Mobile Datenträger sollen nur auf **abgesicherten Terminals** verwendet werden.
- **Malware** darf nicht über mobile Datenträger in das Krankenhaus-Netz gelangen.

Die folgenden Teil-Maßnahmen sollen genau darauf hinwirken.

Deaktivierung von Schnittstellen

Grundsätzlich sollten bei allen Client-PCs und insbesondere Rechnern, die nicht in extra gesicherten Räumen wie einem Rechenzentrum im Klinikum stehen, alle **USB**-Schnittstellen deaktiviert sein. Gleichzeitig ist die Umsetzung dieser Maßnahme nicht ganz einfach, schließlich sind bei den meisten PCs eine notwendige Computer-Maus und die Tastatur ebenfalls über USB angebunden und müssen weiterhin funktionieren. Auch bieten möglicherweise viele medizinischen Geräte die Option der Deaktivierung von Schnittstellen nicht an, weil nicht selten im Hintergrund ein veraltetes Betriebssystem läuft.

Um USB-Schnittstellen ausschließlich für mobile Datenträger zu blockieren, bieten zum Beispiel Windows und Linux softwareseitige Lösungen an, welche die Funktionsfähigkeit von Eingabegeräten nicht beeinträchtigen. Unter **Windows** funktioniert das über den *Editor für lokale Gruppenrichtlinien*. Darin gibt es in den *Administrativen Vorlagen* eine Richtlinie zur Verwendung von *Wechseldatenträgern*. Bei Aktivierung kann der Lese- und auch der Schreibzugriff unterbunden werden. Unter **Linux** wird eine Lösung auf Ebene von Kernel-Modulen angeboten.

Für Geräte, bei denen die eben genannten Lösungen nicht infrage kommen, kann dennoch die Nutzung der USB-Schnittstellen erschwert werden. Im Versandhandel werden unter anderem unter der Bezeichnung *USB Port Locks* unterschiedliche Verschlüsse für USB-Buchsen angeboten, welche sich ohne Werkzeug nur schwierig entfernen lassen.

Einrichtung sicherer Terminals

Ein generelles Verbot von USB-Sticks funktioniert üblicherweise nicht. Wie beschrieben, ist ihre Nutzung hin und wieder notwendig – spätestens, wenn Patienten digitale Dokumente mit medizinischen Daten darauf mitbringen. Eine mögliche Lösung ist die Installation dafür konfigurierter **Terminals** (d. h. dennoch klassische PCs), welche einen ersten Virenscan für Dateien auf mitgebrachten USB-Sticks durchführen. Diese dürfen nicht durch Malware langfristig kompromittierbar sein und müssen vor allem verhindern, dass Produktiv-Rechner, welche den Betrieb eines Krankenhauses unterstützen, infiziert werden. Dafür sind folgende Maßnahmen empfehlenswert:

- Terminals in ein **separates Subnetz** setzen. Auch sollte die Kommunikation der Terminals untereinander via Firewall unterbunden werden, damit sie sich nicht gegenseitig mit Malware infizieren (vgl. Maßnahme 5.2 Logische Aufteilung des Krankenhausnetzes).
- Die Verwendung eines **Live-Systems**. Live-Systeme laufen ausschließlich im RAM (Arbeitsspeicher) eines PCs – eine Festplatte auf den Terminals ist dabei nicht notwendig und kann vollkommen weggelassen werden. Bei einer Infizierung eines Live-Systems kann das komplette Terminal durch einen einfachen Neustart wieder auf einen sicheren Ausgangspunkt gesetzt werden, wenn das Boot-Medium nicht infiziert ist. Das Boot-Medium sollte daher immer nur im *Read-Only* Modus geladen werden.

Die weitere Vorgehensweise kann je nach Bedarf umgesetzt werden: Beispielsweise kann auch ein getrennter, schmutziger Speicherort eingebunden werden, d.h. ein dediziertes Netzlaufwerk, auf dem zweifelhafte, von Extern kommende Dateien gespeichert werden, deren Status noch nicht geklärt ist und die von einem Spezialisten überprüft werden müssen.

Vertrauenswürdige USB-Sticks

Eine Alternative zur Deaktivierung der Schnittstellen für USB-Wechseldatenträger ist die Nutzung eines **USB-Wächters**. Der USB-Wächter ist eine (auch als Freeware erhältliche) Software, welche nur die Nutzung zugelassener USB-Geräte zulässt. Dabei arbeiten diese Anwendungen in der Regel mit einem Whitelisting-Verfahren. Das heißt, zugelassene USB-Geräte müssen beim USB-Wächter registriert werden und können dann problemlos genutzt werden. Werden jedoch nicht-registrierte USB-Geräte verwendet, werden diese blockiert und ihre Nutzung ist nicht möglich.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 22 (Schutz vor Schadsoftware)
- **B3S im Krankenhaus** – Kap. 7.13.4 (Schutz vor Schadsoftware)
- **ISO/IEC 27001** – A.11.2.1 (Platzierung und Schutz von Geräten und Betriebsmitteln), A.12.2 (Schutz vor Schadsoftware)
- **BSI IT-Grundschutz-Kompendium** – SYS.3.4 (Mobile Datenträger)

6.6 Benutzerfreundliche Absicherung der Endgeräte zur mobilen Visite ■

Kurzbeschreibung

Komplettsysteme zur mobilen Visite haben in den vergangenen Jahren starken Einzug in die Krankenhäuser gehalten. Diese Rechner, die praktisch im öffentlichen Raum stehen, müssen einerseits entsprechend abgesichert werden; andererseits sind vor allem benutzerfreundliche Lösungen notwendig, um die Akzeptanz bei Ärzten und Pflegepersonal mit den Sicherungen nicht zu stark zu strapazieren.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			
IT-Abteilung	•		
Personal/Nutzer			•

Die Umsetzung der Maßnahmen muss durch die IT-Abteilung erfolgen. Dabei sollte diese ebenfalls in regelmäßigem Kontakt mit den eigentlichen Nutzern aus der Medizin bleiben und Probleme im Betrieb mit umgesetzten Maßnahmen diskutieren.

Umsetzung der Maßnahme

Bei Clients für die mobile Visite sind einige Aspekte zu berücksichtigen, insbesondere auch **hygienische Richtlinien**, welche aber in dieser Maßnahme nicht behandelt werden, da hier ausschließlich Aspekte der IT-Sicherheit genannt werden.

Gefahren in der mobilen Visite

Bei der client-gestützten mobilen Visite müssen unterschiedliche Gefahren berücksichtigt werden. Einerseits werden diese Rechner im **öffentlichen Raum** eingesetzt, sodass potenziell viele (auch unbekannte) Personen Zugriff auf die Systeme bekommen können. Entsprechend müssen **unautorisierte Einsicht** von Informationen sowie **unautorisierter Zugriff** auf Daten und Funktionen verhindert werden.

Da Clients für die mobile Visite mobil sind, ist **Diebstahl** ein zu berücksichtigendes Problem. Hier muss, abgesehen vom finanziellen Schaden durch den Verlust des Gerätes, vor allem sichergestellt werden, dass **keine nutzbaren Daten** über Patienten oder Interna entwendet werden können.

Auch muss die **Kommunikation** zwischen Diensten (z. B. dem KIS) und Clients **abgesichert** werden. Mobile Geräte sind üblicherweise über WLAN angebunden, welches entsprechend abgesichert werden muss.

Automatische Bildschirmsperre

Um zu vermeiden, dass Clients potenziell unbeaufsichtigt und für jedermann zugriffsbereit herumstehen, muss eine automatische **Bildschirmsperre** aktiviert werden. Dabei sollte mit dem medizinischen Personal ein geeigneter Kompromiss hinsichtlich einem geeigneten Timeout (z. B. nach **10 Minuten** Inaktivität) gefunden werden, damit die Sperre nicht als störend im Betrieb empfunden wird.

Authentifizierung

Eine geeignete Authentifizierung ist besonders wichtig für die Benutzerakzeptanz (vgl. auch Maßnahme 6.9 Benutzerfreundliche Authentifizierung im Krankenhausbetrieb ■). Der klassische Passwort-Login funktioniert zwar, ist aber relativ zeitintensiv (besonders mit Nutzerwechsel). Nutzer neigen daher oft dazu, eigentlich notwendige Bildschirmsperren nicht einzusetzen, sondern Rechner ungesperrt zu lassen. Eine möglicherweise geeignete Alternative bieten **kontaktlose Smart Cards**, die im Betrieb viel Zeit sparen können. Oft kann die Nutzung zur Erhöhung der Sicherheit mit einem kurzen **PIN** kombiniert werden. Gleichzeitig können dieselben Smart Cards für die Zutrittskontrolle zu Räumen genutzt werden (vgl. Maßnahme 8.2 Managebare Zutrittskontrolle zu nicht-öffentlichen Bereichen ■■).

Festplattenverschlüsselung

Etwaige Datenträger in Clients für die mobile Visite müssen verschlüsselt sein, um insbesondere bei Diebstahl die Vertraulichkeit der sich darauf befindenden Daten sicherzustellen. Dabei sollte jedoch auch die Benutzerfreundlichkeit berücksichtigt werden; zum Beispiel, indem nicht bei jedem Neustart das Passwort für die Festplattenverschlüsselung manuell durch die IT-Abteilung eingegeben werden muss. Produkte wie Microsoft **Bitlocker** unterstützen ebenfalls die Smart-Card-Authentifizierung, um Datenträger zu entschlüsseln.

Einsatz von Thin-Clients

Eine andere Variante zur Absicherung besteht darin, gar keine vertraulichen Daten persistent auf den Clients zu halten, sondern Thin-Clients einzusetzen (vgl. auch Maßnahme 6.1 Handhabbarkeit von Arbeitsplatzrechnern und Rechnern des medizinischen Betriebs ■). Im Falle des Diebstahls eines Geräts entsteht dann lediglich ein finanzieller Schaden. Da Thin-Clients ausschließlich über das Netz arbeiten, ist zu beachten, dass ein breiter Ausbau des **WLANs** vorausgesetzt ist und es auf den Stationen keine „Funklöcher“ gibt. Auch muss

die notwendige Bandbreite zuverlässig vorhanden sein (vgl. Maßnahme 5.6 Sicheres WLAN für Personal und Patienten).

Sicherer Kommunikationskanal

Schließlich muss auch die Kommunikation von Geräten der mobilen Visite abgesichert werden, falls eine vermeintlich sichere WLAN-Konfiguration durch Schwächen ausgehebelt werden kann. Einige reale Gefahren wurden in Maßnahme 5.6 Sicheres WLAN für Personal und Patienten zusammengefasst. Eine relativ einfache Variante zur Absicherung ist die Einrichtung eines virtuellen privaten Netzes (VPN). Auf diese Weise kann der Kommunikationskanal von Clients zum Krankenhaus-Rechenzentrum abgesichert werden. Ein VPN ist heutzutage relativ einfach einzurichten, beispielsweise über das inzwischen etablierte *OpenVPN*[7] oder sehr moderne Lösungen wie *WireGuard*.[8]

Sonstiges

Natürlich müssen mobile Geräte für die Visite auch vor Malware geschützt werden. Dazu sollten alle nicht unbedingt benötigten Schnittstellen deaktiviert werden (siehe Maßnahme 6.5 Schnittstellen und sichere mobile Datenträger im Krankenhaus), die mobilen Geräte in ihrem eigenen Netz liegen und nur mit notwendigen Systemen kommunizieren können (Maßnahme 5.2 Logische Aufteilung des Krankenhausnetzes).

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 21 (Härtung und sichere Basiskonfiguration der Systeme und Anwendungen), 27 (Mobile Sicherheit, Telearbeit, Bring Your Own Device (BYOD))
- **B3S im Krankenhaus** – 7.13.7 (Sichere Authentifizierung), 7.13.8 (Kryptographische Absicherung), 7.13.1 (Netz- und Systemmanagement)
- **ISO/IEC 27001** – A.9.4 (Zugangssteuerung für Systeme und Anwendungen), A.13.1.3 (Trennung in Netzwerken), A.13.2 (Informationsübertragung), A.14.1 (Sicherheitsanforderungen an Informationssysteme), A.12.2 (Schutz vor Schadsoftware)
- **BSI IT-Grundschutz-Kompendium** – SYS3.1 (Laptops), ORP.4 (Identitäts- und Berechtigungsmanagement), NET.1.1 (Netzarchitektur und -design)

[7] https://openvpn.net/
[8] https://www.wireguard.com/

6.7 Sichere mobile Geräte für den Krankenhausbetrieb ■ ■ ■

Kurzbeschreibung

Der Nutzen mobiler Geräte wie Smartphones und insbesondere Tablet-PCs wird im Zuge der Digitalisierung auch für Krankenhäuser bedeutsamer, beispielsweise zur Kommunikation oder mobilen Visite. Die Absicherung mobiler Geräte unterscheidet sich jedoch von jener der klassischen Endgeräte.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			
IT-Abteilung	•		
Personal/Nutzer			

Die Absicherung mobiler Geräte muss durch die IT-Abteilung vorgenommen werden.

Umsetzung der Maßnahme

Im Gegensatz zu stationären Clients zeichnet sich der Einsatz mobiler Geräte im Krankenhaus durch einige Unterschiede aus. Sie sind generell über **WLAN** angebunden, sind leicht und **handlich**, wodurch sie jedoch auch Gefahr laufen, einfacher gestohlen oder beschädigt zu werden, und bringen softwaretechnisch die Besonderheit mit, dass sie unter Umständen nicht ganz so lange und gut hinsichtlich Softwareupdates und **Sicherheitspatches** vom Hersteller versorgt werden.

Sichere Netzanbindung

Um mobile Geräte sicher ans Krankenhausnetz anzubinden, muss die Netzinfrastruktur geeignet abgesichert und konzipiert sein. Die Absicherung der WLAN-Infrastruktur ist in Maßnahme 5.6 Sicheres WLAN für Personal und Patienten ■ detailliert beschrieben. Hier ist es zum Beispiel wichtig, ein vom Patienten-WLAN **abgetrenntes internes WLAN** zu betreiben, um betriebliche mobile Geräte von denen der Patienten auch im Netz grundlegend zu trennen. Dieses sollte entsprechend abgesichert sein, z. B. über **802.1X**-Authentifizierung statt des einfacheren PSK-Verfahrens und starker Verschlüsselung. Des Weiteren kann auch hier für besonders sensible Informationen noch ein zusätzliches virtuelles Netz via VPN (mit zusätzlicher Authentifizierung) darübergelegt werden, um beispielsweise interne Dienste (z. B. eine Dateiablage) zu erreichen.

Maßnahmen gegen Verlust und Beschädigung

Gleichermaßen anwendbare Aspekte zum Verlust eines Geräts werden ebenfalls in Maßnahme 6.6 Benutzerfreundliche Absicherung der Endgeräte zur mobilen Visite ■, Maßnahme 8.1 Zonenkonzepte und ihre Realisierung im Krankenhaus ■■ sowie Maßnahme 8.3 Physischer Schutz von Geräten und Informationen im öffentlichen Raum ■■ beschrieben. Gegen Diebstahl und Verlust ist es vor allem von Bedeutung, dass **keine Daten oder Einstiegspunkte** (d. h. Fremde können über Geräte Krankenhaus-Dienste nutzen) für unautorisierte Nutzer verwendbar sind. Dafür sind einerseits Standardmaßnahmen wie **Bildschirmsperren**, **Authentifizierung**, **Verschlüsselung der Datenträger**, jedoch auch sogenannte **Mobile Device Management** (MDM) Lösungen sehr empfehlenswert. Letztere ermöglichen in der Regel nicht nur eine Remote-Verwaltung solcher Geräte, sondern erlauben auch eine **Sperrung** oder **komplette Werkzustandsherstellung** des Geräts. Seine Daten und Funktionen können dann nicht mehr verwendet werden.

Mobile Geräte tendieren wegen des häufigen Herumtragens jedoch auch dazu, schneller einen **Defekt** zu bekommen (z. B. versehentliches Fallenlassen). Genau wie durch Diebstahl ist das Fehlen dieser Ressource im Betrieb das Resultat. Das einzige wirksame Mittel dagegen ist die Vorrathaltung von **Ersatzgeräten**; eine eigenständige Reparatur ist in der Regel nicht möglich.

Absicherung der Software

Bei mobilen Geräten wie Smartphones oder auch Tablet-PCs mit einem entsprechenden Betriebssystem für mobile Geräte ist zu beachten, dass der Markt sehr schnelllebig ist und entsprechende Geräte von Softwareherstellern oft nur vergleichsweise **kurz unterstützt** werden. Entsprechend sollte man auf Hersteller setzen, die vergleichsweise lange Support-Zeiträume garantieren.

Ein weiterer wichtiger Aspekt ist die Beschränkung von Nutzerrechten auf mobilen Geräten. Üblicherweise sollen Nutzer **nicht alle Apps** auf einem mobilen Gerät **nutzen** (z. B. Administrationsanwendungen) und **keine Apps installieren** dürfen. Auch hierfür gibt es üblicherweise Lösungen für gängige mobile Geräte, um genau dieses einzuschränken. So werden ausgewählte Apps durch eine PIN gesichert. Auf diese Weise kann verhindert werden, dass vertrauensunwürdige und schadhafte Programme heruntergeladen und ausgeführt werden. Generell ist zu beachten, dass ausschließlich Apps aus vertrauenswürdigen Quellen installiert werden.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 21 (Härtung und sichere Basiskonfiguration der Systeme und Anwendungen), 27 (Mobile Sicherheit, Telearbeit, Bring Your Own Device (BYOD))
- **B3S im Krankenhaus** – Kap. 7.13.9 (Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit)
- **ISO/IEC 27001** – A.6.2 (Mobilgeräte und Telearbeit)
- **BSI IT-Grundschutz-Kompendium** – SYS.3.2.1 (Allgemeine Smartphones und Tablets), SYS.3.2.2 (Mobile Device Management (MDM)), SYS.3.2.3 (iOS (for Enterprise)), SYS.3.2.4 (Android), SYS.3.3 (Mobiltelefon)

6.8 Absicherung nicht managebarer Geräte

Kurzbeschreibung

Einige Geräte sind nicht effektiv managbar, d. h. sie können nicht wie klassische IT-Systeme (Server oder Clients) abgesichert werden und behalten daher oft für lange Zeit bekannte Schwachstellen in ihrer Software. Dennoch müssen diese Systeme besonders abgesichert werden, da sie hochsensible Daten generieren, verarbeiten und ins Krankenhausnetz kommunizieren. In dieser Maßnahme werden einige praktische Möglichkeiten aufgezeigt.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			
IT-Abteilung	•		
Personal/Nutzer			•

Umsetzung der Maßnahme

Die Hauptproblematik medizinischer Geräte ist die darauf erzwungene Sicht als **Black-Box-System**: Betreiber können nicht, wie anderswo, Sicherheitspatches einspielen oder Sicherheitssoftware installieren. Entsprechend müssen Maßnahmen daran angepasst werden. Zunächst ist es sinnvoll, sich einen Überblick über **offensichtliche Schwachstellen** zu verschaffen.

Schwachstellensuche

Auch hier kann praktisch nur von außen nach Schwachstellen gesucht werden. Dennoch gelten hier ähnliche Regeln wie bei anderen netzangebundenen Black-Box-Systemen ohne direkten Zugriff. Da derartige Methoden zu Abstürzen oder unerwartetem Verhalten führen können, sollte **nur an momentan nicht produktiv eingesetzten Geräten** getestet werden.

Zunächst sollte sich ein Betreiber über etwaige auf dem Gerät über das Netz erreichbare **Dienste** informieren, in der Praxis über einen **Port-Scan** (z. B. mit nmap[9]). Dieser listet offene **Ports** auf und kann unter Umständen auch das Betriebssystem und die Dienst-Software (inklusive Version) dahinter identifizieren.

Anhand des Ergebnisses des Port-Scans können dann weitere Maßnahmen getroffen werden, beispielsweise das manuelle **Nachschlagen von Schwachstellen** für das detektierte Betriebssystem und die Dienst-Software (z. B. bei der CVE[10] oder bei Hersteller-Meldungen).

Für detektierte Software, wie beispielsweise *Telnet* oder *SSH*, kann auch nach **schwachen Login-Daten** gesucht werden, zum Beispiel per Websuche nach bekannten Default-Login-Daten oder über automatisierte Login-Brute-Force-Anwendungen (im Web sind mehrere zu finden).

```
ms@ubuntutest:~$ sudo nmap -sS -O -sV 10.0.20.5

Starting Nmap 7.01 ( https://nmap.org ) at 2020-02-18 15:37 CET
Nmap scan report for 10.0.20.5
Host is up (0.00025s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE     VERSION
22/tcp  open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu L
inux; protocol 2.0)
80/tcp  open  http        Apache httpd 2.4.18 ((Ubuntu))
139/tcp open  netbios-ssn Samba smbd 3.X (workgroup: TESTBUNTU)
445/tcp open  netbios-ssn Samba smbd 3.X (workgroup: TESTBUNTU)
MAC Address: 08:00:27:3D:F1:17 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.0
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect res
ults at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.05 seconds
```

Abbildung 6.4: Beispielhafte Ausgabe von nmap

Auch kann die Sicherheit etwaiger **verschlüsselter Kommunikation eingeschätzt** werden, beispielsweise in TLS anhand eingesetzter *Cipher-Suites* (oft werden aus Kompatibilitätsgründen veraltete Verfahren eingesetzt). Im Web gibt es Anleitungen für das *OpenSSL*–Tool unter Linux. Auch bietet Mozilla[11] eine erste Übersicht über sichere und unsichere Ciphers.

In diesem Kontext ist es zudem wichtig, sich bei gefundenen offensichtlichen Schwachstellen mit dem jeweiligen **Hersteller in Verbindung** zu setzen, um diese möglicherweise flächendeckend über einen Patch der Systeme zu schließen.

Absicherung am Gerät

Um gefundene potenzielle Lücken (im Netz) zu schließen, können am Gerät einige Maßnahmen angewandt werden. Eine praktische Maßnahme am Gerät ist es beispielsweise, eine kleine **zusätzliche Appliance** im Netz zwischen medizinischem Gerät und Netzdose zu installieren. Geräte mit **zwei RJ45**–Netzdosen können als **Firewall** zwischengeschaltet werden, um offene Dienste am medizinischen Gerät zu sperren. Auch kann ein **VPN-Gateway** davorgeschaltet werden, das potenziell ungesicherte Kommunikation verschlüsselt. Eine weitere Möglichkeit, diese Appliances zu nutzen, besteht darin, gesonderte **Netzwerk-Sniffer** (z.B. tcpdump, tshark) darauf zu installieren und Verbindungen aus dem Krankenhaus-Netz zu einem jeweiligen medizinischen Gerät im Detail zu überwachen und *dubiose* Verbindungen zu sperren (was jedoch im Fehlerfall auch zu Beeinträchtigungen der Funktionalität des Geräts führen kann).

[9] https://nmap.org/
[10] https://cve.mitre.org/
[11] https://wiki.mozilla.org/Security/Server_Side_TLS

Eine ebenfalls allgemein empfehlenswerte und einfache Maßnahme besteht darin, **ungenutzte** medizinische Geräte **vom Netz zu trennen**. So wird auch die Ausbreitung von Malware verhindert und die Verfügbarkeit ungenutzter Geräte erhöht.

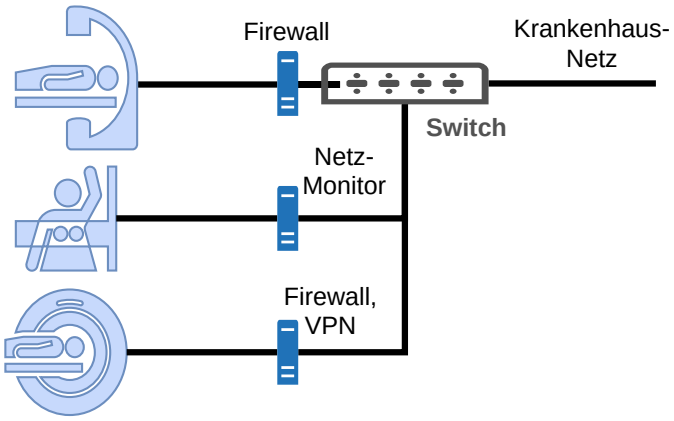


Abbildung 6.5: Appliances zur Absicherung von medizinischen Geräten

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 19 (Netz- und Systemmanagement), 23 (Firewall, Intrusion Detection)
- **B3S im Krankenhaus** – 7.13.5 (Intrusion Detection/Prevention), 7.13.8 (Kryptographische Absicherung)
- **ISO/IEC 27001** – A.9.1.2 (Zugang zu Netzen und Netzwerkdiensten), A.10 (Kryptographie), A.12.2 (Schutz vor Schadsoftware), A.13.1.3 (Trennung in Netzwerken)
- **BSI IT-Grundschutz-Kompendium** – NET.1.1 (Netzarchitektur und -design), NET.3.2 (Firewall), NET.3.3 (VPN)

Absicherung im Netz

Eine andere (unter Umständen kostengünstigere) Variante ist die Möglichkeit, diese Geräte dediziert über geeignete Netzmaßnahmen abzusichern. Im Idealfall werden diese Maßnahmen jedoch komplementär eingesetzt.

Einerseits bietet die in Maßnahme 5.2 Logische Aufteilung des Krankenhausnetzes ■ beschriebene Netzsegmentierung bereits einen relativ guten Schutz. Sie verhindert, dass medizinische Geräte im Krankenhausnetz von nicht autorisierten Systemen erreicht werden (beispielsweise aus der Verwaltung oder dem Patienten-Subnetz). Hier sollte darauf geachtet werden, dass medizinische Geräte nur mit notwendigen Gegenstücken (z. B. dem KIS) in einem Netz liegen. Auch sollte die Kommunikation der medizinischen Geräte nach Möglichkeit untereinander unterbunden werden, damit etwa Malware sich nicht so leicht unter diesen ähnlichen Systemen ausbreiten kann.

Eine weitere sinnvolle Maßnahme, die zur Absicherung von medizinischen Geräten beiträgt, ist das in Maßnahme 5.5 Schließen von Einfallswegen für und Eindämmung von Malware im Krankenhausnetz ■■■ beschriebene **DNS-Blacklisting**. Diese Blacklisten haben oft nicht nur Werbe-Domainnamen gebannt, sondern auch bösartige Domains, von denen Malware oft notwendige Kommandos empfängt (z. B. C&C Server von Botnetzen) oder weitere schädliche Malware nachlädt. Eine komplette Sicherheit kann dadurch zwar auch nicht geboten werden, aber sie wird weiter erhöht.

6.9 Benutzerfreundliche Authentifizierung im Krankenhausbetrieb ■

Kurzbeschreibung

Eine an den medizinischen Betrieb angepasste Authentifizierung an Endgeräten und insbesondere medizinischen Clients ist notwendig, damit das medizinische Personal Sicherheitsrichtlinien, wie Bildschirmsperren, *im Alltag umsetzen kann. Eine Kombination aus Benutzername und Passwort, wobei letzteres noch möglichst komplex und lang sein muss, um als sicher zu gelten, ist nicht selten hinderlich im laufenden Betrieb. Andere Methoden sind deutlich zeitsparender und aufgrund besserer Akzeptanz bei Nutzern sicherer.*

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			•

Die IT-Abteilung muss eine geeignete Authentifizierungslösung für diese Zwecke finden. Da je nach Lösung variierende Kosten anfallen können, muss die Geschäftsführung einbezogen werden und die entsprechende Lösung freigeben. Endnutzer (das medizinische Personal) sollten hinsichtlich der Anforderungen (z. B. Zeitersparnis, Hygiene) befragt werden.

Umsetzung der Maßnahme

Die auch in Krankenhäusern oft eingesetzte **Benutzername-Passwort-Kombination** zur Authentifizierung an Endgeräten lässt sich oft **nicht optimal** mit dem medizinischen alltäglichen Betrieb vereinbaren. So wird es nicht selten als hinderlich empfunden, bei jedem Verlassen eines Endgeräts dessen Bildschirm zu sperren und bei der nächsten Benutzung mit einem möglichst sicheren Passwort (vgl. *Bildschirmsperren* und *Passwort-Richtlinie* aus Maßnahme 3.4 Sicherheitsrichtlinien im Krankenhaus ■) wieder zu entsperren. Entsprechend kommt es vor, dass diese **Vorgaben umgangen** und Rechner nicht gesperrt werden, wobei der Sicherheitsgewinn komplett verloren geht.

Andere Authentifizierungslösungen, wie beispielsweise **biometrische** Verfahren, **Smart-Card**-Authentifizierung oder **USB-Stick**-basierte Verfahren, scheinen ein vielversprechender Ersatz zu sein. Andere wünschenswerte Ansätze, wie mobile Authentifizierungsverfahren, zum Beispiel über ein Smartphone, würden zwar eine praktische Lösung bereitstellen, sind jedoch in einer Krankenhausumgebung oft ungeeignet.

USB-Stick- und Smart-Card-Authentifizierung

Die erste Variante zur Ablösung passwortbasierter Authentifizierungsverfahren im medizinischen Betrieb ist die Einführung eines **USB-Stick**- oder **Smart-Card**-basierten Verfahrens. In diesem Fall würde jeder IT-System-Nutzer (insbesondere für Clients im medizinischen Betrieb) einen eigenen USB-Stick mit sich führen. Zur Authentifizierung wird der USB-Stick am jeweiligen Gerät **eingesteckt** und eine PIN eingegeben, wodurch er authentifiziert und **am System angemeldet** wird. Bei **Abziehen** des USB-Sticks wird die **Sitzung wieder gesperrt**. Für Smart-Cards gilt diese Vorgehensweise analog. Dabei muss darauf geachtet werden, dass **Verzeichnisdienste** wie AD oder LDAP, sofern sie genutzt werden, auch von der jeweiligen Lösung unterstützt werden.

Eine andere Variante sind kontaktlose Authentifizierungsverfahren. Auch hier können einerseits **Smart-Cards** eingesetzt werden, die Schnittstelle zum jeweiligen Gerät ist aber üblicherweise über **Near-Field-Communication** (NFC) realisiert.

Vorteil dieses Verfahrens ist es, dass eine sehr zügige Authentifizierung stattfinden kann und das Personal somit Zeit spart. Auch können so schwache Passwörter aus dem Netz entfernt werden. Oft sind diese USB-Sticks/Smart-Cards zudem sehr robust und wasserfest, können gereinigt werden und sind damit sehr hygienisch.

Nachteil dieser Verfahren ist es, dass USB-Ports an Rechnern zugänglich sein müssen bzw. für Smart-Cards oft zusätzliche Hardware (z. B. USB-Smart-Card-Lesegeräte, ggf. in die Tastatur integriert) notwendig ist. USB-Schnittstellen können daher schwieriger abgesichert werden.

Biometrische Verfahren

Biometrische Verfahren zur Authentifizierung sind inzwischen im Alltag eines jeden angekommen. Praktisch jedes neuere Mobilfunktelefon unterstützt **Fingerabdruck**-, teilweise auch **Gesichtserkennung**. Auch im Krankenhaus sind solche Verfahren denkbar und können Passwörter selektiv ablösen. Andere Varianten, wie Handvenen-, Fingervenen- und **Stimmerkennung**, sind auch möglich, jedoch in einer Krankenhausumgebung nur bedingt nützlich. Stimmerkennung ist wohl nur in Umgebungen mit wenig Hintergrundgeräuschen (z. B. einem separaten Behandlungsraum) einsetzbar, aus hygienischer Sicht aber, ebenso wie die Gesichtserkennung, wohl von Vorteil.

Single-Sign-On

Wesentlich zur Nutzerfreundlichkeit kann **Single-Sign-On** mit der Nutzung mehrerer Dienste (z.B. auch Netzlaufwerke) durch eine einzige Anmeldung beitragen. So spart eine automatische Anmeldung im KIS-Client

bei Anmeldung am Arbeitsplatz ebenfalls Zeit. Derartige Lösungen gibt es teilweise entweder von KIS-Herstellern oder von Drittanbietern, aber nicht für jedes System/KIS.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 25 (Sichere Authentisierung)
- **B3S im Krankenhaus** – Kap. 7.13.7 (Sichere Authentisierung)
- **ISO/IEC 27001** – A.9.4.2 (Sichere Anmeldeverfahren)
- **BSI IT-Grundschutz-Kompendium** – ORP.4 (Identitäts- und Berechtigungsmanagement), SYS.2.1 (Allgemeiner Client)

Kapitel 7

Sichere zentrale Dienste

Dieser dritte technische Block betrifft die Absicherung der überaus wichtigen zentralen Dienste im Krankenhaus. Der Fokus liegt hier auf der Absicherung der Systeme, die in einem Krankenhaus-Serverraum betrieben werden. Dabei werden die folgenden Thematiken angesprochen:

- Die Absicherung eines Serverraums (bzw. Rechenzentrums) in einem Krankenhaus, um somit die physische Plattform – die Server – von Diensten zu schützen.
- Möglichkeiten zur Abmilderung von krankenhausspezifischen Problemen wie einer Rund-um-die-Uhr-Verfügbarkeitsanforderung.
- Spezifika bei der Server-Überwachung (im Gegensatz zur Überwachung von Endgeräten).
- Die Absicherung von Netzspeichern, welche nicht selten einen Single-Point-of-Failure im Betrieb darstellen.
- Die Erhöhung der Handhabbarkeit von Krankenhaus-Diensten über Virtualisierung.

Die Maßnahmen zur Absicherung zentraler Dienste richten sich vor allem an das Personal der IT-Abteilung im Krankenhaus.

7.1 Sichere Rechenzentren und Serverräume ■ ■ ■

Kurzbeschreibung

Das Rechenzentrum und die Serverräume stellen im Krankenhaus eine zentrale Sammelstelle für Dienste und empfindliche Informationen dar. Da das Funktionieren eines modernen Krankenhauses von ihnen stark abhängig ist, müssen Serverräume besonders abgesichert werden. Es ist zu beachten, dass diese Maßnahme den Fokus nur auf sicherheitsrelevante Aspekte legt; andere wichtige Themen, wie beispielsweise eine ausreichende Kühlung, sind davon unabhängig umzusetzen.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung	•	•	
IT-Abteilung	•		
Haustechnik	•		
Personal/Nutzer			

Die Auswahl und Absicherung von Serverräumen betrifft mehrere Abteilungen: Die Geschäftsführung, die Haustechnik und auch die IT-Abteilung.

Umsetzung der Maßnahme

Auf dem Weg zu einem sicheren Serverraum gibt es einige Hürden. Angefangen bei der Wahl des *richtigen* Raumes über die Installation notwendiger Systeme für dessen Absicherung bis hin zur Sicherung von Systemen und Diensten.

Auswahl geeigneter Räume

Die Wahl eines ungeeigneten Serverraums kann ein Krankenhaus und die Verantwortlichen im betrieblichen Alltag dauerhaft belasten und einsetzbare Maßnahmen stark dezimieren. Zunächst muss darauf geachtet werden, dass die **Wahl des Raumes** zukünftige Maßnahmen unterstützt, beispielsweise hinsichtlich Löschanlagen, Alarm- und Überwachungssystemen, Klimaanlagen, usw. Altbau-Räume oder Gebäude, die als **Baudenkmale** eingestuft sind, machen derartige Vorhaben oft unmöglich oder mindestens sehr schwierig und sollten von vornherein ausgeschlossen werden.

Auch ist die **Lage des Serverraumes** nicht unerheblich, da er als Sicherheitsbereich gelten muss (vgl. auch Maßnahme 8.1 Zonenkonzepte und ihre Realisierung im Krankenhaus ■ ■). Er sollte nicht direkt an öffentliche Bereiche (Fenster sowie Türen) grenzen, um Unberechtigten jeglichen Zugriff zu erschweren. Beispielsweise kann bereits ein dünner Gartenschlauch, durch einen Spalt geschoben, das Ende der IT-Infrastruktur bedeuten. Deshalb ist es ebenfalls notwendig, Räume mit Fenstern für diesen Zweck zu vermeiden oder diese zumindest entsprechend so abzusichern, wie es im Laufe der Maßnahme beschrieben wird.

Ebenso ist die **Beschaffenheit des Raumes** wichtig. So sollte er langfristig nutzbar und entsprechend groß gewählt sein. Zur Nutzbarkeit zählen auch Aspekte wie die Ausbaufähigkeit der Netzinfrastruktur und Netzanbindung. Neben verstärkten Fenstern und Türen müssen auch die Wände zum Serverraum eine angemessene Festigkeit aufweisen. Gipskarton-Wände sind daher völlig unzureichend. Jedoch sind auch weniger intuitive Aspekte zu beachten, beispielsweise die Reinigung und das Staubpotenzial von Räumen. Ein Serverraum sollte einfach zu reinigen sein und unnötige Objekte (Teppich, Stühle, Tische, Bücher, usw.) sollten aus diesem Grund entfernt werden.

Wie in Maßnahme 6.4 Automatisierte Datensicherung zur effektiven Wiederherstellung ■ beschrieben, ist es auch ratsam, für Backups einen weiteren separaten Serverraum vorzusehen.

Grundabsicherung – Zugriff und Feuer

Generell muss ein Serverraum grundlegend hinsichtlich unterschiedlicher Aspekte gesondert abgesichert werden.

Zunächst muss sichergestellt werden, dass nur **berechtigte Personen Zugang** zum Serverraum haben. Entsprechend müssen Türen und Fenster (und Wände) effektiv vor einem gewaltsamen Eindringen geschützt sein. Fenster müssen, wenn sie leicht von außen zugänglich sind (z. B. im Erdgeschoss in Richtung öffentliche Straße), durch **Sicherheitsfenster** ersetzt werden. Ein Gitter allein hilft beispielsweise nicht gegen das Eindringen von Wasser in den Serverraum. Auch muss an Fenstern ein **Sichtschutz** (z. B. mit Folierung) angebracht sein.

Bei Türen hingegen empfiehlt sich ein **elektronisches Türschloss** (z. B. mit Token oder Fingerabdruck), durch das gleichzeitig der Zutritt **protokolliert** und nachvollzogen werden kann. Ein mechanisches Türschloss (mit sicher verwahrtem Schlüssel) sollte jedoch als Notfallsystem existieren (z. B. bei Stromausfall). Die **Zutrittsprotokollierung** ist darüber hinaus z. B. für Gäste oder Service-Mitarbeiter ebenfalls unbedingt vorzunehmen, beispielsweise über eine Papier-Liste (mindestens mit Angabe von Name, Firma, Datum, Zweck, Unterschrift), welche direkt innen am Zugang aufbewahrt wird. Darüber hinaus sollten nicht nur der Serverraum selbst, sondern auch Systeme darin vor unmittelbarem Zugriff geschützt werden, beispielsweise über **abschließbare Serverschränke**.

Besonders bei **Brandfällen** ergeben sich für Serverräume weitere Hürden. Zunächst muss eine geeignete Brandmeldeanlage installiert sein, welche unter Um-

ständen mit einer automatischen Gaslöschanlage (in der Regel mit Argon oder Stickstoff) verknüpft ist. Mindestens müssen aber ausreichend Feuerlöscher in unmittelbarer Nähe erreichbar sein. Um im Brandfall bis dahin verschonte Systeme nicht durch das Löschmittel (insbesondere Wasser, Schaum, Pulver) zu zerstören, eignen sich in der Praxis nur **CO_2-Feuerlöscher**. (Deren Anwendung ist in geschlossenen Räumen und bei falscher Handhabung wiederum lebensgefährlich.) Es ist ein Gesamtkonzept aufzustellen und das Personal entsprechend einzuweisen.

Kontrollierbare Verfügbarkeit

Von der Verfügbarkeit der zentralen Dienste hängt heutzutage der effektive Betrieb im Krankenhaus ab. Entsprechend muss sichergestellt werden, dass die **Stromversorgung** ausreichend stabil und abgesichert ist. Ansonsten können bereits kurze Schwankungen im Stromnetz oder auch kleinste Stromausfälle (bzw. sogenannte Stromwischer) den Ausfall der gesamten Infrastruktur und folglich des Krankenhausbetriebs kurz- oder mittelfristig bewirken.

Deshalb ist die Einrichtung einer geeigneten **Unterbrechungsfreie Stromversorgung** (USV) unbedingt notwendig. Diese sollte einerseits kurze bis mittellange **Ausfälle** (durchaus mehrere Stunden) in der Stromversorgung kompensieren und andererseits **Spannungsspitzen** und Überspannung abschwächen können.

Eine USV ist jedoch nicht für längerfristige Ausfälle das Mittel der Wahl, sondern fängt kürzere Probleme mit der Stromversorgung ab. Somit kann sie den jeweiligen Administratoren die notwendige Zeit geben, um einerseits IT-Systeme kontrolliert herunterzufahren und den Krankenhausbetrieb koordiniert in einen *Notfallmodus* mit beschränkter IT-Unterstützung zu bringen (vgl. Maßnahme 3.7 Erstellung von Notfallkonzepten und Wiederanlaufplänen ■) oder andererseits, um **Netzersatzanlagen** (NEA) in Betrieb zu nehmen. Eine NEA ist in der Praxis üblicherweise ein diesel- oder benzinbetriebener Stromgenerator, welcher Stromausfälle längerfristig (Stunden bis Tage) kompensieren kann.

Diese Anlagen müssen unbedingt regelmäßig **gewartet** sowie **getestet** werden. Da die meisten Dienste im Krankenhaus rund um die Uhr lauffähig sein müssen, können als Testinfrastruktur beispielsweise ungenutzte Systeme verwendet werden, deren Ausfall den Produktivbetrieb nicht beeinflusst.

Überwachung von Serverräumen

Die Überwachung von Serverräumen ist genauso wichtig wie die von Systemen und Servern (für Letzteres siehe auch Maßnahmen 6.2 Überwachung von Endgeräten ■ und 7.3 Überwachung von Serversystemen ■).

Wichtige zu überwachende Kennzahlen von Serverräumen sind mindestens die **Raumtemperatur**, die **Luftfeuchtigkeit** (denn diese kann zu Kondensation auf der Hardware führen) und **Hinweise auf Überflutungen** sowie eine generelle **Zutritts-** und **Zugriffsüberwachung**.

Eine Zutrittsüberwachung sollte durch Sensoren an geeigneten Stellen, insbesondere an möglichen Zugängen wie Türen und Fenstern, aber auch an Türen zu Serverschränken angebracht sein. Darüber hinaus sollte ein Serverraum als gesonderter Sicherheitsbereich zusätzlich durch **Videoüberwachung** abgesichert sein. Schilder an den Zugängen zum Serverraum, welche auf die Videoüberwachung hinweisen, erfüllen dabei einerseits den Zweck der Informierung des Personals, andererseits der Abschreckung. Außerdem sind sie aus datenschutzrechtlichen Aspekten notwendig.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 11 (Robuste/resiliente Architektur), 10 (Physische Sicherheit)
- **B3S im Krankenhaus** – Kap. 7.7 (Physische Sicherheit), Kap. 7.13.15 (Protokollierung)
- **ISO/IEC 27001** – A.11 (Physische und umgebungsbezogene Sicherheit), A.12.4 (Protokollierung und Überwachung)
- **BSI IT-Grundschutz-Kompendium** – INF.2 (Rechenzentrum sowie Serverraum)
- **DIN EN 50600**

7.2 Patchen zentraler Dienste mit geringer Auswirkung auf den Krankenhausbetrieb

Kurzbeschreibung

Regelmäßige Sicherheitspatches und -Updates sind essenziell, um die Systemsicherheit aufrechtzuerhalten. Gerade aber bei Servern und zentralen Diensten können diese durch erforderliche System-Neustarts zur Nicht-Verfügbarkeit und der Beeinträchtigung des Krankenhausbetriebs führen. Mit entsprechenden Systemen und Konzepten können die Auswirkungen geringer gehalten werden.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			(•)
IT-Abteilung	•		
Personal/Nutzer			

Für die Umsetzung ist die IT-Abteilung verantwortlich. Die Geschäftsführung kann bei der Planung zur Minimierung der Auswirkungen, beispielsweise durch die Definition geeigneter Wartungsfenster, involviert werden.

Umsetzung der Maßnahme

Die regelmäßige Installation von Updates und die gleichzeitige Aufrechterhaltung des Betriebs schließen sich nicht aus. Einerseits gibt es Tools, die Live-Patching von Betriebssystemen ermöglichen, andererseits können geeignete Konzepte den updatebedingten Ausfall von Diensten abfangen.

Hilfreiche Werkzeuge

Bei Serversystemen erfordern vor allem Updates des Betriebssystems einen langwierigeren Neustart. Einzelne Dienste hingegen sind relativ schnell aktualisiert und neu gestartet. Für das unter Servern besonders verbreitete **Linux** gibt es bereits mehrere Werkzeuge, die **Live-Patching** unterstützen und einen Neustart in vielen Fällen unnötig machen. Die bekanntesten sind **kpatch**, **ksplice**, **kgraft** oder **livepatch**.

Für Windows-basierte Server ist aktuell nichts Vergleichbares bekannt.

Dienst- und System-Redundanz

Auch wenn Live-Patching einige *Ausfälle* kompensieren kann, ist als geeignetes Konzept für verfügbare Dienste **Redundanz** deutlich sicherer. Systeme können dann nicht nur ohne Ausfälle gepatcht werden, sondern überstehen unter Umständen auch Abstürze oder ähnliches.

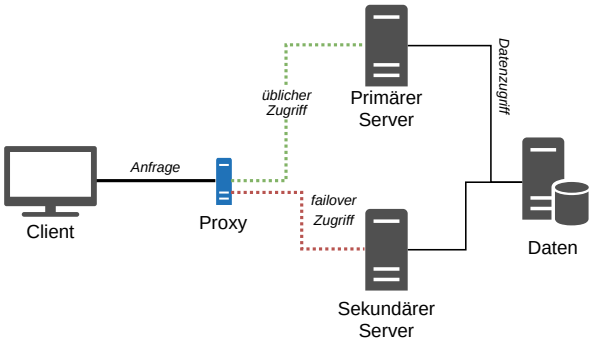


Abbildung 7.1: Redundante Dienste

Beim Aufbau eines redundanten Dienstes wird ein sekundärer Server desselben Dienstes mit derselben Konfiguration wie der primäre Server aufgesetzt. Ein eingesetzter Proxy-Dienst behandelt dann die Anfragen von Clients und überwacht die Erreichbarkeit des primären und des sekundären Servers. Bei Ausfall des primären Servers schaltet der Proxy dann automatisch auf den sekundären Server um.

Vereinfachungen können beispielsweise durch eine **zentralisierte Datenhaltung** vorgenommen werden. Dadurch ist eine aufwändigere Synchronisation der Daten zwischen dem primären und dem sekundären Server nicht notwendig. Auch **Virtualisierung** kann hier sehr hilfreich sein. Beispielsweise kann durch das Klonen einer bestehenden Server-Instanz sehr einfach eine sekundäre Instanz mit derselben Konfiguration eingerichtet werden. Auch kann **Snapshot**-Funktionalität von Virtualisierungssystemen ein funktionierendes Roll-Back-System bereitstellen.

Sobald ein Dienst redundant aufgesetzt ist, können Updates und Patches relativ einfach und sicher installiert werden. Beispielsweise zunächst bei allen sekundären Servern, dann *zeitversetzt* und nach angemessenen *Funktionstests* auch beim primären Server, wobei der Proxy-Dienst zur Überbrückung auf den sekundären Server umschaltet.

Als **Proxy-Dienst** gibt es bereits einige auch frei nutzbare sowie Open-Source-Anwendungen mit detaillierten Anleitungen im Web. Ein beliebter und funktionsreicher Proxy-Dienst ist *HAProxy*[1].

Organisatorisches

Generell bietet es sich an, für Patches und Updates der zentralen Infrastruktur ein regelmäßiges **Wartungsfenster** festzulegen. Das hat den Vorteil, dass einerseits Updates überwiegend gesammelt erfolgen und somit mögliche Ausfallzeiten konzentriert an einem

[1] http://www.haproxy.org/

Zeitpunkt stattfinden, und andererseits, dass Verwaltung, Ärzte und Pflege sich auf mögliche Probleme einstellen können. Da ein Krankenhaus prinzipiell einen 24-Stunden-Betrieb aufrechterhalten muss, ist die Findung eines geeigneten Wartungsfensters keine leichte Aufgabe. In Abstimmung mit der Geschäftsführung sollte hier ein geeignetes Zeitfenster (z. B. *jeden Dienstag zwischen 7:00 und 8:00 Uhr*) gefunden werden.

Auch kann dabei zwischen kritischen und weniger kritischen Diensten unterschieden werden. So ist der Web-Auftritt eines Krankenhauses weniger kritisch als das KIS und könnte auch außerhalb des Wartungsfensters mit Updates versorgt werden, um den Aufwand zu entzerren.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 11 (Robuste/resiliente Architektur), 30 (Patch- und Änderungsmanagement)
- **B3S im Krankenhaus** – Kap. 7.13.13 (Patch- und Änderungsmanagement),
- **ISO/IEC 27001** – A.11.2.4 (Instandhalten von Geräten und Betriebsmitteln), A.13.1.2 (Sicherheit von Netzwerkdiensten)
- **BSI IT-Grundschutz-Kompendium** – OPS.1.1.3 (Patch- und Änderungsmanagement), SYS.1.1 (Allgemeiner Server)

7.3 Überwachung von Serversystemen ■

Kurzbeschreibung

Die Überwachung von Servern ist jener von Clients (siehe Maßnahme 6.2 Überwachung von Endgeräten ■) relativ ähnlich. Jedoch müssen hier weitere Aspekte berücksichtigt werden, welche auch unabhängig von Malware-bedingten Vorfällen die Nutzung davon abhängiger Dienste beeinflusst.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			
IT-Abteilung	•		
Personal/Nutzer			

Die Überwachung von Serversystemen muss durch die IT-Abteilung vorgenommen werden.

Umsetzung der Maßnahme

Neben der auch bei der Überwachung von Endgeräten wichtigen Erkennung und Behebung von Malware und Einbruchserkennung sind zusätzliche Parameter hinsichtlich Hardware- und Software-Gesundheit zu berücksichtigen. Diese können den Absturz von wichtigen zentralen Diensten wie dem KIS oder dem zentralen Dateiserver verursachen und somit den Krankenhausbetrieb enorm stören.

Wichtige überwachenswerte Parameter

Damit alle Dienste zuverlässig funktionieren, müssen ihre Hostsysteme unterschiedliche Voraussetzungen erfüllen. Es muss ausreichend **Festplattenspeicher** sowie **Arbeitsspeicher** verfügbar sein, die CPUs dürfen hinsichtlich der Performanz sowie der Anzahl an zu erbringenden Diensten nicht unterdimensioniert sein (was üblicherweise einfach über die **Load Average** in Zahlen ausgedrückt wird). Zusätzlich muss der **Netzdurchsatz** ausreichend dimensioniert sein, damit Dienste zuverlässig auf andere Dienste zugreifen können und ebenso auch Clients (z. B. Netzspeicher).

Auf der anderen Seite sollten wichtige Dienste (im Sinne von Systemdiensten auf Servern) selbst überwacht werden. Dazu zählt in erster Linie die zentrale Überwachung der **Verfügbarkeit** der Dienst-Plattform bzw. des **Servers**, auf dem der jeweilige Dienst läuft, und des Weiteren die Verfügbarkeit der **Anwendung**, die den Dienst realisiert, sowie Hilfsdienste auf den Servern (z. B. SSH, RDP). Auch sollte überwacht werden, ob und wie viele **Updates** auf einem Host bereit zur Installation sind und noch ausstehen.

Generell muss die Überwachung **zentralisiert** sein, d. h. Informationen über alle Server müssen zentral gesammelt und zur Übersichtlichkeit mit einer entsprechenden **graphischen Nutzeroberfläche** visualisiert werden. Auch sind proaktive automatische Benachrichtigungen, beispielsweise via **E-Mail**, sehr hilfreich, um Probleme schnell zu erkennen und zu behandeln.

Werkzeuge zur Überwachung

Ein mögliches Monitoring-Werkzeug, das die im vorherigen Abschnitt genannten Anforderungen praktisch direkt erfüllen kann, ist das Open-Source-Tool **Icinga2**.[2]

Icinga2 erlaubt die Unterteilung des überwachten Netzes in Zonen, wobei eine Zone üblicherweise durch einen **Satellite**-Knoten überwacht wird. Das gesamte Netz wird durch einen **Master**-Knoten überwacht, welcher alle Ereignisse von Satellite-Knoten und **Agent**-Knoten (jeweils auf einem überwachten Host separat installiert oder direkt über SSH überwacht) sammelt. Generell können Satellite-Knoten auch weggelassen werden; sie können jedoch in einem großen Netz mit vielen Subnetzen für eine sicherere Zugriffs-Struktur sorgen, da beispielsweise die Kommunikation zwischen Master und Satellites leichter über entsprechende Firewall-Regeln zwischen den Sub-Netzen gelöst werden kann, anstatt jeden Host einzeln freizuschalten.

Icinga2 basiert auf Nagios und erlaubt die Verwendung seiner bereits stark ausgebauten Monitoring-Plugins. Ein wichtiger Vorteil ist, dass Icinga2 eine klare und selbsterklärende Web-UI bereitstellt. Sie kann praktisch von jedem Host im Browser aufgerufen werden und zeigt eine Zusammenfassung überwachter **Systeme**, ihren generellen Verfügbarkeitszustand und den Status verschiedener **Dienste** und Parameter (vgl. vorherigen Abschnitt). Auch erlaubt Icinga2 die Festlegung von Schwellwerten (z.B. für die Auslastung von Festplattenspeicher und von CPU-Load). Generell besteht auch die Möglichkeit zur Erweiterung von Checks und Plugins, was besonders für spezialisierte Dienste, wie sie im Krankenhausbetrieb benötigt werden, notwendig ist.

Die Installation von Icinga2 ist teilweise allerdings etwas kompliziert und trotz Anleitung fehleranfällig, da an mehreren Stellen (z. B. auch beim Hinzufügen von jedem Agenten) eine manuelle Konfiguration am Master notwendig ist. Eine einfachere vergleichbare Alternative ist **Zabbix**.[3]

Im Web finden sich darüber hinaus zahlreiche Vergleichsübersichten über die Vielzahl angebotener Systeme zur Netzüberwachung.

[2] https://icinga.com/
[3] https://www.zabbix.com/

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 31 (Protokollierung und Auswertung)
- **B3S im Krankenhaus** – Kap. 7.9 (Vorfallerkennung und Überwachung)
- **ISO/IEC 27001** – A.12.2 (Schutz vor Schadsoftware), A.12.4 (Protokollierung und Überwachung)
- **BSI IT-Grundschutz-Kompendium** – OPS.1.1.4 (Schutz vor Schadprogrammen), SYS.2.1 (Allgemeiner Client)

7.4 Sicherer Netzspeicher

Kurzbeschreibung

Ein zentraler Netzspeicher ist heutzutage in jeder IT-Umgebung eine wichtige Komponente, um sie vielen Clients und Diensten bereitzustellen. Außerdem ist er ein wichtiger Bestandteil von Sicherheitsmaßnahmen. Gleichzeitig ist er ein prädestinierter Single-Point-of-Failure sowie ein besonders schützenswerter Bereich mit wertvollen Informationen aus verschiedenen Diensten, wie oft dem KIS selbst.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			
IT-Abteilung	•		
Personal/Nutzer			

Sichere Netzspeicher fallen in die Zuständigkeit der IT-Abteilung.

Umsetzung der Maßnahme

Ein zentraler Netzspeicher erleichtert generell die Handhabung von Daten und ihrer Sicherung (z. B. in den Maßnahmen 6.1 Handhabbarkeit von Arbeitsplatzrechnern und Rechnern des medizinischen Betriebs, 6.4 Automatisierte Datensicherung zur effektiven Wiederherstellung, 6.6 Benutzerfreundliche Absicherung der Endgeräte zur mobilen Visite, 7.2 Patchen zentraler Dienste mit geringer Auswirkung auf den Krankenhausbetrieb) und ist daher generell sehr empfehlenswert.

Übersicht über Dienste

Als Netzspeicher werden überwiegend zwei Dienste verwendet: Entweder **CIFS/SMB** oder **NFS**. Alle üblichen Betriebssysteme können mit beiden umgehen. In der Praxis bleibt für einen einfachen sicheren Netzspeicher jedoch nur CIFS und SMB übrig, da eine sichere geeignete Konfiguration unter NFS vergleichsweise sehr aufwendig ist. Ein sicherer Dienst umfasst **Authentifizierung** und **Autorisierung**, **Verschlüsselung** und **Integritätsschutz**.

In SMB können Verschlüsselung und Integritätsschutz einfach konfiguriert werden. Ebenso kann die Authentifizierung gemäß den Anforderungen und der existierenden Infrastruktur des jeweiligen Krankenhauses konfiguriert werden – entweder auf lokaler Ebene, über einen Domänen-Controller (AD, LDAP) oder über Kerberos. Für Krankenhäuser ist üblicherweise die Authentifizierung über den zentralen Domänen-Controller am geeignetsten, in *kleinen* Umgebungen auch über das lokale System.

```
1 [global]
2 log level = 2
3 log file = /var/log/samba/log.%m
4 debug pid = yes
5 debug uid = yes
6 syslog = yes
7
8 security = user     # domain, ads
9
10 encrypt passwords = yes
11 server signing = mandatory # "auto" für Kompatibilität
12 smb encrypt = mandatory    # "auto" für Kompatibilität
13
14
```

Abbildung 7.2: Übersicht wichtiger Sicherheitsparameter für SMB

Wichtig ist es, ein geeignetes Log-Level zu definieren und auch fehlgeschlagene Login-Versuche zu loggen, um mögliche Angriffe zu detektieren. Der Parameter `security` gibt, wie oben beschrieben, die Art der Authentifizierung an. Es ist unbedingt notwendig, Passwörter verschlüsselt auszuhandeln (`encrypted passwords`). Im Idealfall kann man über die `mandatory`-Option für `server signing` sowie `smb encryption` den Integritätsschutz und eine Verschlüsselung forcieren. Manche Clients unterstützen dazu jedoch nicht die notwendigen Protokolle. Hier kann die Option `auto` diesbezüglich das *Bestmögliche* herausholen. Es ist aber nicht unwahrscheinlich, dass gerade spezielle medizinische Geräte keine Verschlüsselung unterstützen und die Verbindung dann nicht abgesichert ist. Hier kann beispielsweise eine individuelle VPN-Verschlüsselung, wie in Maßnahme 6.8 Absicherung nicht managebarer Geräte beschrieben, Abhilfe schaffen.

Generell muss immer darauf geachtet werden, aktuellste Softwareversionen zu verwenden, sowohl beim Server als auch bei Clients. Die Überwachung des Netzspeichers muss insbesondere die **Verfügbarkeit** und Zugreifbarkeit des Dienstes und **abhängiger** Dienste (z. B. LDAP) sowie die Verfügbarkeit von ausreichend **Speicherplatz** sicherstellen.

Geeignete Architekturen

SMB bietet bereits einige Sicherheitsmechanismen, abgesehen von sicherer **Verfügbarkeit**. Diese Problematik kann jedoch ebenfalls relativ einfach durch das Aufsetzen eines identischen Dienstes auf einer anderen (eventuell virtuellen) Maschine und einer entsprechenden Fail-Over-Behandlung realisiert werden (wie in Maßnahme 7.2 Patchen zentraler Dienste mit geringer Auswirkung auf den Krankenhausbetrieb im Kontext Patching beschrieben).

Laufwerke können dennoch zentral hinter den identischen SMB-Diensten stehen. Sie sind jedoch nach der SMB-Failover-Architektur der Single-Point-of-

Failure. Um diesen abzuschwächen, muss in jedem Fall ein geeignetes **RAID** eingerichtet werden (wie in Maßnahme 6.4 Automatisierte Datensicherung zur effektiven Wiederherstellung ■ für Backup statt generellem Netzspeicher beschrieben).

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 11 (Robuste/resiliente Architektur)
- **B3S im Krankenhaus** – Kap. 7.6 (Robuste/resiliente Architektur), Kap. 7.13.7 (Sichere Authentisierung), Kap. 7.13.8 (Kryptographische Absicherung)
- **ISO/IEC 27001** – A.9.1.2 (Zugang zu Netzen und Netzwerkdiensten), A.9.2 (Benutzerzugangsverwaltung), A.9.4 (Zugangssteuerung für Systeme und Anwendungen), A.10 (Kryptographische Maßnahmen)
- **BSI IT-Grundschutz-Kompendium** – APP.3.3 (Fileserver), APP.3.4 (Samba)

7.5 Handhabbarkeit von Dienstinstanzen und Konsolidierung

Kurzbeschreibung

Virtualisierung von Ressourcen bildet heute eine der wichtigsten Grundlagen für mehrere Aspekte im Krankenhaus: (Virtuelle) Serversysteme können einfacher überwacht und gesteuert werden, Rechenleistung wird effizienter ausgenutzt, finanzielle und auch personelle Mittel werden gespart. Außerdem dient Virtualisierung als ausgezeichnete Grundlage für vielerlei Sicherheitsmaßnahmen.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			
IT-Abteilung	•		
Personal/Nutzer			

Die Handhabbarkeit von Dienstinstanzen und deren Konsolidierung fallen in die Zuständigkeit der IT-Abteilung.

Umsetzung der Maßnahme

Virtualisierung hilft generell bei der Verwaltung von IT-Ressourcen. Virtuelle Systeme lassen sich einfach und integriert **überwachen**, können in mehrerlei Hinsicht wesentlich zur **Sicherheit** beitragen und nutzen physische Ressourcen ideal aus. Lediglich die **Performanz leidet** in der Praxis etwas; in den meisten Fällen kommt es dadurch jedoch zu keinerlei spürbaren Einschränkungen.

Nützliche Sicherheitsmaßnahmen

Ein paar Maßnahmen, in denen Virtualisierung eine Rolle spielt, wurden in früheren Abschnitten bereits behandelt. Die Wichtigsten darunter sind die Maßnahmen 6.1 Handhabbarkeit von Arbeitsplatzrechnern und Rechnern des medizinischen Betriebs ■ (hier v. a. Client-Virtualisierung), 5.5 Schließen von Einfallswegen für und Eindämmung von Malware im Krankenhausnetz ■■■, 6.5 Schnittstellen und sichere mobile Datenträger im Krankenhaus ■ und 7.2 Patchen zentraler Dienste mit geringer Auswirkung auf den Krankenhausbetrieb ■.

Weitere nützliche Sicherheitsaspekte durch Virtualisierung sind Folgende:

- Dienste auf demselben physischen Host sind **voneinander getrennt**. Die Kompromittierung eines Dienstes gefährdet deshalb in der Regel nicht das gesamte System.
- Die meisten Hypervisor unterstützen **Snapshots**, sodass virtuelle Systeme zuverlässig komplett gesichert und einfach wiederhergestellt werden können (z. B. bei Fehlkonfiguration oder bei Malware-Befall). Snapshots können dann einfach in einem Backup gezielt gesichert werden. Zu beachten ist jedoch, dass nicht zu viele Snapshots zu lange aufbewahrt werden, da ansonsten ihr Verwaltungsaufwand den Nutzen übersteigen kann.
- Die **Migration** virtueller Maschinen und dadurch realisierter Dienste wird üblicherweise unmittelbar unterstützt; hilfreich ist dies bei der Anschaffung von neuen Host-Systemen oder bei Hardware-Defekten eingesetzter Hosts, der Erstellung von redundanten Systemen oder dem vielfachen Einsatz von Standard-Images (z. B. von Sicherheitsfunktionen wie einem NIDS oder einer Firewall).
- Virtuelle Systeme können über eine zentrale virtuelle **Managementanwendung** oft von jedem Client über eine Web-Oberfläche verwaltet werden – oft auch Hypervisor-übergreifend (bei *IaaS*, vgl. unten). Eine notwendige physische Präsenz am Gerät wird minimiert. Somit bietet Virtualisierung nicht nur oftmals mehr Sicherheit, sondern erhöht auch Ressourcen- und Zeiteffizienz von System-Administratoren.

Arten von Systemen und Beispiele

Virtuelle Maschinen werden über einen sogenannten **Hypervisor** realisiert. Sie erlauben ihre Konfiguration (z. B. Anzahl CPUs, RAM, Netzwerkadapter, Grafikunterstützung) und Steuerung (Starten, Anhalten, Einfrieren, Snapshot-Erstellung, Import, Export, uvm.).

Die Auswahl an Hypervisoren ist groß; **kommerzielle Systeme inklusive Support** sind ebenso wie ausgereifte Open-Source-Varianten (z. B. KVM und Xen), jedoch ohne Hersteller-Support, vielfach vorhanden. Zu beachten ist, dass nicht alle Systeme für den Einsatz im Rechenzentrum geeignet, sondern teilweise mehr für den Betrieb auf Clients ausgelegt sind (z. B. Virtualbox oder Bochs). Generell ist es auch sinnvoll, sich bei Anbietern von Spezialsoftware (z. B. KIS, LIS) im Krankenhaus hinsichtlich der Unterstützung von Hypervisor-Plattformen zu informieren.

Darauf aufbauend existieren ebenfalls weitere (sogenannte Infrastructure-as-a-Service (IaaS)) Systeme, welche nicht nur die Verwaltung mehrerer (in der Regel gleichartiger) Hypervisoren erlauben, sondern ebenfalls Speicher und (virtuelle) Netzressourcen über **mehrere Hosts** verwalten können. Anders gesagt können Ressourcen mehrerer geographisch verteilter Serverräume somit über eine zentrale Oberfläche gemanagt werden.

Sie erlauben üblicherweise auch die einfache und dynamische Erweiterung eines **Pools** virtueller Ressourcen (insbesondere Rechenressourcen und Speicher). Ein gutes Beispiel für ein vergleichsweise benutzerfreundliches und ausgereiftes, frei nutzbares IaaS-System ist **OpenNebula**.[4]

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 19 (Netz- und Systemmanagement)
- **BSI IT-Grundschutz-Kompendium** – SYS.1.5 (Virtualisierung)

[4] https://opennebula.org/

7.6 Krankenhäuser und Cloud-Dienste ■

Kurzbeschreibung

Cloud-Dienste bieten eine attraktive Lösung, um Kosten in der IT-Infrastruktur zu sparen und einen Teil der Managementaufgaben an Dienstleister abzugeben. Diese Dienste (und darunterliegende IT-Ressourcen) werden üblicherweise durch einen externen Anbieter betrieben. Zudem sind sie klassischerweise über nutzerfreundliche (Web-) Portale steuerbar. Eine sichere Nutzung von Cloud-Diensten erfordert aber die Beachtung einiger technischer und rechtlicher Aspekte. Auf diese wird in dieser Maßnahme näher eingegangen.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	•
IT-Abteilung	•		
Personal/Nutzer			

Für die technische Absicherung ist die IT-Abteilung zuständig. Dazu gehören jedoch, wie im Folgenden ausgeführt, unter Umständen auch größere Maßnahmen, die mit der Geschäftsführung abgestimmt sind oder teilweise auch genehmigt werden müssen. Eine Einbeziehung der Geschäftsführung ist daher empfohlen.

Umsetzung der Maßnahme

Cloud-Dienste stehen, sofern sie nicht als lokale Private Cloud aufgebaut werden, über das Internet zur Verfügung und laufen bei einem Cloud-Anbieter in einem geographisch entfernten Rechenzentrum. Die Verantwortlichkeiten sind üblicherweise vertraglich fix geregelt. Durch diese Beschreibung lassen sich die wichtigsten Bedrohungen für Cloud-Dienste ableiten, wie in den folgenden Abschnitten beschrieben wird.

Für Cloud-Dienste und IT-Ressourcen gelten generell mindestens dieselben Sicherheitskriterien wie für Dienste und Systeme im Krankenhaus. Bei der Anmietung von Cloud-Systemen muss entsprechend darauf geachtet werden, dass der jeweilige Cloud-Anbieter geeignete Maßnahmen durchführt, was beispielsweise durch eine gültige Zertifizierung nach ISO/IEC 27001 nachgewiesen werden kann.

Ebenfalls ist zu beachten, dass Cloud-Dienste genauso wie krankenhausinterne Dienste und Systeme dokumentiert werden müssen. Grundlegende Aspekte für ein Vorgehen der Identifikation und Dokumentation von Prozessen und damit verbundenen Systemen und Diensten wurde in Maßnahme 3.5 Identifikation kritischer Systeme im Krankenhaus ■ beschrieben. Kriterien zur Einstufung von Cloud-Systemen (z. B. Welchen Rahmen der Verfügbarkeit sichert ein Cloud-Anbieter zu? Gibt es geplante Dienstausfälle, z. B. durch ein vom Cloud-Anbieter definiertes Wartungsfenster?) fließen dabei direkt in die Auswahl eines geeigneten Cloud-Anbieters ein.

Sichere Daten und Prozesse

Daten, die auf Cloud-Diensten verarbeitet werden, verlassen das krankenhausinterne Netz und sind damit unter Umständen einfacher abgreifbar, manipulierbar und können auch verloren gehen. Insofern muss darauf geachtet werden, dass die **Kommunikation** zwischen Krankenhaus und Cloud-Dienst sicher ist. Dazu gehört eine Verschlüsselung der Daten zum einen auf Netzebene, z. B. ein VPN zwischen Krankenhaus und Cloud-Anbieter, zum anderen zwischen Diensten, d. h. klassischerweise mit TLS. Sicher konfiguriert, bieten VPNs und TLS ebenfalls eine Integritätssicherung, d. h. Überprüfung, dass die Daten nicht beim Transport beschädigt oder manipuliert wurden. Eine Übersicht sicherer TLS-Verbindungen bietet beispielsweise Mozilla an.[5] Auch muss hier auf eine entsprechende Authentifizierung an den Dienst-Schnittstellen geachtet werden. Auf diese Weise wird verhindert, dass nicht-authentifizierte und somit nicht-autorisierte Nutzer oder Anwendungen (z. B. Tools für Penetrationstests) mit den Cloud-Diensten kommunizieren.

Ein anderer wichtiger Aspekt ist – wie auch in krankenhausinternen Rechenzentren –, dass sowohl die vom Cloud-Anbieter eingesetzte Software als auch die vom Kunden auf der Cloud installierte **Software** stets **aktuell** ist. Auf diese Weise werden angreifbare Software-Schwachstellen geschlossen (vgl. auch Maßnahme 7.2 Patchen zentraler Dienste mit geringer Auswirkung auf den Krankenhausbetrieb ■) und können nicht mehr von Malware oder Angreifern ausgenutzt werden. Hier gelten allgemein die gleichen Kriterien wie auch für Dienste, die im Krankenhaus selbst betrieben werden – nur dass die Verantwortung nun der Cloud-Anbieter übernehmen und dieselben Maßnahmen für die von ihm angebotene IT-Infrastruktur ergreifen muss.

Teilweise bieten Cloud-Anbieter auch einen **Back-Up**-Dienst für von ihm gemietete (virtuelle) Server und Dienste an. Diese Standard-Maßnahme (vgl. Kriterien auch in Maßnahme 6.4) ist auch für Cloud-Dienste und Daten in der Cloud obligatorisch. Es muss jedoch darauf geachtet werden, ob vom Cloud-Anbieter vorhandene Lösungen ebenfalls ein hohes Maß an Sicherheit (mindestens eine geeignete Verschlüsselung und Integritätssicherung) bieten und datenschutzkonform sind.

Ein weiterer Aspekt, der insbesondere im Cloud-Computing zu beachten ist, stellen Schwachstellen der **Hardware-Plattform** dar. Dazu zählen insbesondere Seitenkanalangriffe wie SPECTRE, MELTDOWN,[6] und

[5] https://wiki.mozilla.org/Security/Server_Side_TLS
[6] https://meltdownattack.com/

andere.[7] Eine pragmatische Maßnahme zur grundlegenden Absicherung ist die Vermeidung der Nutzung bzw. Anmietung virtueller Maschinen, die unter Umständen mit virtuellen Maschinen anderer unbekannter Nutzer dieselbe Hardware-Plattform teilen. Stattdessen sollten dedizierte physische Plattformen bzw. Systeme angemietet werden. Viele Hosting- und Cloud-Anbieter haben Entsprechendes in ihrem Portfolio.

Verfügbarkeit der Dienste

Einer der wichtigsten Vorteile von Clouds, der einfache Zugriff über das Internet, bringt gleichzeitig einen offensichtlichen Nachteil mit sich: Die Abhängigkeit von öffentlichen Netzinfrastrukturen sowie der eigenen und der **Cloud-Anbieter-Netzanbindung**. Ein professioneller Cloud-Anbieter ist dabei üblicherweise mehrfach an das Internet angebunden und auch das Krankenhaus sollte, wie in Maßnahme 5.1 Absicherung des Netzzugangs und generelle Netz-Zonen empfohlen, redundante Netzanbindung haben.

Durch die redundante Netzanbindung auf beiden Seiten ist die Sicherstellung der Verfügbarkeit des Netzes zwar deutlich erhöht, jedoch bei weitem kein Garant dafür, dass diese nicht dennoch ausfallen kann. Entsprechend muss ein Krankenhaus, das wichtige Dienste in die Cloud ausgelagert hat, dennoch ein Notfall-Konzept für den Fall der Nicht-Verfügbarkeit von Cloud-Diensten bereithalten. Schließlich können nicht nur Netzprobleme zum Ausfall von Cloud-Diensten führen, sondern insbesondere auch Konfigurations- oder Implementierungsfehler genauso wie die Kompromittierung eines Dienstes. Eine Möglichkeit zur weiteren Absicherung bietet hier einerseits die Anmietung **redundanter Cloud-Ressourcen** bei einem anderen Anbieter aus einer anderen Region (z. B. bei einem regionalem Stromausfall) und andererseits die **Vorhaltung** ausgelagerter Dienste auf der krankenhausinternen IT-Infrastruktur.

Sicherer Management-Zugang

Des Weiteren sind Cloud-Dienste über netzbasierte **Managementschnittstellen** überwachbar und konfigurierbar. Auch diese sind nicht selten über das Internet erreichbar und bieten eine mögliche Angriffsoberfläche. In der Regel ist davon auszugehen, dass eine Kompromittierung der Management-Schnittstelle einer Kompromittierung aller dadurch konfigurierbarer Systeme und Dienste gleichkommt. Entsprechend muss auch hier darauf geachtet werden,

- dass der Zugriff auf die Managementoberfläche über eine verschlüsselte Kommunikation stattfindet (z. B. TLS),
- dass der Cloud-Anbieter dazu gültige Zertifikate verwendet,
- dass Zugangsdaten zur Management-Schnittstelle sicher gespeichert werden (z. B. in einem Passwort-Safe),
- dass die Zugangsdaten nur ausgewählten Mitarbeitern zugänglich sind.

Rechtliche Anforderungen

Beim Einsatz von Cloud Computing im Krankenhaus sind diverse datenschutzrechtliche Aspekte zu berücksichtigen. Grundsätzlich gilt, dass die Verantwortung für die Daten beim Nutzer eines Cloud-Dienstes verbleibt – in unserem Fall das Krankenhaus. Daher muss die IT-Abteilung des Krankenhauses sicherstellen, dass der Cloud-Anbieter die entsprechenden Vorschriften und Rechtsgrundlagen einhalten muss. Dabei ist der Cloud-Anbieter als Dienstleister anzusehen und daher gelten für dessen Einsatz die Vorschriften, wie sie in der Maßnahme 9.5 Externe Dienstleister für Krankenhäuser aufgeführt sind.

Insbesondere ist zu beachten, dass bei der Speicherung von Gesundheitsdaten in einer Cloud die Cloud-Anbieter keinen unbefugten Zugriff auf diese Daten erhalten. Ein weiterer wichtiger Aspekt ist der **Speicherort** bei Cloud Computing: Je nachdem, wo der Cloud-Anbieter seine Systeme verwaltet, sind besondere Vorschriften bei der Datenübertragung zu beachten (z. B. für externe Dienstleister außerhalb der EU). Es wird empfohlen, Cloud-Anbieter in der EU bzw. im nationalen Raum zu bevorzugen, da diese der gleichen Datenschutzgrundverordnung (DSGVO) unterliegen.[8]

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 17 (Externe Dienstleister)
- **BSI IT-Grundschutz-Kompendium** – OPS.2.2 (Cloud-Nutzung)
- **BSI Leitfaden** – Sichere Nutzung von Cloud-Diensten, August 2016

[7] https://en.wikipedia.org/wiki/Transient_execution_CPU_vulnerability

[8] https://www.datenschutz-bayern.de/tbs/tb28/k14.html#14.2

Kapitel 8

Gebäudesicherheit und physischer Schutz

Es gilt auch, Maßnahmen der Gebäudesicherheit und für einen physischen Schutz im Krankenhaus zu berücksichtigen. Die beschriebenen Maßnahmen umfassen dabei

- die Bildung von physischen Zonen in einem Krankenhaus
- sowie Besonderheiten bei der Absicherung nicht-öffentlicher Bereiche ebenso wie Besonderheiten bei der Absicherung öffentlicher Bereiche.

Diese Maßnahmen richten sich vor allem an das Gebäude-Management bzw. die Haustechnik, jedoch durchaus mit dem Potenzial der Unterstützung durch die IT-Abteilung sowie die Geschäftsführung.

8.1 Zonenkonzepte und ihre Realisierung im Krankenhaus

Kurzbeschreibung

Ein Krankenhaus wird von vielen fremden Personen frequentiert. Umso wichtiger ist die Festlegung von Sicherheitszonen: Wer ist befugt, sich wo im Gebäude aufzuhalten? In dieser Maßnahme werden eine Anleitung zur Erstellung eines Zonenkonzepts sowie die daraus resultierenden Folgemaßnahmen erläutert. Mit der Umsetzung dieses Konzepts soll der Zutritt Unbefugter in Bereiche mit schutzbedürftigem Material und ebensolchen Daten verhindert werden.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung	•		
IT-Abteilung	•		
Haustechnik	•		
Personal/Nutzer			•

Die Planung zur Einteilung des Krankenhauses in verschiedene Sicherheitszonen sollte durch die IT-Abteilung (bzw. den Sicherheitsbeauftragten) und in Absprache mit der Geschäftsführung erfolgen, da dadurch in der Regel weitere Maßnahmen impliziert werden. Das Personal muss über eine geeignete Handhabung instruiert werden.

Umsetzung der Maßnahme

In einem Krankenhaus gibt es eine Vielzahl von Abteilungen und Bereichen. Aus Sicht der IT-Sicherheit ist vor allem eine **Klassifizierung** nach in den Bereichen vorzufindenden (Netz-)Zugängen, **Geräten** und verarbeiteten **Informationen** notwendig.

Gefahrenübersicht

Die Möglichkeit des tatsächlichen Zutritts erlaubt unbefugten Personen eine Vielzahl potenzieller beabsichtigter oder versehentlicher Schadensauswirkungen. Dazu zählen beispielsweise:

- **Diebstahl** von Informationen, Dokumenten, Geräten, Instrumenten, usw.
- **Beschädigung** (z. B. Brände, Verschmutzung oder auch nur Fehlalarme) von Einrichtungen, Inventar, Gerätschaften und Dokumenten (z. B. Wassereinleiten in Serverraum über ungesicherte Fenster)
- **Zugriff** auf und **Manipulation** von **IT-Systemen** (nicht-gesperrte Rechner, Dateien, geöffnete Dokumente, USB-Schnittstellen und Einstecken von Wechseldatenträgern, usw.) und ihre Nutzung als *Sprungbrett* ins interne Netz
- **Zugriff** auf und **Manipulation** von **Netzen** (geschaltete Netzdosen zu Subnetzen, WLAN-Reichweite, Verkabelung, Access-Points, Router, Switches, usw.)
- **Manipulation** von **Zugängen**, Entriegelung bzw. Offenhalten von Türen und Fenstern

Technische Maßnahmen (Absicherung von Zugängen, Geräten und Dokumenten) in Kombination mit geeigneten Richtlinien für das Personal (eine Vorlage ist in Anhang A.4) können viele dieser Gefahren verhindern.

Definition von Zonen

Einerseits ist jedes Krankenhaus individuell aufgebaut, andererseits gibt es Gemeinsamkeiten, welche überall gelten. Ein möglicher Vorschlag ist in der an diese Maßnahme angehängten Abbildung zusammengefasst. Die Unterteilung erfolgt hier in **vier Zonen**.

Zone 0 umfasst alle *öffentlichen Bereiche* eines Krankenhauses, d. h. den Außenbereich sowie alle Bereiche, in denen sich jedermann aufhalten darf. Im Krankenhaus sind das beispielsweise notwendigerweise der Eingangs- und Informationsbereich, das öffentliche WC, der Kiosk und auch die Patientenaufnahme.

Zone 1 entspricht dem kontrollierten Innenbereich, in dem ein **bedingter** Aufenthalt auch unbekannter Personen möglich ist. Das Aufenthaltsrecht hier kann von gewissen Uhrzeiten und Situationen (z. B. Normalbetrieb vs. Notfälle) abhängig sein. Das Personal sollte aufmerksam sein. Im Krankenhaus können dazu die Stationen und gewisse Behandlungsbereiche (z. B. Warteräume und Gänge bei Röntgen, MRT und anderen Behandlungsräumen) gezählt werden.

Zone 2 umfasst den internen Bereich, welcher nur für Personal oder berechtigte Personen zugänglich ist. Das umfasst im Krankenhaus klassischerweise Räumlichkeiten der Verwaltung, Koordinierungsbereiche für den medizinischen Betrieb (z. B. der Notaufnahme) und der Triage.

Zone 3 umfasst den eingeschränkten internen Bereich, welcher nur für ausgewählte Mitarbeiter zugänglich ist. Das betrifft die Räumlichkeiten der Technik und Versorgung oder auch das Labor.

Generell sollte darauf geachtet werden, dass Übergänge von einer **Zone** nur in Zonen der gleichen, nächst höheren oder nächst niedrigeren Einstufung erfolgen kann. So sollte es etwa keinen Zugang von einer Zone 0 (z. B. Außenbereich) zu einem Bereich in Zone 3 (z. B. Serverräume) geben. Auch sollten Bereiche der Zonen 2 und Zonen 3 markiert werden, beispielsweise durch Hinweisschilder („Zutritt nur für Personal“, o. Ä.).

Die Definition von Zonen und Einteilung der Räumlichkeiten kann an die jeweilige Situation in einem Krankenhaus **angepasst** werden.

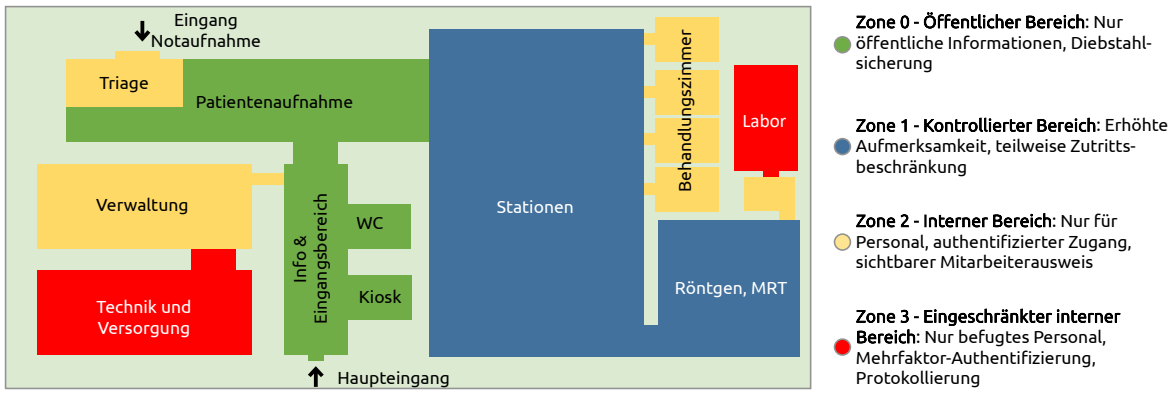


Abbildung 8.1: Beispielhafte Zonenunterteilung im Krankenhaus

Maßnahmen zur Absicherung

Je nach Zone müssen auch unterschiedliche technische Maßnahmen zur Absicherung von Räumen, Geräten und Dokumenten umgesetzt werden. Die Maßnahmen zielen vor allem auch darauf ab, den Zugang zu höheren Zonen zu unterbinden.

In **Zone 0** muss der Zutritt fremder Personen eingeplant werden. Zugänge wie Türen und Fenster sollten gängigen Sicherheitsstandards folgen. Im Normalfall wird der Zutritt jedoch – vor allem innerhalb eines Krankenhauses – jedem gewährt. Da in diesem Bereich Diebstahl und Beschädigungen am wahrscheinlichsten sind, müssen Systeme (z. B. Informations- oder Kiosk-Systeme) entsprechend immobil angebracht sein. Auch dürfen auf ihnen keine internen Daten abgelegt sein und sie müssen in besonders getrennten Netzbereichen liegen. In Zone 0 dürfen lediglich Dokumente und Systeme bereitgestellt werden (als Dokumente oder auf Speichermedien von Systemen selbst), welche öffentlich einsehbare Informationen bieten. Mehr Details zur Absicherung der Zone 0 sind in Maßnahme 8.3 Physischer Schutz von Geräten und Informationen im öffentlichen Raum zu finden.

In **Zone 1** gelten dieselben technischen Maßnahmen wie in Zone 0. Hinsichtlich der Zugänge können hier jedoch einseitig verschließbare Türen (eventuell auch mit Zeitschalter) eingesetzt werden, um zu bestimmten Uhrzeiten oder in bestimmten Situationen den Zugang zu beschränken. In diesem Bereich sollten auch bereits Hinweisschilder zu Zutrittsrichtlinien (z. B. „Für Unbefugte nicht mehr nach 22 Uhr“) sichtbar bereitgestellt werden. Mitarbeiter müssen dahingehend geschult werden, dass sie (je nach Situation) augenscheinlich unberechtigte oder *unpassend* scheinende Personen, die sich innerhalb dieses Bereichs befinden, ansprechen. Mitarbeiter sollten gut sichtbar Mitarbeiterausweise tragen. Systeme müssen ähnlich wie in Zone 0 abgesichert werden, wobei teilweise schützenswerte Informationen (z. B. Patientenakten) notwendig sind. Der Zugriff muss durch entsprechende Aufmerksamkeit des Personals, durch Bildschirmsperren, Geräteverschlüsselung u. Ä. gesichert werden.

Bereiche in **Zone 2** müssen vor allem vor unberechtigtem Zutritt geschützt werden. In erster Linie wird das durch gesicherte Zugänge und widerstandsfähige Türen und Fenster realisiert. Der Zugang erfolgt nur nach Authentifizierung. Im Krankenhausbetrieb sind programmierbare Token dafür geeignet, da sie (z. B. gegenüber PIN oder Passwort) individualisiert und zeitsparend sind und generell protokolliert werden können. Türen müssen zudem selbstschließend sein. Unberechtige Personen sind ab dieser Zone zu begleiten.

In **Zone 3** müssen Türen und Fenster entsprechende Widerstandsfähigkeit aufweisen. Zugänge müssen protokolliert werden (z. B. automatisch mit Token-basierter Authentifizierung). Ein zusätzlicher Authentifizierungs-Faktor ist zudem ratsam (z. B. PIN-Code oder Fingerabdrucksensor), um beispielsweise den Zugang über gestohlene oder gefundene Tokens Dritter zu verhindern. Ansonsten gelten generell Richtlinien wie in Zone 2 und 1 – unbekannte Personen müssen angesprochen werden und zunächst unberechtigte Personen (z. B. Techniker) sollten begleitet werden. Mehr Details am Beispiel eines Serverraums ist in Maßnahme 7.1 Sichere Rechenzentren und Serverräume zu finden.

Generell sollten **Fluchtwege** nur von höheren Zonen in niedrigere Zonen erfolgen und Fluchttüren nur vonseiten höherer Zonen aus zu öffnen sein.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 10 (Physische Sicherheit)
- **B3S im Krankenhaus** – Kap. 7.7 (Physische Sicherheit)
- **ISO/IEC 27001** – A.11.1 (Sicherheitsbereiche), A.11.2 (Geräte und Betriebsmittel)
- **BSI IT-Grundschutz-Kompendium** – INF.1 (Allgemeines Gebäude)
- **DIN EN 1627** – Prüfnorm für Fenster, Türen, Vorhangfassaden, Gitterelemente, Abschlüsse
- **DIN EN 50600**

8.2 Managebare Zutrittskontrolle zu nicht-öffentlichen Bereichen

Kurzbeschreibung

Zutrittskontrolle ist die grundlegendste (in der Regel technische) Maßnahme der physischen Sicherheit. Durchgänge zwischen den Zonen müssen praktisch immer abgesichert werden, bei höheren Zonen mit mehr Anforderungen beispielsweise durch eine Protokollierung des Zutritts. In dieser Maßnahme werden verwaltbare und nutzerfreundliche Lösungen aufgezeigt.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung	•	•	
IT-Abteilung	•		
Haustechnik	•		
Personal/Nutzer			

Im Falle eines Austauschs des Zutrittskontrollsystems eines Krankenhauses entstehen unmittelbar finanzielle Mehrkosten für die Technik. Die Geschäftsführung muss daher in den Prozess integriert sein, ebenso auch die Haustechnik. Die IT-Abteilung muss unter Umständen die Technik mitbetreiben.

Umsetzung der Maßnahme

Bei der Auswahl einer geeigneten Lösung zur Zutrittssicherung sind sowohl Aspekte aus dem Bereich Sicherheit als auch hinsichtlich der Nutzerfreundlichkeit zu beachten. Für eine **sichere Lösung** ist beispielsweise relevant,

- dass der **Diebstahl oder Verlust** eines Schlüssels handhabbar sein muss,
- dass Schlüssel **nicht unbegrenzt** gültig sein dürfen,
- dass Zugänge, wenn nötig, **selbstschließend** sind,
- dass Zutrittsrechte einfach **konfigurierbar** sein müssen,
- dass eine **Protokollierung** inhärent unterstützt wird und
- dass auch bei **Stromausfall** Zutritt für Berechtigte möglich ist.

Gleichzeitig müssen Lösungen **benutzerfreundlich** sein, damit Richtlinien, wie **stets geschlossene Türen**, nicht von Nutzern umgangen werden. Dazu zählt unter anderem,

- dass eine berechtigte Türentriegelung **schnell** gehen muss,
- dass es **einen Schlüssel** für das gesamte Haus geben muss (platz- und zeitsparend),
- aber auch, dass der Schließmechanismus **hygienische Verhältnisse** fördert.

Eine Lösung für das ganze Haus

Eine einfach managebare Lösung zur Zutrittssicherung ist praktisch immer **elektronisch**. Altbewährte Schlüssel erfüllen (mit Ausnahme eines Stromausfalls) praktisch keine der Anforderungen. Eine oftmals gute Lösung ist ein im Haus einheitliches und **zentralisiertes** System. Jeder Mitarbeiter bekommt einen eigenen **Transponder** zur Authentifizierung. Die Zutrittsberechtigung für jeden Transponder kann dann in der Regel individuell für jeden Zugang konfiguriert werden. Derartige Systeme haben auch den Vorteil, dass sie teilweise eine **Protokollierung** unterstützen und damit den Zutritt (wer, wann) auch rückwirkend nachvollziehbar machen.

Dabei sollten Lösungen bevorzugt werden, bei denen der Transponder nach einem gewissen Zeitraum vom Nutzer reaktiviert werden muss. So kann der unbefugte Einsatz bei Verlust des Transponders und das Auffinden und der Gebrauch durch einen Patienten erschwert werden. Im Falle eines Diebstahls oder Verlusts haben Transponder zudem den Vorteil, dass sie zentral deaktiviert werden können, ohne großen finanziellen Aufwand zu verursachen. Auch haben Transponder im Gegensatz zu Fingerabdrucksensoren oder Pin-Code-Schlössern einen hygienischen Vorteil, da sie oft sogar kontaktlos arbeiten.

Elektronische Schließanlagen für Transponder arbeiten üblicherweise mit einer Batterie, welche mehrere Jahre lang halten kann. Stromausfälle sind somit zwar handhabbar, dennoch sollten unterschiedliche Lösungen dahingehend verglichen werden, wie lange eine Batterie hält. Schließanlagen mit optischer Warnung bei schwacher Batterie (z. B. Leuchtdiode) zeigen an, wann ein Batteriewechsel notwendig ist, bevor die Schließanlage ausfällt.

Eine automatische Schließung von Zugängen ist insbesondere bei Zonenübergängen wie auch zu Behandlungs- und Arztzimmern notwendig (vgl. Maßnahme 8.1 Zonenkonzepte und ihre Realisierung im Krankenhaus). Dazu können im einfachsten Fall simple und günstige Türschließer verbaut werden. Ausgefeiltere programmierbare Anlagen, welche beispielsweise zeitgesteuert schließen (z. B. für die Stationen), sind aufwendiger und üblicherweise nicht unbedingt notwendig.

Bewährt haben sich Lösungen, bei denen die Transponder nicht nur für die Schließung, sondern zum Beispiel zum Bezahlen an Kaffeeautomaten oder in der

Kantine oder an Etagendruckern verwendet werden können; diese weiteren Nutzungsmöglichkeiten reduzieren die Wahrscheinlichkeit, dass Transponder liegengelassen oder unerlaubt verliehen werden.

Zweifaktor-Anmeldung

In besonders gesicherten Bereichen, in die nur bestimmte Mitarbeiter gehen dürfen (z. B. Techniker in Serverraum, MTLAs in Labor), sollte eine Zweifaktorauthentifizierung installiert werden. Dazu kann beispielsweise ein zweiter Schließmechanismus oder eine Schleuse mit einer separaten Transponder-Anlage eingerichtet werden. Geeignet sind hier vor allem auch wenig aufwendige Verfahren, wie PINs oder biometrische Methoden, sodass Personen nicht zusätzliche Schlüssel bzw. Tokens mit sich herumtragen müssen.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 10 (Physische Sicherheit)
- **B3S im Krankenhaus** – Kap. 5.2.2.4 (Versorgungstechnik), Kap. 7.7 (Physische Sicherheit)
- **ISO/IEC 27001** – A.11.1 (Sicherheitsbereiche), A.11.2 (Geräte und Betriebsmittel)
- **BSI IT-Grundschutz-Kompendium** – INF.1 (Allgemeines Gebäude)

8.3 Physischer Schutz von Geräten und Informationen im öffentlichen Raum ■■

Kurzbeschreibung

Wie bereits in Maßnahme 8.1 Zonenkonzepte und ihre Realisierung im Krankenhaus ■■ beschrieben, sind öffentliche Räume im Krankenhaus immer vorhanden. Eine Absicherung fällt entsprechend schwer, da fremde Personen sich sehr häufig in diesen Bereichen aufhalten. Besondere Herausforderungen umfassen hier Diebstahl, Beschädigung und die Einsicht in besonders schützenswerte Informationen.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung			
IT-Abteilung	•		
Haustechnik	•		
Personal/Nutzer			•

Für die Umsetzung der Maßnahme sind vor allem die Haustechnik und die IT-Abteilung zuständig. Das Personal muss jedoch hinsichtlich möglicher Gefahren sensibilisiert werden und in entsprechenden geeigneten Handlungsverfahren für den Alltag geschult werden.

Umsetzung der Maßnahme

Sicherheit von Daten und eine zuverlässige **Funktionsfähigkeit der IT** sind im Krankenhaus in diesem Zusammenhang die Kernziele zum Schutz von Patienten. Andere Problematiken, wie der reine Verlust von Hardware bei Diebstahl oder Beschädigung, sind im Vergleich noch eher zu kompensieren.

Denkbare und inzwischen nicht selten anzutreffende IT-Systeme sind zum Beispiel **Kiosk-** oder **Informationssysteme**, Netzkomponenten wie **Access-Points** und teilweise auch versteckte **Switches**. Jedoch zählen dazu auch übliche **Client-Rechner**, beispielsweise beim Krankenhaus-Empfang.

Befestigung von Equipment und Überwachung

Ein wichtiger Teil der Absicherung von Daten und Geräten ist die physische Befestigung von Geräten. Die Möglichkeit zur schnellen Entwendung eines Geräts soll damit verhindert werden. Das geschieht im besten Fall durch professionelle **Montagesets**, welche direkt für das entsprechende Gerät verfügbar sind. Oftmals besteht diese Möglichkeit jedoch nicht, weshalb Alternativen notwendig sind. Als günstige Möglichkeit zur Befestigung von Geräten jeder Art bietet sich ein **Kensington-Schloss** an, wie es auch im Einzelhandel oft eingesetzt wird. Viele Monitore, Notebooks oder Desktop-PCs haben eine spezielle Öffnung, die genau diesem Zweck dient.

Ein weiterer wichtiger Punkt ist die Überwachung entsprechender Geräte im öffentlichen Raum. Das kann einerseits durch **aufmerksames Personal** geschehen, das unter Umständen derartige Geräte auch im Alltag immer im Blick hat (z. B. das Personal am Krankenhaus-Empfang), aber auch durch alle anderen Mitarbeiter, die sich öfter in diesen Bereichen aufhalten (z. B. Reinigungspersonal). Insbesondere auf den Stationen müssen auch Pflegepersonal und Ärzteschaft dazu beitragen und Auffälligkeiten melden (z. B. beschädigte Geräte, Zugriff durch Unbefugte). Eine weitere denkbare Möglichkeit – einerseits zur Abschreckung, andererseits zur Sicherung – ist auch im öffentlichen Raum der Einsatz von **Videoüberwachung**. Hier muss jedoch insbesondere auf die Rechte von Mitarbeitern und Patienten geachtet werden, weshalb der Einsatz von Videoüberwachung gut begründet werden muss. Weitere Hinweise aus DSGVO-Sicht sind auch in einem Leitfaden des *European Data Protection Board* zusammengefasst,[1] unter anderem auch mit einer Vorlage zu datenschutzkonformen Hinweisschildern auf die Videoüberwachung.

Trennung von Daten

Eine sichere Befestigung von Geräten kostet Diebe und Vandalen üblicherweise nur wertvolle Zeit, aber verhindert den Diebstahl und eine Sachbeschädigung nicht zuverlässig. Daher muss darauf geachtet werden, dass **keine vertraulichen Daten** durch Diebstahl entwendet werden oder durch Sachbeschädigung verloren gehen können. Entsprechend werden bestenfalls derartige Daten gar nicht erst auf diesen Geräten gespeichert. Dazu gehören aber auch **Passwörter** (z. B. für genutzte Dienste wie SMB/NFS, WLAN, usw.) oder andere Authentifizierungsdaten wie Public-Key-Infrastrukture (PKI)-**Zertifikate** und **Schlüssel**. Soweit möglich, muss darauf geachtet werden, dass sich nur die Geräte im öffentlichen Raum befinden, die dort auch wirklich notwendig sind. Beispielsweise müssen in den meisten Fällen nicht die eigentlichen PCs und Rechner vor Ort sein, sondern lediglich Bildschirme und eingeschränkte Eingabemöglichkeiten. Es muss darauf geachtet werden, dass keine **ungewollten Eingabemöglichkeiten** vorhanden sind, wie versteckte Tasten, Touch-Screens oder nutzbare USB-Schnittstellen, an denen eine Maus oder Tastatur angeschlossen werden kann.

Sofern möglich, ist es auch hier sinnvoll, **Thin-Client-Lösungen** einzusetzen und Daten sowie die gesamte Verarbeitung im Hintergrund auf Serversystemen zu belassen. Durch einen Diebstahl geht so ledig-

[1] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf

lich der Wert des jeweiligen Gerätes verloren und diese Systeme lassen sich relativ schnell ersetzen, da nur der Zugriff zum Host konfiguriert werden muss. Eine Herausforderung besteht hier jedoch darin, dass Geräte im öffentlichen Raum auf keinen Fall mit dem **internen Krankenhaus-Netz** verbunden sind (vgl. folgender Abschnitt), hier helfen jedoch teilweise Security-Gateways und Tunnel (z. B. SSH oder VPN), um Netze klarer zu trennen.

Unterbindung von Netz-Zugriff

Neben der Gefahr, dass Daten mit Geräten entwendet oder vernichtet werden, besteht auch die Gefahr, dass Geräte im öffentlichen Raum einem Angreifer **Zugang zum Krankenhaus-Netz** geben. Offene Ethernet-Ports an Netzgeräten oder die Möglichkeit zum Ausführen bzw. Öffnen anderer Anwendungen auf Informationsgeräten können Angreifern unter Umständen Zugriff auf das gesamte Netz geben. Findet ein Angreifer z. B. eine Möglichkeit, das eigentliche Programm abstürzen zu lassen, liegt vor ihm oft ein frei zugänglicher Zugang zu einem handelsüblichen Betriebssystem und seinen Mitteln.

Deshalb müssen **Ethernet-Ports** an Netzgeräten, insbesondere wohl Access-Points und teilweise auch Switches, deaktiviert werden. Netzdosen, die im öffentlichen Raum zugänglich sind, müssen ebenso wie alle Geräte in ein extra **abgeschottetes Netz** (siehe auch Maßnahme 5.2 Logische Aufteilung des Krankenhausnetzes). Alternativ können nicht-managebare Ports auch physisch blockiert werden, z. B. durch schwer entfernbare Verschlüsse und Stöpsel aus Gummi.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 10 (Physische Sicherheit)
- **B3S im Krankenhaus** – Kap. 7.7 (Physische Sicherheit)
- **ISO/IEC 27001** – A.11.1 (Sicherheitsbereiche), A.11.2 (Geräte und Betriebsmittel)
- **BSI IT-Grundschutz-Kompendium** – INF.1 (Allgemeines Gebäude)

Kapitel 9

Datenschutz und rechtliche Konformität

Im Krankenhaus werden viele Daten über Patienten, Mitarbeiter und Besucher erfasst. Bei der Verarbeitung dieser Daten, insbesondere Gesundheitsdaten von Patienten, müssen datenschutzrechtliche Anforderungen und Bedingungen anderer Rechtsnormen berücksichtigt werden. Dieses Kapitel umfasst Maßnahmen mit Informationen über (datenschutz)rechtliche Aspekte, die bei der Verarbeitung von Daten im Krankenhaus relevant sind. Dazu werden folgende Themen näher betrachtet:

- Datenkategorisierung, Datenverarbeitung und das Datenschutzmanagement
- Anforderungen und Maßnahmen für eine datenschutzkonforme Telearbeit im Krankenhaus
- Umsetzung von Bring Your Own Device (BYOD) im Krankenhaus
- Maßnahmen für einen datenschutzkonformen Informationsaustausch
- Einsatz von externen Dienstleistern für die Datenverarbeitung im Krankenhaus

Da es in diesem Kapitel hauptsächlich um die Datenverarbeitung in ausgewählten Fällen geht, sind die Maßnahmen größtenteils für die IT-Abteilung des Krankenhauses relevant, da diese meistens für die Umsetzung verantwortlich ist. Für den Gesamterfolg und einen gesetzeskonformen Umgang mit personenbezogenen Daten ist die entsprechende Beteiligung des Krankenhauspersonals und der Geschäftsleitung unabdingbar.

9.1 Grundlegendes zum Datenschutz

Kurzbeschreibung

Kurzbeschreibung

Diese Maßnahme gibt einen Überblick über grundlegende Aspekte, die bzgl. des Datenschutzes in Krankenhäusern relevant sind. Dazu zählen sowohl die Datenkategorisierung und die Datenverarbeitung als auch das Datenschutzmanagement und die entsprechenden Verantwortlichkeiten. Diese Maßnahme orientiert sich am Leitfaden „Anforderungen an das Datenschutzmanagement in bayerischen öffentlichen und privaten Krankenhäusern" des Bayerischen Landesbeauftragten für den Datenschutz.[a]

[a] https://www.datenschutz-bayern.de/presse/20180308_Leitfaden_Datenschutzmanagement_Krankenhaus.html

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung	•		
IT-Abteilung			•
Personal/Nutzer	•		

Die Hauptverantwortung für die Einhaltung der Datenschutz-Grundverordnung (DSGVO) trägt der Geschäftsführer des Krankenhauses. Damit verbundene Aufgaben können auch delegiert werden. Ein Team, das zuständig für das Datenschutzmanagement ist, sollte zusammengestellt werden und aus Vertretern der jeweiligen Fachabteilungen bestehen. Dazu zählt auch die IT-Abteilung. Grundsätzlich sollte dem **gesamten Krankenhauspersonal** bewusst sein, dass jeder Einzelne beim erfolgreichen Datenschutz gefragt und an der Umsetzung beteiligt ist.

Umsetzung der Maßnahme

Das Ziel dieser Maßnahme ist, sich einen Überblick zu verschaffen über die **Datenkategorien**, die im Krankenhaus gegenwärtig sind, wie diese **verarbeitet** werden und was dabei zu berücksichtigen ist. Außerdem ist es wichtig, die Verantwortlichkeiten und den Gesamtumfang eines **Datenschutzmanagements** festzulegen und kennenzulernen.

Datenkategorisierung

Für den richtigen Umgang mit Daten im Krankenhaus ist es wichtig, festzustellen, mit welcher Art von Daten hauptsächlich im Krankenhaus gearbeitet wird. Daher muss zuerst eine Kategorisierung erfolgen, damit die entsprechenden rechtlichen Vorschriften identifiziert und eingehalten werden können.

Der Datenschutz bezieht sich im Kern auf personenbezogene Daten. Diese werden in Art. 4 DSGVO definiert und betreffen zusammengefasst alle Informationen, die eine Person identifizierbar machen. Dazu gehören zum Beispiel der Name, Kontaktdaten und Adressen der Patienten. Des Weiteren gibt es auch Daten, die den besonderen Kategorien von personenbezogenen Daten (Art. 4 DSGVO) zugeordnet werden und als besonders schützenswert gelten. Dazu zählen Daten aus denen (a) die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, (b) Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person, (c) genetische Daten, (d) biometrische Daten und (e) Gesundheitsdaten.

Da im Krankenhaus hauptsächlich mit **Patientendaten**, also Gesundheitsdaten, gearbeitet wird, gelten besondere Vorgaben bei der Verarbeitung ebendieser. Außerdem fallen sie zusätzlich unter das Arztgeheimnis und damit unter eine strenge Verschwiegenheitspflicht.

Für die Verarbeitung von Daten muss gemäß Art. 30 DSGVO ein Verarbeitungsverzeichnis angelegt werden. Dabei muss auch die Datenkategorie angegeben werden.

Datenverarbeitung

Bei personenbezogenen Daten gilt grundsätzlich Art. 6 DSGVO und verschärft sich weiter in Art. 9 für besondere Kategorien persönlicher Daten. Da es sich im Krankenhaus bei Patientendaten um personenbezogene Daten besonderer Kategorien handelt (Gesundheitsdaten), sind besondere rechtliche Voraussetzungen für die Verarbeitung zu berücksichtigen, denn die Datenverarbeitung ist **nur** in Ausnahmefällen (Art. 9 Abs. 2 DSGVO) möglich. Dazu zählen die ausdrückliche Einwilligung des Patienten, das Vorliegen eines Behandlungsverhältnisses oder der nachgewiesene Zweck der Gesundheitsvorsorge, medizinischen Diagnostik oder Verwaltung von Systemen und Diensten im Gesundheitsbereich. Die Patienteneinwilligung bezieht sich auch auf einen bestimmten Zweck, der genannt werden muss, und daher darf die Datenverarbeitung nicht für andere Zwecke erfolgen.

Für die Erstellung des Verarbeitungsverzeichnisses können Sie sich an der Arbeitshilfe des Bayerischen Staatsministeriums des Innern für Sport und Integration[1] orientieren.

[1] https://www.stmi.bayern.de/sus/datensicherheit/datenschutz/reform_arbeitshilfen/index.php

Datenschutzmanagement

Für die erfolgreiche Umsetzung eines Datenschutzmanagements empfiehlt sich die Aufstellung eines Teams, das die Verantwortlichkeiten für die einzelnen Themenbereiche innehat. Das Team sollte aus Vertretern der einzelnen Abteilungen bestehen und dem Datenschutzbeauftragten, der bei Fragen unterstützen kann. Die Verantwortlichkeiten für die folgenden Themen sollten klar definiert und dokumentiert sein:

- Verzeichnis für Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Einhaltung technischer und organisatorischer Maßnahmen während der Datenverarbeitung[2] (Art. 32 DSGVO)
- Datenschutzkonzepte und -richtlinien (für das Personal)
- Auftragsverarbeitung und externe Dienstleister
- Risikoabschätzung[3] & Folgenabschätzung (Art. 35 DSGVO)
- Datenschutzverletzungen (Art. 33 DSGVO)
- Kommunikation mit Datenschutzaufsichtsbehörde
- Umgang mit Kundenanfragen (Betroffenenrechte)
- Zertifizierungen

Das Datenschutzmanagement sollte stets auf Aktualität überprüft und bei Änderungen entsprechend angepasst werden.

Neben dem Leitfaden kann auch die Checkliste „Cybersicherheit für medizinische Einrichtungen“[4] weitere Orientierung für die Berücksichtigung von Datenschutz in IT-Sicherheitsthemen geben. Eine Auswahl von datenschutzrelevanten Themen für Krankenhäuser behandeln wir in den folgenden Kapiteln.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 3 (Datenschutz)
- **B3S im Krankenhaus** – Kap. 7.13.19 (Datenschutz)
- **ISO/IEC 27001** – A.18 (Compliance)
- **BSI IT-Grundschutz-Kompendium** – CON.2 (Datenschutz), M 2.503 (Aspekte eines Datenschutzkonzeptes)

[2] Good Practice des Bayerischen Landesbeauftragten für den Datenschutz bei technischen und organisatorischen Maßnahmen https://www.lda.bayern.de/de/checklisten.html

[3] WP248 der Article29 Working Party https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

[4] https://www.lda.bayern.de/de/checklisten.html

9.2 Datenschutzkonforme Telearbeit im Krankenhaus

Kurzbeschreibung

Kurzbeschreibung

Der Zugriff auf Daten und deren Verarbeitung außerhalb des Arbeitsplatzes – Telearbeit – bringen einige Risiken und Herausforderungen mit sich. In Krankenhäusern handelt es sich um besonders schützenswerte personenbezogene Daten. Daher müssen entsprechende Vorsichtsmaßnahmen getroffen werden, um Telearbeit für das Krankenhauspersonal zu ermöglichen.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer	•		

Die IT-Abteilung ist für die Umsetzung und Ermöglichung der Telearbeit zuständig, indem sie die benötigte technische Infrastruktur bereitstellt und deren IT-Sicherheit gewährleistet. Das Krankenhauspersonal ist essenziell für die erfolgreiche datenschutzrechtliche Umsetzung von Telearbeit, denn es ist für den verantwortungsbewussten Umgang mit personenbezogenen Daten auch außerhalb der Arbeitsstelle verantwortlich.

Umsetzung der Maßnahme

Der Begriff **Telearbeit** wurde im November 2016 in § 2 Abs. 7 (1) ArbStättV wie folgt definiert:

> „Telearbeitsplätze sind vom Arbeitgeber fest eingerichtete Bildschirmarbeitsplätze im Privatbereich der Beschäftigten, für die der Arbeitgeber eine mit den Beschäftigten vereinbarte wöchentliche Arbeitszeit und die Dauer der Einrichtung festgelegt hat. Ein Telearbeitsplatz ist vom Arbeitgeber erst dann eingerichtet, wenn Arbeitgeber und Beschäftigte die Bedingungen der Telearbeit arbeitsvertraglich oder im Rahmen einer Vereinbarung festgelegt haben und die benötigte Ausstattung des Telearbeitsplatzes mit Mobiliar, Arbeitsmitteln einschließlich der Kommunikationseinrichtungen durch den Arbeitgeber oder eine von ihm beauftragte Person im Privatbereich des Beschäftigten bereitgestellt und installiert ist.“

Da es sich bei Patientendaten im Krankenhaus um besonders schützenswerte Daten handelt, sollte stets eine Abwägung des Risikos und der notwendigen Schutzmaßnahmen für die Datenverarbeitung bei Telearbeit erfolgen. Für eine sichere und datenschutzkonforme Telearbeit sorgen die folgenden Maßnahmen, die regulatorische, aber auch technische und organisatorische Aspekte beschreiben.

Richtlinie für Telearbeit

Für das Krankenhauspersonal, welches Telearbeit nutzen möchte, sollte eine Richtlinie existieren, an welcher sich das Personal orientieren kann. Die Richtlinie sollte mögliche Risiken bei der Telearbeit beschreiben, insbesondere in Bezug auf die Schutzziele – Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit. Außerdem sollte die Richtlinie klar regeln, für **welche Mitarbeiter** in **welchem Kontext und Umfang** Telearbeit möglich ist. Für das Personal, welches Telearbeit nutzen möchte und kann, sollten in der Richtlinie weitere Hinweise auf Maßnahmen existieren, die bei der Durchführung von Telearbeit zu berücksichtigen sind. Für die Sensibilisierung des Krankenhauspersonals hinsichtlich seiner Verantwortung während der Telearbeit bietet sich eine Nutzungsrichtlinie an, die das Personal unterschreiben muss, **bevor** die Möglichkeit zur Telearbeit genutzt werden kann.

Technische und organisatorische Maßnahmen

Grundsätzlich sind bei Telearbeit einige technische und organisatorische Maßnahmen einzuhalten. Dazu ge-

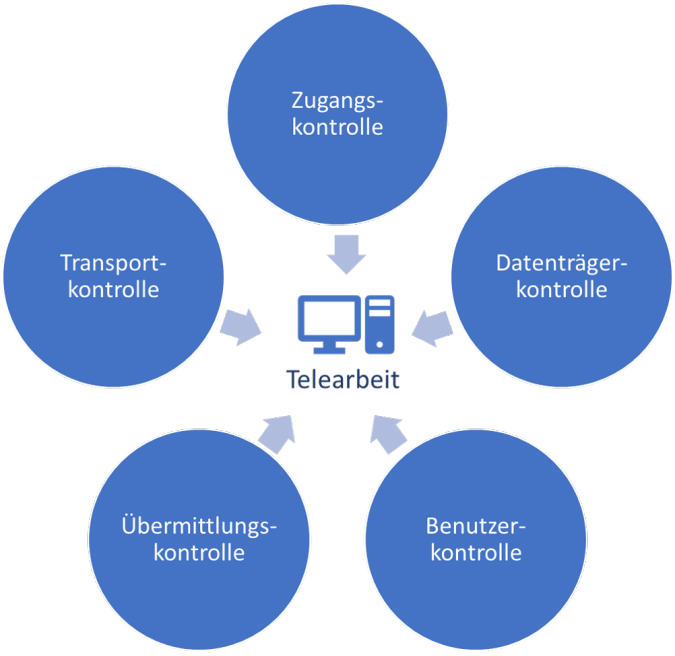


Abbildung 9.1: Übersicht der notwendigen Kontrollen für Telearbeit.

hören wesentliche Kontrollen gemäß Art. 7 Abs. 2 BayDSG:

- Zugangskontrolle: Unbefugte dürfen keinen Zugang zu Datenverarbeitungsanlagen erhalten.
- Datenträgerkontrolle: Inhalte von Datenträgern dürfen nicht durch Unbefugte verarbeitet werden.
- Benutzerkontrolle: Datenverarbeitungen dürfen nur von Befugten erfolgen.
- Übermittlungskontrolle: Feststellung und Überprüfung von personenbezogenen Daten und Systemen, aus welchen sie übertragen werden dürfen.
- Transportkontrolle: Bei der Übertragung und dem Transport von Datenträgern dürfen diese nicht durch Unbefugte verarbeitet werden.

Bei Patientendaten sind Desktop-Virtualisierung (vgl. Maßnahme 6.1 Handhabbarkeit von Arbeitsplatzrechnern und Rechnern des medizinischen Betriebs), Terminalserver und VPN (vgl. Maßnahmen 5.1 Absicherung des Netzzugangs und generelle Netz-Zonen und 6.6 Benutzerfreundliche Absicherung der Endgeräte zur mobilen Visite) wichtige Bestandteile, um Telearbeit zu ermöglichen. Diese Maßnahmen gewährleisten eine gesicherte Verbindung zu den Informationssystemen des Krankenhauses, sodass die Tätigkeiten direkt auf den Servern und nicht lokal durchgeführt werden müssen. Weitere Punkte, die für Telearbeit zu berücksichtigen sind:

- Keine Nutzung von Privatgeräten
- Systemzugriffe beschränken
- Zugriffsprotokollierung auf Systeme, Dienste und Daten
- Starkes Authentifizierungsverfahren
- Gesicherte, verschlüsselte Datenübertragung

Eine Herausforderung, die bei der Umsetzung technischer Maßnahmen auftreten kann, ist das Patch-Management (vgl. Maßnahme 7.2 Patchen zentraler Dienste mit geringer Auswirkung auf den Krankenhausbetrieb), da die Geräte für Telearbeit gelegentlich für Patches direkt im Krankenhausnetz angeschlossen werden müssen. Trotz der Umsetzung diverser technischer Maßnahmen gibt es dennoch weitere Risiken bei der Telearbeit, die auf mangelnde Awareness zurückgeführt werden können. So stellen zum Beispiel unberechtigte Einsichtnahmen von angezeigten Daten auf einem Bildschirm durch Unbefugte ein Risiko dar. Um diesem entgegenzuwirken, ist eine Sichtschutzfolie für Bildschirme und eine automatische Bildschirmsperre nach Timeout dringend zu empfehlen. Auf Ausdrucke, Kopien, Dokumente oder Patientenakten in Papierform sollte bei Telearbeit soweit wie möglich verzichtet werden, da diese Dokumente ein hohes Risiko für unbefugte Datenverarbeitung darstellen und Möglichkeiten für eine Risikominimierung, wie absperrbare Aktenschränke am Telearbeitsplatz, nicht immer zuverlässig umgesetzt werden.

Eine eigene krankenhausinterne Sicherheitsrichtlinie für Telearbeit mit geltenden Bestimmungen können Sie auf Basis der Vorlage aus Anhang A.4 Sicherheitsrichtlinie erstellen.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 27 (Mobile Sicherheit, Telearbeit, Bring Your Own Device (BYOD))
- **B3S im Krankenhaus** – Kap. 7.13.9 (Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit, ANF–MN 116–118)
- **ISO/IEC 27001** – A.6.2 (Mobilgeräte und Telearbeit)
- **BSI IT-Grundschutz-Kompendium** – OPS.1.2.4 (Telearbeit), INF.8 (Häuslicher Arbeitsplatz), INF.9 (Mobiler Arbeitsplatz)

9.3 Bring Your Own Device (BYOD) im Krankenhaus

Kurzbeschreibung

Kurzbeschreibung

Die Nutzung der eigenen privaten Endgeräte (Smartphone, Tablet, o. Ä.) im beruflichen Umfeld wird „Bring your own Device" (BYOD) genannt und führt im Krankenhaus zu Risiken. Die Trennung von privaten und beruflichen Daten gelingt bei der Nutzung eines Endgerätes oftmals nicht. Diese Maßnahme umfasst die rechtlichen Herausforderungen und Risiken sowie mögliche technische und organisatorische Maßnahmen, die BYOD absichern können.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			•

Nutzen einige Mitarbeiter BYOD für die Kommunikation und Arbeit mit Patientendaten, bleibt die Verantwortung für den Schutz der Patientendaten stets beim Krankenhaus und wird nicht auf eine einzelne Person übertragen. Daher muss die Geschäftsführung, die für Datenschutzverstöße haftet, eine datenschutzkonforme Umsetzung des BYOD sicherstellen. Dabei muss die IT-Abteilung bei der Umsetzung einbezogen werden, da diese für die Bereitstellung der Infrastruktur und Schulung von Mitarbeitern bzgl. des richtigen Umgangs bei BYOD benötigt werden.

Umsetzung der Maßnahme

Die Nutzung des privaten Smartphones für dienstliche Zwecke hat für viele Krankenhausangestellte einige Vorteile: Man hat nur ein Endgerät (ein separates Dienstgerät ist nicht notwendig) und damit auch alle Kontaktinformationen an einem Ort, das private Endgerät ist eventuell technologisch besser ausgestattet als die vom Krankenhaus bereitgestellten Dienstgeräte, der Umgang mit dem privaten Endgerät ist gewohnt. Trotzdem ist der Einsatz von BYOD im Krankenhaus datenschutzrechtlich kritisch zu betrachten. Die Deutsche Krankenhausgesellschaft und der Bayerische Landesbeauftragte für den Datenschutz raten sogar von BYOD im Krankenhaus ab, aufgrund des hohen Risikos für Patientendaten und der schwierigen datenschutzkonformen Umsetzung. Es kann nicht hinreichend sichergestellt werden, dass kein Unbefugter Einsicht in die Patientendaten bekommt, selbst wenn eine Speicherung der Daten nicht auf dem Endgerät erfolgt. Welche weiteren Risiken und rechtlichen Herausforderungen BYOD mit sich bringt, wird im nächsten Abschnitt erläutert. Anschließend werden technische und organisatorische Maßnahmen genannt, die für ein sicheres BYOD zwingend notwendig sind.

Rechtliche Anforderungen und Risiken

Beim Einsatz von BYOD im Krankenhaus sollte besonders Art. 27 Abs. 4 Sätze 1 bis 4 BayKrG beachtet werden. Diese Rechtsgrundlage besagt, dass Patientendaten nur von Personen eingesehen und genutzt werden dürfen, wenn dies für die Erfüllung der Aufgaben notwendig ist. D. h. alle Zugriffe auf Krankenhausinformationssysteme dürfen nur bei einer dienstlichen Notwendigkeit erfolgen.

Bei BYOD ist die Sicherstellung einer solchen kontrollierten Zugriffsmöglichkeit auf Krankenhausinformationssysteme nicht vollständig möglich. Ein weiteres Risiko ist die fehlende Kontrolle und Weisungsbefugnis über das private Endgerät des Krankenhauspersonals. Damit ergeben sich folgende Risiken:

- **Authentifizierung**: Eine sichere Bildschirmsperre ist als Zugriffsauthentifizierung für Krankenhausdaten zwingend notwendig. Doch bei privaten Endgeräten kann eine entsprechende Sicherheitsvorkehrung nicht kontrolliert bzw. durchgehend sichergestellt werden.
- **Schadsoftware**: Das Krankenhauspersonal kann auf seinem privaten Endgerät sämtliche Apps installieren, ohne dass diese von der IT-Abteilung des Krankenhauses auf IT-Sicherheitslücken überprüft und freigegeben wurden. Dies steigert das Risiko für Schadsoftware, die sich durch Zugriffe auf Krankenhausinformationssysteme im Krankenhaus weiter verbreiten können – eventuell auch ein neues Einfallstor für Cyberangriffe.
- **Updates**: Die regelmäßige Installation von Updates sichert nicht nur das Betriebssystem, sondern auch Apps vor IT-Sicherheitslücken. Doch die privaten Endgeräte können hinsichtlich der Durchführung regelmäßiger Updates nicht vom Krankenhaus kontrolliert bzw. gesteuert werden.
- **Verlust**: Bei Verlust des privaten Endgeräts kann eine Löschung von Patientendaten oder des Zugangs zum Krankenhausinformationssystem nicht mehr gewährleistet werden. Außerdem hat das Krankenhaus keine Möglichkeit, den Verleih oder die Weitergabe des Endgeräts an eine andere Person zu unterbinden.
- **Datentrennung**: Eine Trennung von privaten und dienstlichen Daten ist für die Einhaltung der unterschiedlichen datenschutzrechtlichen Anforde-

rungen zwingend notwendig, jedoch auf BYOD-Geräten kaum umsetzbar.

Eine Funktion, die BYOD im Krankenhaus beliebt macht, ist die Nutzung von Messenger-Diensten (z. B. WhatsApp, Signal, Threema, Telegram). Doch genau diese stellt BYOD vor weitere Risiken, da nicht alle Messenger-Dienste einen hohen IT-Sicherheitsstandard nachweisen, der für die Verarbeitung von Patientendaten notwendig ist. Technische Datenschutzanforderung für Messenger-Dienste im Krankenhauskontext wurden als „Whitepaper" im Rahmen der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder verfasst und bieten grundlegende Informationen über den sicheren und datenschutzkonformen Einsatz. [5]

Technische Maßnahmen

Wird bei der Nutzung von BYOD **nicht** auf hochsensible, personenbezogene Daten der besonderen Kategorien zugegriffen, sind folgende technische Maßnahmen für eine datenschutzkonforme Nutzung von privaten Endgeräten zu dienstlichen Zwecken notwendig:

- **Verschlüsselung**: Dienstliche personenbezogene Daten auf dem privaten Endgerät müssen verschlüsselt und separat von privaten Daten gespeichert werden. Die Verschlüsselung muss ebenfalls separat erfolgen, sodass die privaten Daten nicht durch Mitarbeiter der IT-Abteilung (Administratoren) eingesehen werden können.
- **Trennung von Apps und Daten – privat und dienstlich**: Private Apps dürfen keinen Zugriff auf dienstliche Daten (z. B. Adressbücher) haben. Auch die Datenablage muss getrennt erfolgen.
- **Mobile Device Management (MDM)**: Ein MDM ermöglicht die Steuerung und Kontrolle eines Endgerätes aus der Ferne. Dazu muss das Endgerät einen MDM-Client installiert haben. Bei Sicherheitsvorfällen oder Verlust ist es möglich, die Daten auf dem Endgerät zu verschlüsseln oder zu löschen (vgl. Maßnahme 6.7 Sichere mobile Geräte für den Krankenhausbetrieb ■■■).
- **Desktop-Virtualisierung**: Ein Remote-Zugriff auf Krankenhausinformationssysteme kann durch eine Desktop-Virtualisierung erreicht werden. Dabei werden Daten nicht lokal gespeichert und die Kontrolle über die Daten und Zugriffe bleiben beim Krankenhaus (vgl. Maßnahme 6.1 Handhabbarkeit von Arbeitsplatzrechnern und Rechnern des medizinischen Betriebs ■).
- **Container-Apps**: Dieser Ansatz ermöglicht das Erzeugen von Containern, sog. *„virtuellen Smartphones"*, auf dem Smartphone. Nur innerhalb eines solchen Containers kann auf dienstliche Daten und Anwendungen zugegriffen werden und das Krankenhaus behält den Zugriff auf diesen dienstlichen Container für Wartung, Sperrung und Löschung von Daten aus der Ferne.

Zentrale technische Maßnahmen können **unabhängig vom Endgerät** umgesetzt werden und erhöhen den Schutz für personenbezogene Daten. Einige passende Sicherheitsvorkehrungen sind in den Maßnahmen 5.1 Absicherung des Netzzugangs und generelle Netz-Zonen ■, 5.2 Logische Aufteilung des Krankenhausnetzes ■ und 5.4 Zentralisierte Überwachung ■ nachzulesen.

Organisatorische Maßnahmen

Beim Einsatz von BYOD sollten nicht nur technische Maßnahmen ergriffen werden, sondern auch organisatorische, die das Verantwortungsbewusstsein des Mitarbeiters stärken. Denn das unbefugte Lesen von Daten kann immer noch erfolgen, wenn der Nutzer unachtsam mit seinem Endgerät umgeht. Die folgenden Maßnahmen sind daher zu empfehlen:

- **Richtlinie**: Eine BYOD-Richtlinie sollte in Zusammenarbeit des Datenschutzbeauftragten, des IT-Sicherheitsbeauftragten, der juristischen Beratung und des Betriebsrats im Krankenhaus erstellt werden. Dabei sind die Mitarbeiter zu Sicherheitsmaßnahmen zu verpflichten. Ein Beispiel für Inhalte können Sie im Buch „Bring your own Device" von A. Kohne; S. Ringleb und C. Yücel nachlesen.[6]
- **Schulungen**: Eine Schulung für den richtigen Umgang mit Krankenhausdaten bei der Nutzung eines privaten Endgerätes ist eine Maßnahme, die die Sensibilisierung der Mitarbeiter bzgl. der Risiken steigert und den datenschutzkonformen Umgang fördert. In einer Schulung sollten die Themen „sicheres Passwort", „App-Sicherheit" und „Umgang bei Auffälligkeiten (IT-Sicherheitsvorfälle, Verlust, Diebstahl)" behandelt werden.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 27 (Mobile Sicherheit, Telearbeit, Bring Your Own Device (BYOD))
- **B3S im Krankenhaus** – Kap. 7.13.9 (Mobile Sicherheit, Sicherheit Mobiler Zugang und Telearbeit (ggf. „Bring Your Own Device" BYOD))
- **ISO/IEC 27001** – A.6.2 (Mobilgeräte und Telearbeit)
- **BSI IT-Grundschutz-Kompendium** – SYS.3.2 (Tablet und Smartphone)

[5] https://www.datenschutzkonferenz-online.de/media/oh/20191106_whitepaper_messenger_krankenhaus_dsk.pdf

[6] https://doi.org/10.1007/978-3-658-03717-8

9.4 Möglichkeiten zum Informationsaustausch

Kurzbeschreibung

Kurzbeschreibung

Bei der Übertragung von Daten an Dritte müssen rechtliche Anforderungen berücksichtigt werden, damit die Gesundheitsdaten dabei entsprechend dem Schutzbedarf geschützt sind. Diese Maßnahme beschreibt die rechtlichen Anforderungen für einen gesetzeskonformen Informationsaustausch mit Patienten, anderen Krankenhäusern und Ärzten sowie Forschungseinrichtungen.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			•

Die IT-Abteilung trägt die Verantwortung für die Bereitstellung der Infrastruktur (Tools, Systeme, Richtlinien, Schulungen etc.), die sich für einen gesetzeskonformen Datenaustausch eignet. Beim Einsatz eines Tools für den Informationsaustausch sollte das Datenschutzmanagement bzw. der Datenschutzbeauftragte involviert werden, damit die Einhaltung der entsprechenden Anforderungen sichergestellt werden kann.

Umsetzung der Maßnahme

Beim Austausch von Patientendaten muss beachtet werden, dass nur Behandelnde und damit Berechtigte Zugriff auf die entsprechenden Patientendaten erhalten. Insbesondere der elektronische Informationsaustausch muss sich der Herausforderungen einer dokumentengenauen Zugriffsberechtigung stellen. So muss es möglich sein, dass für jedes Dokument separat bestimmt werden kann, wer darauf Zugriff hat. Im Folgenden werden zuerst die rechtlichen Anforderungen für den Informationsaustausch mit Patienten und die, durch den Patienten beauftragte, Datenübertragung an andere Einrichtungen erläutert. Anschließend werden die aktuellen Risiken und Chancen des elektronischen Informationsaustauschs thematisiert und letztlich eine Zusammenfassung zum Informationsaustausch mit Forschungseinrichtungen gegeben. Eine Richtlinie zum sicheren Informationsaustausch kann beispielsweise auf Basis der Vorlage aus Anhang A.4 Sicherheitsrichtlinie definiert werden.

Rechtliche Anforderungen

Die Patienten können als Betroffene von ihrem Auskunftsrecht (Art. 15 DSGVO) Gebrauch machen und ihre personenbezogenen Daten vom Krankenhaus verlangen. Dabei müssen folgende Informationen an die Patienten übermittelt werden:

- Verarbeitungszwecke
- Kategorien der personenbezogenen Daten
- Empfänger der Daten
- Speicherdauer
- Informationen zum Recht auf Löschung
- Einschränkung der Bearbeitung und des Widerspruchsrechts gegen eine Verarbeitung
- Bestehen eines Beschwerderechts
- Herkunft der Daten (falls sie nicht von der betroffenen Person stammen)
- mögliche automatisierte Entscheidungsfindungen, basierend auf den personenbezogenen Daten

Außerdem muss eine Kopie der personenbezogenen Daten erstellt und übermittelt werden, die im Krankenhaus verarbeitet werden (Art. 15 Abs. 3 (1) DSGVO). Die Bereitstellung der verarbeiteten Daten erfolgt **elektronisch**, wenn der Patient den Antrag elektronisch stellt und dieser keine weiteren Angaben über die Form der Bereitstellung enthält (Art. 15 Abs. 3 (3) DSGVO).

Der Patient hat gemäß Art. 20 DSGVO das Recht auf eine Datenübertragung an andere Einrichtungen. Dabei ist besonders interessant, dass Art. 20 Abs. 1 DSGVO vorgibt, dass die Daten in einem *„strukturierten, gängigen und maschinenlesbaren Format“* an den Patienten bzw., *„wenn technisch machbar“*, direkt an einen anderen Verantwortlichen (Art. 20 Abs. 2 DSGVO) zu übertragen sind.

Betrachtet man den Austausch von Patientendaten zwischen Krankenhäusern bzw. Ärzten ohne die explizite Aufforderung des Patienten auf Grundlage des Art. 20 DSGVO, gilt dies als Weitergabe von Daten an Dritte und dabei muss die ärztliche Schweigepflicht gemäß §203 StGB als auch Art. 27 Abs. 4 BayKrG berücksichtigt werden. Diese Fälle werden in der Maßnahme 9.5 Externe Dienstleister für Krankenhäuser erläutert.

Elektronischer Informationsaustausch

Der Deutsche Bundestag verabschiedete das Patientendaten-Schutz-Gesetz (PDSG) im Juli 2020 trotz einiger Kritikpunkte der unabhängigen Datenschutzaufsichtsbehörden. Basierend auf dem PDSG wurde die elektronische Patientenakte (ePA) im Januar 2021 eingeführt, die einen elektronischen Informationsaustausch zwischen Ärzten vereinfachen soll. In der ePA können alle Gesundheitsdaten eines Patienten gesammelt werden. Die Informationsbeschaffung und -vermittlung für eine Behandlung bei einem neuen bzw. anderen Arzt ist nicht mehr notwendig, da sie in der ePA zentral abgerufen werden kann. Dies soll

dazu führen, dass Doppeluntersuchungen vermieden werden und eine effizientere Behandlung erfolgen kann.

Die unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder schätzen das PDSG und damit auch die ePA aufgrund von elementaren Widersprüchen zur DSGVO als europarechtswidrig ein und raten von der Nutzung der ePA in der aktuellen Form ab, bis (voraussichtlich 2022) entsprechende Verbesserungen und Erweiterungen vorgenommen wurden und die ePA auch DSGVO-konform ist.[7] Im Folgenden werden die aktuellen Hauptkritikpunkte erläutert, die zentrale Elemente einer elektronischen Informationsaustauschplattform beschreiben:

- **Zugriffsmanagement**: Momentan können Patienten, die die ePA nutzen möchten, nur festlegen, wann welcher Arzt alle abgespeicherten Unterlagen einsehen darf. Ein separates Zugriffsmanagement für jedes Dokument existiert nicht. Dies bedeutet, der Patient muss entweder alle seine Daten komplett freigeben oder keine.
- **Authentifizierung**: Da es sich in der ePA um Gesundheitsdaten handelt, muss gemäß DSGVO ein höchstmögliches Sicherheitsniveau beim Authentifizierungsverfahren sichergestellt werden.
- **Vertreterlösungen**: Dieser Kritikpunkt beschreibt die einzige Alternative – einen Vertreter – für Patienten, die kein Endgerät haben oder nutzen wollen, um die ePA zu befüllen bzw. zu managen. Damit müssen die Patienten dem Vertreter alle Zugriffsrechte gewähren und haben keine Möglichkeit, selbst zu entscheiden und ihre Dokumente eigenständig zu verwalten. Eine Alternative wären Terminals, an denen Patienten bei Bedarf ihre ePA verwalten können.

Möchten Patienten die ePA nutzen und Ärzte Befunde und Dokumente zur Behandlung in die ePA abspeichern, so ist eine Einwilligung des Patienten einzuholen.

Eine weitere Möglichkeit für den elektronischen Informationsaustausch stellen Datenaustauschplattformen dar. Die datenschutzrechtlichen Anforderungen und eine Checkliste für diese Plattformen im Gesundheitswesen wurden von der Arbeitsgruppe Datenschutz des Bundesverbands Gesundheits-IT e.V. erarbeitet.[8] Dabei wurden folgende technische Maßnahmen beschrieben, die dabei zu berücksichtigen sind:

- **Pseudonymisierung**: Gemäß Art. 32 DSGVO ist Pseudonymisierung eine Maßnahme, die zur Sicherheit der Daten beiträgt und ggf. (bei fehlender Umsetzung) begründet werden muss, weshalb keine Pseudonymisierung stattgefunden hat. Dabei ist wichtig, dass pseudonymisierte Daten nicht mehr einer identifizierten natürlichen Person zugewiesen werden können (Art. 4 Nr. 5 DSGVO).
- **Verschlüsselung**: Bei dieser Maßnahme gilt wie bei der Pseudonymisierung, dass gemäß Art. 32 DSGVO eine Verschlüsselung zur Sicherheit der Daten beiträgt und ggf. (bei fehlender Umsetzung) begründet werden muss, weshalb keine durchgeführt werden konnte.
- **Schutzziele**: Es sind entsprechende Maßnahmen für die Einhaltung der Schutzziele (Vertraulichkeit, Integrität, Verfügbarkeit) umzusetzen.

Informationsaustausch mit Forschungseinrichtungen

Um Patientendaten mit einer Forschungseinrichtung auszutauschen, müssen diverse rechtliche Anforderungen erfüllt werden. Gemäß Art. 9 DSGVO ist eine Weitergabe im Sinne des öffentlichen Interesses (der öffentlichen Gesundheit und dem Schutz vor Gesundheitsgefahren) möglich. Doch um die ärztliche Schweigepflicht (§203 StGB) und Betroffenenrechte nicht zu verletzen, müssen die Gesundheitsdaten **pseudonymisiert** werden, es sei denn, der Patient gibt eine Einwilligungserklärung für die Weitergabe seiner Daten an Forschungseinrichtungen ab. Der Informationsaustausch kann auch als Auftragsverarbeitung eingestuft werden. Sind die notwendigen Voraussetzungen dafür gegeben (vgl. Maßnahme 9.5 Externe Dienstleister für Krankenhäuser), so ist in Bayern die Auftragsverarbeitung zu Forschungszwecken eingeschränkt bzgl. der Schweigepflicht (§203 StGB), der Weitergabe an Forschungsstellen, die keine Kliniken sind und eine Genehmigung der Aufsichtsbehörde ist notwendig. Der Austausch mit **internen Forschungsabteilungen** ist in Bayern im Regelfall ohne eine Einwilligung zulässig.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 17 (Externe Dienstleister), 18 (Überprüfung im laufenden Betrieb)
- **B3S im Krankenhaus** – Kap. 7.13.16 (Umgang mit Datenträgern, Austausch von Datenträgern)
- **ISO/IEC 27001** – A.8.3 (Media handling), A.13.2 (Informationsübertragung)
- **BSI IT-Grundschutz-Kompendium** – OPS.1.2.3 (Informations- und Datenträgeraustausch)

[7] https://www.datenschutz-bayern.de/dsbk-ent/DSK_98p-PDSG.html

[8] https://www.gesundheitsdatenschutz.org/html/austauschplattformen.php

9.5 Externe Dienstleister für Krankenhäuser

Kurzbeschreibung

Kurzbeschreibung

In Krankenhäusern gibt es einige Tätigkeiten, Prozesse und Services, die durch externe Dienstleister durchgeführt bzw. unterstützt werden können. Insbesondere die IT-Abteilung kann durch externe Datenverarbeitung entlastet werden. Die dabei involvierten Daten müssen hinsichtlich des Datenschutzes bei der Übertragung geschützt werden. Diese Maßnahme beschreibt die rechtlichen Anforderungen und Voraussetzungen für den datenschutzkonformen Einsatz von externen Dienstleistern in Krankenhäusern.

Zuständigkeiten

	Umsetzung	Genehmigung	Einbezogen
Geschäftsführung		•	
IT-Abteilung	•		
Personal/Nutzer			•

Da es sich in dieser Maßnahme hauptsächlich um den Einsatz von externen Dienstleistern für die Datenverarbeitung in der Verwaltung handelt, ist primär die IT-Abteilung bei der Umsetzung involviert. Es können natürlich noch andere Aufgaben im Krankenhaus durch externe Dienstleister durchgeführt werden, wie z. B. das Facility Management, die Kantinenversorgung, usw. Diese Bereiche werden hier nicht behandelt, da es sich dabei nicht primär um eine Datenverarbeitung handelt.

Umsetzung der Maßnahme

Der Einsatz von externen Dienstleistern verringert die Arbeitslast in einigen Abteilungen im Krankenhaus, so kann die IT-Abteilung von einer Datenverarbeitung durch externe Dienstleister profitieren, z. B. zur Überwachung des WLAN-Netzes durch ein externes Threat Intelligence System. Beim Einsatz externer Dienstleister für die Datenverarbeitung muss besonders auf die dabei involvierten Daten geachtet werden.

Handelt es sich um **Gesundheitsdaten**, so müssen die Voraussetzungen für eine Verarbeitung gemäß Art. 9 DSGVO erfüllt sein und eine Auftragsverarbeitung oder die Übermittlung von Gesundheitsdaten an Dritte (externe Dienstleister) ist nicht ohne weiteres möglich. Bei anderen **personenbezogenen Daten**, z. B. IP-Adressen im Gäste-WLAN oder Personaldaten, müssen die Anforderungen aus Art. 6 DSGVO erfüllt sein, um eine Auftragsverarbeitung zu ermöglichen.

In den folgenden Abschnitten wird auf den Begriff **Auftragsverarbeiter** im Sinne der DSGVO und dessen relevanten Artikel als auch auf andere rechtliche Grundlagen eingegangen, die verbunden mit dem Einsatz von externen Dienstleistern relevant sind. Die Inhalte basieren auf der *Orientierungshilfe zum Gesundheitsdatenschutz* des Bundesministeriums für Wirtschaft und Energie.[9] Basierend auf einem Leitfaden des BayLf werden explizite Szenarien für die Auftragsdatenverarbeitung aufgeführt. Außerdem wird darauf eingegangen, wie externe Dienstleister (Dritte) für die Verarbeitung von Gesundheitsdaten eingesetzt werden können.

Generell empfiehlt es sich, alle internen Bestimmungen in einer Sicherheitsrichtlinie (Vorlage in Anhang A.4 Sicherheitsrichtlinie) zentral zu dokumentieren.

Auftragsverarbeitung

Ein externer Dienstleister kann als weisungsgebundener Auftragsverarbeiter fungieren und erhält damit eine Privilegierung bei der Datenverarbeitung. Doch dafür müssen bestimmte Anforderungen gemäß Art. 28 DSGVO zutreffen. Grundsätzlich definiert Art. 4 Nr. 8 DSGVO einen „Auftragsverarbeiter“ als

> „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.“

Das heißt, die Verantwortung für die Daten liegt stets beim Krankenhaus. Darf das Krankenhaus die Daten verarbeiten, so kann es dafür auch externe Dienstleister einsetzen. Beide Parteien (Krankenhaus und Dienstleister) werden als eine datenschutzrechtliche Einheit angesehen. Folgende Punkte beschreiben die notwendigen Voraussetzungen für den erfolgreichen Einsatz eines externen Dienstleisters als Auftragsverarbeiter:

- Es besteht ein Auftragsverarbeitungsvertrag zwischen Krankenhaus und externem Dienstleister.
- Das Krankenhaus weist den Dienstleister an, **wie** die Daten verarbeitet werden und zu welchem **Zweck**.
- Das Krankenhaus kontrolliert und beaufsichtigt die Datenverarbeitung durch externe Dienstleister.
- Die Verarbeitung findet in Gewahrsam des Krankenhauses statt oder die Daten sind unkenntlich gemacht worden (z. B. durch Verschlüsselung).

Für den Auftragsverarbeitungsvertrag können Sie sich an den Musterverträgen der Orientierungshilfe zum

[9] https://www.bmwi.de/Redaktion/DE/Publikationen/Wirtschaft/orientierungshilfe-gesundheitsdatenschutz.html, S. 54 ff.

Gesundheitsdatenschutz (S. 60) orientieren. Der Vertrag muss gemäß Art. 28 Abs. 3 DSGVO die in der Abbildung 9.2 dargestellten Inhalte enthalten. Im Leitfaden des bayerischen Landesbeauftragten für den Datenschutz[10] sind Szenarien zur Auftragsdatenverarbeitung bzgl. Serverstandort; Wartung, Fernwartung; Backup und elektronische Archivierung; Verwaltung des Papierarchivs; Scandienstleister und Entsorgung beschrieben.

Es gibt weitere rechtliche Anforderungen, die eine Privilegierung für die Datenverarbeitung nicht ermöglichen oder einschränken und daher zusätzlich beachtet werden müssen. Dazu zählt auch die Verarbeitung von Gesundheitsdaten.

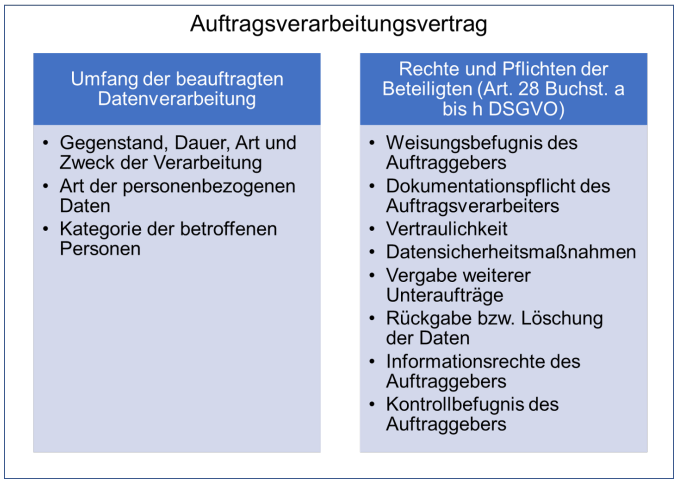


Abbildung 9.2: Inhalte eines Auftragsverarbeitungsvertrags.

Weitere rechtliche Anforderungen

Beim Einsatz von externen Dienstleistern ist Art. 27 Abs. 5 BayKrG zu beachten, welcher, wie auch Art. 9 DSGVO, besagt, dass die Übermittlung von Patientendaten an Dritte nur zulässig ist, wenn dies im Zuge der Behandlung und dessen verwaltungsmäßiger Abwicklung notwendig ist, als auch wenn eine andere Rechtsvorschrift die Übermittlung erlaubt oder der Patient seine Einwilligung dazu erteilt hat. Kann eine Einwilligung des Patienten für die Weitergabe von Patientendaten an vor-, mit- oder nachbehandelnde Ärzte angenommen werden, ist dies ebenfalls zulässig. Für die Datenübermittlung wird gemäß Art. 27 Abs. 6 BayKrG vorgeschrieben, dass technische und organisatorische Schutzmaßnahmen getroffen werden müssen, um Patientendaten vor Unbefugten zu schützen.

Die ärztliche Schweigepflicht ist besonders für das Vertrauensverhältnis mit den Patienten relevant. Das Patientengeheimnis ist gemäß §203 StGB zu schützen und kann bei Verstößen **strafrechtlich** verfolgt werden. Diese rechtliche Anforderung muss auch bei der Weitergabe von Patientendaten an externe Dienstleister berücksichtigt werden. Daher sollte immer eine Zwei-Stufen-Prüfung erfolgen:

- **Stufe 1:** Ist die Weitergabe der Patientendaten an externe Dienstleister datenschutzrechtlich zulässig? (Wenn nein, dann ist die Weitergabe verboten.)
- **Stufe 2:** Ist die Weitergabe der Patientendaten an externe Dienstleister strafrechtlich nach §203 StGB zulässig?

Verarbeitung von Gesundheitsdaten durch externe Dienstleister

Externe Dienstleister sind als „Dritte“ zu verstehen, an die Daten übertragen werden, die die Verantwortung für die Datenverarbeitung selbst tragen und daher nicht von der Privilegierung für Auftragsverarbeiter profitieren. Art. 4 Nr. 10 DSGVO definiert **Dritte** als

> „eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.“

Bei der Beauftragung von Dritten ist eine der folgenden Bedingungen gemäß Art. 9 DSGVO zu erfüllen, vor allem bei der Verarbeitung von Gesundheitsdaten:

- Ein Behandlungsverhältnis liegt vor.
- Die Daten werden zu einem der folgenden Zwecke gespeichert und verarbeitet: Gesundheitsvorsorge, medizinische Diagnostik, Verwaltung von Systemen und Diensten im Gesundheitsbereich.
- Die betroffenen Personen haben eingewilligt.

Neben diesen Bedingungen ist der Standort externer Dienstleister relevant und kann zu weiteren Anforderungen gemäß Art. 44 ff. DSGVO führen. Es sollte stets ein Dienstleister im nationalen oder EU-Raum bevorzugt werden, da für diesen die gleichen (datenschutz)rechtlichen Bestimmungen gelten.

Referenzen auf Standards

- **LSI Orientierungshilfe für Kliniken** – 17 (Externe Dienstleister)
- **B3S im Krankenhaus** – Kap. 7.12 (Lieferanten, Dienstleister und Dritte)
- **ISO/IEC 27001** – 7.1.1 (Sicherheitsüberprüfung), 13.2 (Informationsübertragung), 14.2 (Anschaffen, Entwickeln und Instandhalten von Systemen), 15.1.1 (Informationssicherheitsrichtlinie für Lieferantenbeziehungen)
- **BSI IT-Grundschutz-Kompendium** – OPS 3.1 (Outsourcing für Dienstleister)

[10] https://www.datenschutz-bayern.de/4/info_kh_leitfaden.pdf

Anhang A

Vorlagen für zentrale Dokumente des Informationssicherheitsmanagements

Der Anhang dieses Maßnahmenkatalogs stellt eine Reihe von Vorlagen zentraler Dokumente im Informationssicherheitsmanagement bereit, die von Krankenhäusern als Ausgangsbasis für die Anfertigung eigener Dokumente genutzt werden können. Die Struktur und Inhalte der Vorlagen orientieren sich dabei weitestgehend an bestehenden Vorarbeiten und Gesprächen mit Informationssicherheitsbeauftragten aus bayerischen Krankenhäusern und auch an Inhalten bestehender Standards. Die Vorlagen sind zudem mit dem bayerischen Landesamt für Sicherheit in der Informationstechnik abgestimmt. Das in Anhang A.1 Reifegradmodell für Informationssicherheitsdokumente gezeigte Reifegradmodell dient dabei als Hilfestellung zur Priorisierung von Dokumenten. Vorlagen umfassen die ISMS-Dokumente für

- eine Informationssicherheitsleitlinie,
- eine Dokumentation von Sicherheitsvorfällen,
- Sicherheitsrichtlinien,
- eine Richtlinie für die Bearbeitung von Sicherheitsvorfällen,
- einen Plan zur Mitarbeiterschulung,
- eine Übersicht und Sicherheitseinschätzung von Prozessen,
- eine Übersicht und Sicherheitseinschätzung von Prozessen realisierende Assets und Systemen,
- eine Übersicht und Sicherheitseinschätzung von Bedrohungen.

Die gelb markierten Abschnitte dienen dabei zur Kennzeichnung von Abschnitten, die an das jeweilige Krankenhaus angepasst werden müssen. Dabei werden Unterstützungshinweise gegeben, die beim Ausfüllen helfen sollen. Nicht markierte Abschnitte stellen üblicherweise notwendige Inhalte in den jeweiligen Dokumenten dar, können bei Bedarf jedoch auch angepasst werden. Jedes Dokument ist darüber hinaus mit einem Einstufungs-Vorschlag versehen (*öffentlich*, *intern* oder *geheim*) und orientiert sich dabei an der Richtlinie zur „Lenkung von Dokumenten und Aufzeichnungen“ des BSI.[1]

Um die Vorlagen aus diesem Katalog effektiv nutzen zu können, sind sie ebenfalls auf der Projektwebsite unter https://www.unibw.de/code/smart-hospitals als Word- bzw. Excel-Dateien bereitgestellt.

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Recplast/A03_Richtlinie_Lenkung_Dokumenten_und_Aufzeichnungen.pdf?__blob=publicationFile&v=5

A.1 Reifegradmodell für Informationssicherheitsdokumente

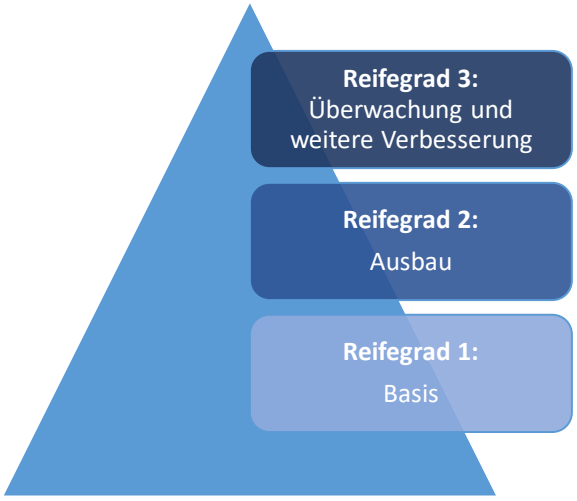
Universität der Bundeswehr München

Landesamt für Sicherheit in der Informationstechnik

Smart Hospitals

Sichere Digitalisierung bayerischer Krankenhäuser

IT-Security-Dokumente nach Reifegradstufen



Reifegradstufe 1: Basis

Dokument	Zweck	Bemerkung
Informationssicherheitsleitlinie	Bekennung der Geschäftsführung zur Umsetzung von IT-Sicherheit und Festlegung grundlegender Ziele, des Anwendungsbereichs, von Rollen und Aufgaben.	Dokumentvorlage in Anlage **Informationssicherheitsleitlinie** Hilfestellung in Maßnahme 3.2 des Maßnahmenkatalogs
Dokumentation über IT-Sicherheitsvorfälle	Strukturierte Befassung mit und Erfassung von Sicherheitsvorfällen und ihre geeignete Dokumentation.	Dokumentvorlage in Anlage **Doku-Sicherheitsvorfälle** Hilfestellung in Maßnahme 3.6 des Maßnahmenkatalogs
Risikoeinschätzung: Prozesseinschätzung	Definition der wichtigsten Prozesse im Krankenhaus. Jeder Prozess wird gemäß seiner Relevanz eingestuft; es werden grundlegende Überlegungen zum Ersatz oder Kompensation bei Ausfall definiert.	Dokumentvorlage in Anlage **Prozesseinschätzung** Hilfestellung in Maßnahme 3.5 des Maßnahmenkatalogs
Grundlegende Notfallplanung und Betriebswiederherstellung	Für die wichtigsten Prozesse wird eine tiefergreifende Notfallplanung mit Maßnahmen zur	Dokumentvorlage in Anlage **Richtlinie Sicherheitsvorfälle**

	Aufrechterhaltung des Betriebs erstellt. Außerdem grundlegende Überlegungen zur Wiederherstellung des Normalbetriebs des jeweiligen Prozesses.	Hilfestellung in Maßnahme 3.7 des Maßnahmenkatalogs
Plan zur Mitarbeiterschulung	Awareness für IT-Sicherheit bei Mitarbeitern ist aufgrund der hohen Bedeutung möglichst früh herzustellen. In Phase 1 wird daher bereits ein Plan dafür angelegt, welcher über 1-2 Jahre laufen soll.	Dokumentvorlage in Anlage **Plan-Mitarbeiterschulung** Hilfestellung in Maßnahmen 4.1-4.4 des Maßnahmenkatalogs

Reifegradstufe 2: Ausbau

Dokument	**Zweck**	**Bemerkung**
Sicherheitsrichtlinie Passwort	Festlegung krankenhausweit geeigneter Kriterien für sichere Passwörter anhand der Länge und Komplexität. Unterscheidung nach Bereich und Privilegien möglich.	*Dokumentvorlage in Anlage* ***Sicherheitsrichtlinie*** Hilfestellung in Maßnahme 3.4 des Maßnahmenkatalogs
Sicherheitsrichtlinie Backup	Festlegung von Kriterien geeigneter Backups, insb. Prozess, Häufigkeit, Art des Backups, Häufigkeit Wiedereinspielungs-Tests.	Dokumentvorlage in Anlage ***Sicherheitsrichtlinie*** Hilfestellung in Maßnahme 6.4 des Maßnahmenkatalogs
Sicherheitsrichtlinie Clean-Desk	Bestimmung zur sicheren Verwahrung und einem datenschutz-konformen Gebrauch von Dokumenten und Systemen. Insbesondere Anweisung zum Verschluss sensibler Dokumente nach Gebrauch.	Dokumentvorlage in Anlage ***Sicherheitsrichtlinie*** Hilfestellung in Maßnahme 3.4 des Maßnahmenkatalogs
Sicherheitsrichtlinie Informationsaustausch	Festlegung von Kriterien zum sicheren Austausch von Daten im Krankenhaus und darüber hinaus. Z.B. mit sicheren Kommunikationswegen,	Dokumentvorlage in Anlage ***Sicherheitsrichtlinie*** Hilfestellung in Maßnahme 9.4 des Maßnahmenkatalogs

	Kryptographie-Verfahren und Software-Werkzeugen	
Sicherheitsrichtlinie Verhalten in Arbeitszonen	Festlegung von Verhalten der Mitarbeiter in physisch definierten Schutzzonen (z. B. öffentlicher Bereich, kontrollierter Bereich, usw.).	Dokumentvorlage in Anlage ***Sicherheitsrichtlinie*** Hilfestellung in Maßnahme 8.1 des Maßnahmenkatalogs
Sicherheitsrichtlinie Lieferanten und Dienstleister	Festlegung des Umgangs mit Dienstleistern unter Aspekten der IT-Sicherheit. Dazu zählen notwendige Vertragsklauseln, Schulungen, Richtlinien zum Informationsaustausch und die Überprüfung von Lieferanten.	Dokumentvorlage in Anlage ***Sicherheitsrichtlinie*** Hilfestellung in Maßnahme 9.5 des Maßnahmenkatalogs
Sicherheitsrichtlinie Telearbeit	Festlegung von Verfahren zum sicheren Umgang mit Systemen und Informationen bei Telearbeit (z. B. Home-Office).	Dokumentvorlage in Anlage ***Sicherheitsrichtlinie*** Hilfestellung in Maßnahme 9.2 des Maßnahmenkatalogs
Sicherheitsrichtlinie für Notfallplan	Festlegung von Inhalten und einem Prozess bei der Notfallplanungerstellung; bei bis dato bestehenden Notfallplänen werden hier oft Revisionen notwendig.	Dokumentvorlage in Anlage **Sicherheitsrichtlinie Notfallmanagement** Hilfestellung in Maßnahme 3.7 des Maßnahmenkatalogs
Risikoeinschätzung: Asseteinschätzung	Festlegung wichtiger Assets, insbesondere in Bezug auf zuvor definierte kritische Prozesse im Krankenhausbetrieb. Zuweisung von Abhängigkeiten von Prozessen zu Assets sowie Einschätzung der Kritikalität der einzelnen Assets für darauf aufbauende Prozesse.	Dokumentvorlage in Anlage **Asseteinschätzung** Hilfestellung in Maßnahme 3.5 des Maßnahmenkatalogs

Reifegradstufe 3: Überwachung und weitere Verbesserung

Smart Hospitals

Sichere Digitalisierung bayerischer Krankenhäuser

Dokument	Zweck	Bemerkung
Risikoeinschätzung: Bedrohungseinschätzung	Anlegen einer Sammlung potenzieller Bedrohungen, die die Zuverlässigkeit von Assets und Prozesse negativ beeinflussen. Sammeln möglicher Maßnahmen zur Absicherung gegen Bedrohungen (insb. präventiv und reagierend).	Dokumentvorlage in Anlage **Bedrohungseinschätzung** Hilfestellung in Maßnahme 3.5 des Maßnahmenkatalogs
Sicherheitsrichtlinie für interne Audits	Festlegung eines einheitlichen Prozesses zur internen Auditierung. Dazu zählt die Planung von Audits, die Bestimmung neutraler Auditoren und die Durchführung von Audits.	Dokumentvorlage in Anlage ***Sicherheitsrichtlinie***

A.2 Informationssicherheitsleitlinie

der Bundeswehr Universität München

Landesamt für Sicherheit in der Informationstechnik

Smart Hospitals

Sichere Digitalisierung bayerischer Krankenhäuser

Informationssicherheitsleitlinie für das Klinikum [NAME]

[DATUM]

Klassifizierung: Öffentlich

Universität der Bundeswehr München

Landesamt für Sicherheit in der Informationstechnik

Smart Hospitals

Sichere Digitalisierung bayerischer Krankenhäuser

Zweck

Die Leitung des Klinikums [NAME] äußert mit dieser Leitlinie den hohen Stellenwert der Aufrechterhaltung der Informationssicherheit im Betrieb und darin anfallender und verarbeiteter Daten. Dieses Dokument definiert eine aufgegliederte Zielsetzung im Kontext der Informationssicherheit und legt den Geltungsbereich, eine allgemeine Sicherheitsstrategie mit kontinuierlicher Verbesserungsabsicht sowie den grundlegenden organisatorischen Rahmen fest. Dieses Dokument spiegelt daher die Überzeugungen der Geschäftsführung des Klinikums wider.

Zielsetzung

[Warum Informationssicherheit im Krankenhaus?

- Gesellschaftlicher Auftrag eines Krankenhauses im Gesundheitssystem
- Kritikalität der Informationen, die in Krankenhäusern generiert und verarbeitet werden
- Stellenwert der IT im Krankenhaus]

[Betonung des Stellenwerts der Informationssicherheit, der Bedeutung von Informationen und Geschäftsprozessen]

Ziele, die im Rahmen einer Gewährleistung von Informationssicherheit im Krankenhaus/Klinikum [NAME] verfolgt werden, sind im Einzelnen:

- Der Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen und Diensten
- Der Schutz von Patienten und Personal
- Gewährleistung der Einhaltung gesetzlicher Anforderungen
- Gewährleistung einer effektiven Patientenversorgung
- [Weitere Individualanforderungen]

Geltungsbereich

Die in diesem Dokument festgehaltene Leitlinie der Informationssicherheit gilt für die Betriebsstätten [LISTE BETRIEBSSTÄTTEN] und im besonderen Fokus des medizinischen Betriebs für die Kernprozesse [LISTE KERNPROZESSE, vgl. B3S im Krankenhaus, Kap. 5.2.1 ff]. Jeder (interne als auch externe Dienstleister), der

Informationen oder Infrastruktur des Krankenhauses [HAUS] nutzt, unterliegt dieser Informationssicherheitsrichtlinie und ist zu entsprechendem Handeln verpflichtet.

Bewusst und begründet ausgeschlossen aus dem Geltungsbereich sind…

[LISTE AUSGESCHLOSSENER BETRIEBSSTÄTTEN mit jeweiliger kurzer Begründung]

[LISTE AUSGESCHLOSSENER KERNPROZESSE mit jeweiliger Begründung. Eine Liste der wichtigsten Kernprozesse im Krankenhaus findet sich im Branchenspezifischen Standard B3S der DKG]

Sicherheitsstrategie

- [KURZE/GROBE BESCHREIBUNG GESAMTKONZEPT Hinweis: Die Sicherheitsstrategie kann sinnvoll anhand des Vorgehensmodells der „Orientierungshilfe IT-Sicherheit in Kliniken“ des bayerischen Landesamts für Sicherheit (LSI) in der Informationstechnik festgelegt werden. Dieses Dokument kann vom LSI per E-Mail an beratung-kritis@lsi.bayern.de angefordert werden.
- Hinweis: Verwenden Sie auch unser Reifegradmodell mit Reifegradstufen 1-3 und Zielen zur zeitlichen Erreichung der jeweiligen Reifegradstufe
- **Hinweis: Diese Leitlinie ist allgemein öffentlich einsehbar. Beschreiben Sie hier keine Details zur Ihrer Sicherheitsstrategie, die Externe oder potenzielle Angreifer auf Schwachstellen hinweisen könnten. Eine detaillierte Sicherheitsstrategie müssen Sie in einem internen Dokument beschreiben!]**

Rollen, Verantwortlichkeiten und Pflichten

Die Gesamtverantwortung für die Einhaltung und Erfüllung der Sicherheitsstrategie hat die Geschäftsführung. Des Weiteren sieht das Informationssicherheitsmanagement des Krankenhauses [NAME] weitere im Folgenden aufgelistete Rollen mit entsprechenden Verantwortlichkeiten vor.

Informationssicherheitsbeauftragter (ISB)	Der Informationssicherheitsbeauftragte ist verantwortlich für die organisatorische Umsetzung des Prozesses des Informationssicherheitsmanagements. Er ist diesbezüglich unmittelbar der Geschäftsführung unterstellt. [WEITERE AUFGABEN]
Datenschutzbeauftragter (DSB)	Der Datenschutzbeauftragte ist für die Umsetzung und Kontrolle der Einhaltung rechtlicher Bestimmungen zum Datenschutz innerhalb des Krankenhauses verantwortlich. Darüber hinaus ist er für die Organisation und Bewusstseinsmaßnahmen des Datenschutzes im Krankenhaus zuständig. Um seine Aufgaben effektiv

	ausführen zu können, ist der DSB direkt der Geschäftsführung unterstellt. [WEITERE AUFGABEN]
IT-Sicherheitsmanager	Die Aufgaben eines IT-Sicherheitsmanagers dienen in erster Linie der Umsetzung von Informationssicherheit im Krankenhaus. Dazu gehören unter anderem: • Die Erarbeitung geeigneter Vorgaben und Richtlinien der Nutzung von IT-Systemen • Die Erarbeitung von Vorgaben für sichere Soft- und Hardware • Die Erarbeitung von Lösungen zum Einsatz von Soft- und Hardware zur Absicherung von Systemen und Informationen • Beratung von Anwendern bezüglich Informationssicherheit • [WEITERE]
[WEITERE]	

Basiskriterien der Wirksamkeit

Das ISMS wird grundsätzlich auf Basis folgender Kriterien bewertet:

- Die Bekanntheit dieses Dokuments und der Wille zur Verbesserung der Informationssicherheit unter den Mitarbeitern
- Konformität des ISMS zu gesetzlichen Bestimmungen
- Umsetzungsgrad des ISMS
- [WEITERE]

Meldewege bei Vorfällen

Alle Personen (krankenhausintern als auch extern), die im Geltungsbereich des Dokuments nicht ausdrücklich und begründet ausgeschlossen sind, haben die Pflicht, sicherheitsrelevante Ereignisse, Beobachtungen und erkannte Sicherheitsvorfälle über [MELDEWEG, ROLLE oder MEDIUM] unverzüglich zu melden.

Ein Sicherheitsvorfall ist gegeben, sobald eines der im Abschnitt **Zielsetzung** aufgeführten Ziele erkennbar verletzt wurde. Ein sicherheitsrelevantes Ereignis ist gegeben, sobald eines der aufgeführten Ziele gefährdet erscheint.

Universität der Bundeswehr München

Landesamt für Sicherheit in der Informationstechnik

Smart Hospitals

Sichere Digitalisierung bayerischer Krankenhäuser

Inkrafttreten, Zusicherung und Durchsetzung

Die vorliegende Informationssicherheitsrichtlinie tritt unmittelbar auf Beschluss der Geschäftsführung in Kraft.

Die Geschäftsführung des Klinikums [NAME] bekennt sich zu den in dieser Richtlinie festgelegten Zielen, dem Geltungsbereich und der beschriebenen Sicherheitsstrategie. Verstöße und Zuwiderhandlungen gegen Überzeugungen und Vorgaben der Informationssicherheitsrichtlinie werden gemäß einem formellen Maßregelprozess behandelt.

_____

[NAME GESCHÄFTSFÜHRER]

Klassifizierung: Öffentlich

A.3 Dokumentation von IT-Sicherheitsvorfällen

Universität der Bundeswehr München

Smart Hospitals

Sichere Digitalisierung bayerischer Krankenhäuser

Landesamt für Sicherheit in der Informationstechnik

Dokumentation von IT-Sicherheitsvorfällen

Nr.	Datum Vorfall	Typ	Kritikalität (z.B. hoch, mittel, gering)	Zuständiger Incident-Handler	Beschreibung Vorfall (Auswirkung, Dauer, betroffene Assets)	Folgen und Schäden	Notwendige Korrekturmaßnahmen	Datum Behebung
1	*24.02.21 BEISPIEL*	*ITSV (IT-Sicherheits-vorfall)*	*Hoch (Beeinträchtigung Verfügbarkeit, Patientenversorgung)*	*Max Mustermann*	*Ausfall der Stromversorgung im Serverraum für 45 Minuten. Ausfall zentraler Dienste. USV nicht ausreichend.*	*Ausfall Prozess Aufnahme, Diagnostik und Behandlung.*	*Starten von Generatoren, Hochfahren zentraler Dienste*	*24.02.21*
2	*01.04.21 BEISPIEL*	*DS (Datenschutz-vorfall)*	*Mittel (Mögliche Beeinträchtigung Vertraulichkeit)*	*Erika Mustermann*	*Akten wurden nicht ordnungsgemäß geschreddert sondern unzureichend entsorgt.*	*Keine Folgen oder Schäden*	*Dokumente wurden im Müll entdeckt und ordnungsgemäß entsorgt.*	*01.04.21*
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								
23								
24								

Klassifizierung: Geheim

A.4 Sicherheitsrichtlinie

Universität der Bundeswehr München

Landesamt für Sicherheit in der Informationstechnik

Smart Hospitals

Sichere Digitalisierung bayerischer Krankenhäuser

Sicherheitsrichtlinie

[Titel der Richtlinie]

Informationen zur Version

Version und Datum	Bearbeiter	Änderungsprotokoll

Zielsetzung und Zweck der Richtlinie

[Welche Sicherheitsprobleme sollen durch die Maßnahme geschlossen werden?]

Referenzdokumente

- Informationssicherheitsrichtlinie
- [weitere krankenhausinterne und -externe relevante Dokumente]

Sicherstellung der Wirksamkeit

Die Sicherstellung der Umsetzung der Sicherheitsrichtlinie wird wie folgt erreicht:

- [Hier Maßnahmen zur Überwachung beschreiben, z. B. stichprobenartige Kontrollen]

Herangezogene Kennzahlen zur Messung der Wirksamkeit der Richtlinie sind

- [hier Kennzahlen, z. B. Anzahl der Richtlinienverletzung pro einheitlichem Auditzeitraum]

Klassifizierung: Intern

Universität der Bundeswehr München

Landesamt für Sicherheit in der Informationstechnik

Smart Hospitals

Sichere Digitalisierung bayerischer Krankenhäuser

Gültigkeit

- [Von wann bis wann ist die Maßnahme gültig?]

Verantwortlicher für Sicherheitsrichtlinie:

[Rolle, z. B. Informationssicherheitsbeauftragter]

[Name des Verantwortlichen]

Klassifizierung: Intern

A.5 Richtlinie für das Verhalten bei IT-Sicherheitsvorfällen

Universität der Bundeswehr München

Landesamt für Sicherheit in der Informationstechnik

Smart Hospitals

Sichere Digitalisierung bayerischer Krankenhäuser

Sicherheitsrichtlinie

Verhalten bei IT-Sicherheitsvorfällen

Informationen zur Version

Version und Datum	Bearbeiter	Änderungsprotokoll

Zielsetzung und Zweck der Richtlinie

Mit dieser Richtlinie wird definiert, wie Mitarbeiterinnen und Mitarbeiter des Klinikums [NAME] mit Informationssicherheits- und IT-Sicherheits-Vorfällen umgehen sollen. Alle Mitarbeiterinnen und Mitarbeiter sind durch die Einhaltung dieser Richtlinie dazu angehalten, durch Vorfälle und Notfälle entstehenden Schaden jeglicher Art abzuwenden oder einzudämmen.

Ein IT-Sicherheitsvorfall ist ein Schadensereignis, bei dem Prozesse oder Ressourcen des Klinikums nicht wie vorgesehen funktionieren oder durch Angreifer insofern ausgenutzt werden, dass sie zu einem (personellen, finanziellen, ansehens-, oder sonstig gearteten) Schaden für das Klinikum, seiner Mitarbeiter oder Patienten und Gäste führen können.

[Welche Sicherheitsprobleme sollen durch die Maßnahme geschlossen werden?]

Referenzdokumente

- Informationssicherheitsrichtlinie
- [weitere klinikumsinterne und -externe relevante Dokumente]

Klassifizierung: Intern

Meldestellen im Fall eines erkannten Vorfalls

Wenn Sie einen IT-Sicherheitsvorfall oder -Notfall vermuten, dann melden Sie dies unverzüglich an eine der in der hier gezeigten Tabelle genannten Stellen. Ein IT-Vorfall oder -Notfall kann beispielsweise eine der folgenden Situationen sein:

- Unbefugte Personen im internen Bereich (z. B. Verwaltung, Serverraum, Labor, usw.)
- Erhaltene Phishing- und Betrugs-E-Mails
- Malware auf dem Arbeitsplatzrechner
- [WEITERE]

Meldestelle	**Erreichbarkeit**	**Vertretung**
Informationssicherheitsbeauftragter: [NAME Rollenträger]	[Telefon, E-Mail]	[NAME, ERREICHBARKEIT]
…	…	…

Gültigkeit

- [Von wann bis wann ist die Maßnahme gültig?]

Verantwortlicher für Sicherheitsrichtlinie:

[Rolle, z. B. Informationssicherheitsbeauftragter]

[Name des Verantwortlichen]

A.6 Plan zur Mitarbeiterschulung

Universität der Bundeswehr München

Landesamt für Sicherheit in der Informationstechnik

Smart Hospitals

Sichere Digitalisierung bayerischer Krankenhäuser

Plan für Mitarbeiterschulungen zur Awareness rund um IT-Sicherheit

Informationen zur Version

Version und Datum	Bearbeiter	Änderungsprotokoll

Berücksichtigte Zielgruppe

Dieser Plan beschreibt ein Konzept zur Awarenessschaffung von Mitarbeitern, die zu den folgenden Gruppen gehören:

[Auflistung der Tätigkeitsbereiche die auf die dieser Planung für Awareness-Schulungen angewendet werden soll, z. B.

- Geschäftsführung
- Verwaltung
- Ärzteschaft
- Pflege
- Technik und IT
- Reinigungskräfte
- Externe Dienstleister
- usw.]

Konkrete Ziele der Kompetenzerlangung bei Mitarbeitern

Durch die in diesem Plan festgehaltenen Inhalte und stufenweise Vorgehensweise zur Awareness-Steigerung im Kontext der IT- und Informationssicherheit soll das Personal die folgenden Kompetenzen erlangen bzw. ausbauen:

Klassifizierung: Intern

[Ziele nennen, z.B.

- Erkennen und richtiges Handhaben von Phishing-E-Mails
- Den sicheren Umgang mit personenbezogenen Daten
- Die sichere Benutzung von IT-Systemen (Büro-PCs, mobile Geräte, ausgewählte medizinische Geräte)
- Weitere individuelle, möglichst konkrete Ziele]

Stufenmodell und Zeitplan

Für diesen Plan zur Awareness-Schulung bezüglich der zuvor genannten Zielgruppen und zur Erreichung der zuvor festgelegten Ziele werden die folgenden Stufen gemäß Fox-Kaun-Modell mit jeweils festgelegtem zeitlichem Umfang vorgesehen:

1. Aufmerksamkeit schaffen (Monat [X1] bis Monat [X2 > (größer als Wert von) X1])
    a. Plakat
        i. [Konkrete Aussage und Inhalte festlegen]
    b. Flyer
        i. [Konkrete Aussage und Inhalte festlegen]
    c. Schreiben durch IS-Beauftragten oder Vorstand
        i. [Konkrete Aussage und Inhalte festlegen]
    d. [weitere]

2. Wissensausbau und Schaffung von Awareness-Einstellung (Monat [X3 > X2] bis Monat [X4 > X3])
    a. Informationsveranstaltungen
        i. [Konkrete Ziele und Inhalte festlegen]
    b. Intranet-Seiten
        i. [Konkrete Ziele und Inhalte festlegen]
    c. Individuelle freiwillige Beratung
        i. [Konkrete Ziele und Inhalte festlegen]
    d. [optional z. B. Übungen und Planspiele]
    e. [weitere]
3. Verstärkung von Aufmerksamkeit, Wissen und Einstellung (Monat [X5> X5] bis Monat [X6 > X5])
    a. Preise und Auszeichnungen (z. B. für richtiges Handeln)
        i. [Details]
    b. Quiz und Spiele
        i. [Details]
4. [optional Öffentlichkeitsarbeit]

der Bundeswehr Universität München

Landesamt für Sicherheit in der Informationstechnik

Smart Hospitals

Sichere Digitalisierung bayerischer Krankenhäuser

Terminübersicht

Datum	Stufenzuordnung	Art	Thema	Anmerkungen
[Datum eines Termins]	[Zuordnung gemäß der Stufen aus dem vorherigen Abschnitt, z.B. „1A“, „3B“, usw.]	[Art des Termins, z.B. Treffen, Vortrag, Planspiel, Übung, usw.]	[Thema des Termins, z.B. „Sicherer Umgang mit mobilen Datenträgern“, „Erkennung von Phishing-E-Mails“, usw.]	[Weitere Anmerkungen, z.B. zur Durchführung, Nennung Verantwortlicher, usw.]

Referenzdokumente

- Informationssicherheitsrichtlinie
- [weitere klinikumsinterne und -externe relevante Dokumente]

Klassifizierung: Intern

A.7 Übersicht über Prozesse

Auf unserer Website https://www.unibw.de/code/smart-hospitals finden Sie eine Tabelle zur Beschreibung Ihrer Prozesse im Krankenhaus. Diese Tabelle umfasst die Felder

- **Prozess-ID**, welche für einen von Ihnen beschriebenen Prozess (z. B. Patientenaufnahme) eine eindeutige ID definiert, die auch in anderen Dokumenten für Referenzen genutzt werden kann.
- **Prozessbeschreibung**, die den Zweck des Prozesses beschreibt.
- **Prozess-Kritikalität**, die die Kritikalität des Prozesses klassifiziert und eine Behandlungspriorität vorgibt.
- **Auswirkungen bei Ausfall**, in dem auf einen Blick die Auswirkungen bei einem Ausfall des Prozesses (auch auf andere Prozesse) beschrieben werden.
- **Wahrscheinlichkeit für Ausfall**, wodurch ebenfalls Kriterien für den Schutzbedarf abgeleitet werden können.
- **Mögliche Behandlungsmaßnahmen**, die in diesem Dokument auf einen Blick gesammelt und z. B. auf Detailbeschreibungen zur Behebung referenziert werden können, sodass eine Prozesswiederherstellung schneller vonstatten gehen kann.

A.8 Übersicht über Assets und Systeme

Auf unserer Website https://www.unibw.de/code/smart-hospitals finden Sie eine Tabelle zur Beschreibung Ihrer Assets (*alles was für das Krankenhaus von Wert ist*) und Systeme im Krankenhaus, insbesondere in Hinblick auf ihre Bereitstellung essenzieller Prozesse. Diese Tabelle umfasst die Felder

- **Asset-ID**, die das Asset im Kontext von ISMS-Dokumenten eindeutig beschreibt.
- **Asset-Bezeichner**, der ein Asset informell und gut verständlich beschreibt.
- **Asset-Eigentümer**, der den Hauptverantwortlichen für ein Asset darstellt und bei einem Ausfall auch für dessen Wiederherstellung verantwortlich ist.
- **Abhängige Prozesse**, die von dem jeweiligen Asset abhängen. Mit ihnen können bei einem Ausfall eines Assets beeinträchtigte Prozesse schnell erkannt werden.
- **Maximal tolerierbare Ausfallzeit** des Assets, in der keine schwerwiegenderen Probleme für den Krankenhausbetrieb zu erwarten sind.
- **Kritikalität verarbeiteter Daten** auf dem System/Asset zur Einschätzung des Schutzbedarfs hinsichtlich des Aspekts Datenschutz.
- **Kritikalität Asset**, wodurch eine Priorisierung von Assets und Systemen bei der Behandlung und dem Schutz-Aufwand möglich wird.
- **Begründung der Einschätzung**, die die vorgesehene Kritikalität nachvollziehbar macht.

A.9 Übersicht über Bedrohungen

Auf unserer Website https://www.unibw.de/code/smart-hospitals finden Sie eine Tabelle zur Beschreibung möglicher Bedrohungen für den Betrieb Ihres Krankenhauses. Bedrohungen sollten grundsätzlich definiert sein und neben den Verantwortlichen sollte auch jeder relevante Mitarbeiter auf sie vorbereitet werden. Diese Tabelle umfasst die Felder

- **Bedrohung-ID**, die eine Bedrohungsbeschreibung eindeutig identifiziert.
- **Bedrohung-Kurztitel**, der eine Bedrohung verständlich beschreibt.
- **Schwachstelle**, die von der Bedrohung potenziell ausnutzbare Schwachstellen (in Software, Hardware oder über Personal) beschreiben oder referenzieren.
- **Auswirkung**, die bei Eintreten einer Bedrohung potenziell oder wahrscheinlich zu erwarten ist.
- **Eintritts-Wahrscheinlichkeit** der Bedrohung, wodurch in Verbindung mit den Auswirkungen eine Priorisierung der Absicherung erstellt werden kann.
- **Eintritts-Risiko**, das die Auswirkung und Eintrittswahrscheinlichkeit durch eine Risikoklassifikation zusammenfasst.
- **Betroffene Assets** durch die Bedrohung, auf die über ihre eindeutige ID referenziert wird.
- **Mögliche Behandlungsmaßnahmen**, mit denen ein Eintreten der Bedrohung behandelt oder abgeschwächt werden kann.

ISBN 978-3-943207-54-5

ISBN 978-3-943207-54-5