MATERNA
Information & Communications

Sicherheitsorientierte Digitalisierungsstrategie für Krankenhäuser

Dr. Jörg Kebbedies

MATERNA
Information & Communications

Inhaltsverzeichnis

1 Materna-Kompetenz ... 2

2 Rahmenbedingungen: regulierte Krankenhaus-Digitalisierung ... 3

2.1 Umsetzungsplan KRITIS ... 4

2.2 IT-SiG ... 4

2.3 B3S im Krankenhaus ... 4

2.4 DSGVO ... 5

2.5 SGB I/X ... 5

3 Baustein: strukturierte Sicherheitsanalyse ... 5

3.1 Problem: Sicherheitsbewertung komplexer IT-Systeme ... 5

3.2 Lösung: Architekturbezogene Sicherheitsbewertung ... 6

3.2.1 Methodische Ausrichtung ... 7

3.2.2 Strukturelle Ausrichtung ... 7

3.3 Sicherheits-Dienstleistungen ... 8

4 Baustein: Sicherheitsarchitektur – Sicherheitsentwicklung ... 9

4.1 Problem: Softwareentwicklung – Security-By-Design ... 9

4.1.1 Schwer nachvollziehbares IT-Architekturdesign ... 9

4.1.2 Aufwändige Sicherheitsbewertung ... 9

4.2 Lösung: Strukturiertes Funktions- und Sicherheitsdesign ... 10

4.3 Sicherheits-Dienstleistungen ... 11

5 Baustein: gesetzeskonforme Datenverteilung ... 12

5.1 Problem: Überlagerte Regulierungsziele ... 12

5.2 Lösung: Sichere Kooperation mit Gesundheitsdaten ... 12

5.2.1 Sicherheitsarchitektur ... 13

5.2.2 Sicherheitsziele ... 13

5.3 Sicherheits-Dienstleistungen ... 14

6 Baustein: Krankenhaus Anwendungsschutz ... 15

6.1 Problem: Bedrohte Web-Anwendungs- und Serviceebene ... 15

6.2 Lösung: Entkoppelte Web-Sicherheitsarchitektur ... 16

6.3 Sicherheits-Dienstleistungen ... 17

7 Baustein: sicherer Betrieb – Managed Security ... 18

7.1 Problem: Sicherheit braucht durchgehende Kontrolle ... 18

7.2 Lösung: Security Operation Center (SOC) ... 19

7.3 Sicherheits-Dienstleistungen ... 20

8 References ... 21

Abstract

Der Gesetzgeber hat für die Digitalisierung im Gesundheitswesen grünes Licht gegeben. Gesetzliche Ausrichtungen und finanzielle Rahmenbedingungen fordern jetzt eine konkrete Strategie, um das bestehende Gesundheitssystem in eine qualitativ hochwertige, digitale Gesundheitspraxis zu transformieren.

Disruptive Digitalisierungskonzepte in einem kritischen Segment der Gesellschaft gelingen nur im Bündnis mit einer sicherheitszentrischen Transformationsmethodik. Ohne diese Kopplung entstehen weder gesellschaftliches Vertrauen noch eine verlässliche Technologiegrundlage.

Erfolgreiche Cyber-Angriffe kennzeichnen fast täglich methodische Defizite im Sicherheitsdesign bestehender IT-Lösungen und Verfahren. Die gezielte Vermeidung komplexer Software- oder Systemschwachstellen zeigt sich als eine schwer zu beherrschende Herausforderung im digitalen Fertigungsprozess.

Materna ist ein führender Dienstleister bei der Umsetzung ambitionierter Digitalisierungsziele. Wir stellen die Frage nach einem ganzheitlichen Cyber Security Engineering in den Vordergrund. Wie lässt sich ein qualifiziertes Cyber Security Engineering in fachlich orientierte Digitalisierungsprojekte des Gesundheitssystems gezielt einbinden, sodass die Herausbildung von überprüfbaren Sicherheitsstandards nicht als Option, sondern stets als qualifizierende Zielstellung zugesichert werden kann?

1 Materna-Kompetenz

Materna bietet im Bereich Digitale Krankenhausprozesse für Konzeption und Realisierung einer sicherheitsorientierten Digitalisierungsstrategie abgestimmte Sicherheitsbausteine an. Die Sicherheitsbausteine sind eine Antwort auf die Frage, wie die Umsetzung eines kreativen, digitalen Prozess-Designs im Bereich logistischer und administrativer Prozesse sowie integrierter Behandlungs- und Pflegeleistungen konsequent mit einem begleitenden Sicherheitsdesign zusammengelegt werden kann. Materna hebt die übliche Kompetenztrennung zwischen Funktion und Sicherheit mit einem eigenen Strategie- und Methodenansatz für ein Cyber-Security-Engineering auf. Die Ausprägung der Sicherheitsbausteine orientiert sich an einer Systematik, um einen die integrierten Administrations- und Versorgungsprozesse ganzheitlich in einem Krankenhaus digital auszubauen.

Jeder funktionale Transformationsschritt wird mit dem Baustein „strukturierte Sicherheitsanalyse“ verbunden, denn gesetzliche und regulatorische Anforderungen überführen kontinuierlich den fachlichen Diskurs in eine sicherheitsorientierte Betrachtungsform.

Sicherheitsrelevante Prozessziele, wie z. B. die Zurechenbarkeit von Entscheidungen der Leistungserbringer, die Integrität von Behandlungsprotokollen, die Revisionsfähigkeit im Behandlungsablauf, aber auch die Verfügbarkeit von kritischen Anlagen und Systemen fordern eine qualifizierte, strukturierte Methodik für den gesetzten Sicherheitsanspruch.

Bereits an dieser Stelle ist der Baustein „Sicherheitsarchitektur – Sicherheitsentwicklung“ wirksam. Design-Entscheidungen sind gefordert und führen zu einer an den Sicherheitszielen ausgerichteten Sicherheitsarchitektur.

Materna verfolgt eine Asset-ausgerichtete Sicherheitsstrategie. Digitale Informationen, z. B. Leistungsangebote verschiedener Abteilungen oder Befunde von Patienten, transformieren sich zu ökonomischen, sozialen und datenschutzrechtlichen Werten. Der komplexe Prozess ihrer Verteilung und Verarbeitung unterliegt strengen Regularien und wird über den Baustein „gesetzeskonforme Datenverteilung“ abgedeckt.

Der Baustein „Krankenhaus Anwendungsschutz“ unterstützt einen ganzheitlichen Sicherheitsanspruch auf Vertraulichkeit, Verbindlichkeit und Authentizität im externen wie im internen, digitalen Informationsaustausch. Materna stellt mit dem Baustein „sichererer Betrieb – Managed Security“ sowohl betriebliche Instrumente als auch Erfahrungen und Methoden für die Gestaltung eines operativen Sicherheitsmanagements zur Verfügung.

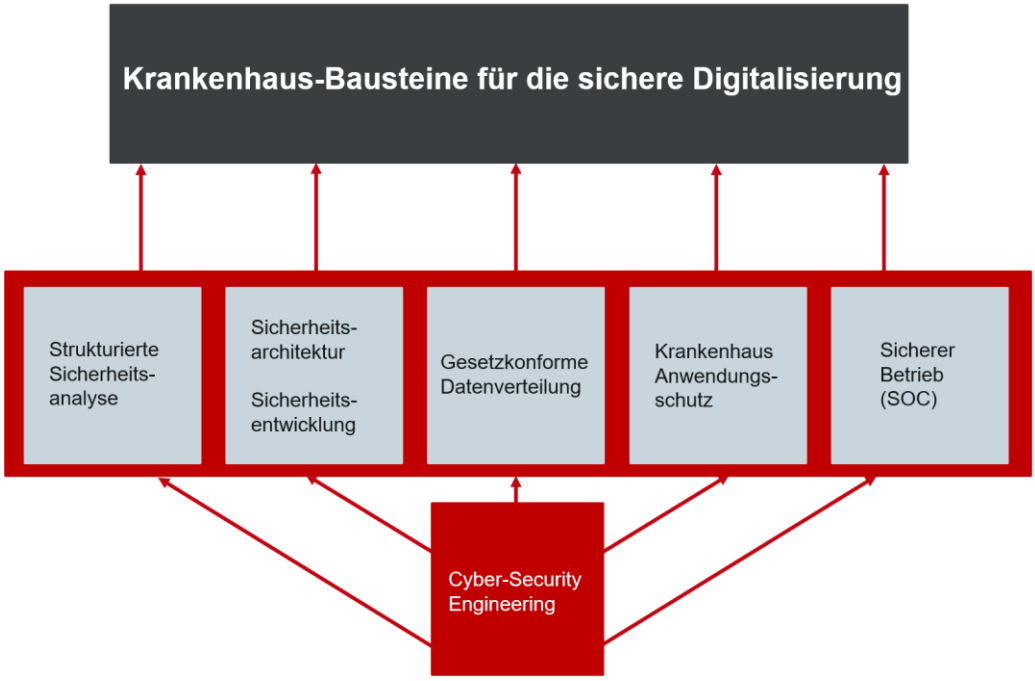

Abbildung 1: Sicherheitsbausteine für Krankenhausprozesse

2 Rahmenbedingungen: regulierte Krankenhaus-Digitalisierung

Das Krankenhauszukunftsgesetz (KHZG) [5] ist Ausgangspunkt zur Entwicklung einer Transformations-Strategie und einer darauf ausgerichteten Transformations-Methodik. Die mit dem Gesetz formulierten Zielstellungen und Aufgaben zur Modernisierung von Krankenhäusern lassen sich ohne eine konkrete Umsetzungsstrategie weder zeitlich, finanziell noch funktional nachvollziehbar abbilden.

Die Komplexität dieser Aufgabenstellung ist hoch und erfordert neben eines medizinischen Fach- und Prozesswissens eine hoch qualifizierte Digitalisierungskompetenz. Der strukturelle Entwurf für eine solche Kompetenz führt in Abbildung 2 zu einem interdisziplinären Transformationsboard. Damit vereinigen sich Kompetenzen im Bereich digitale Technologien und Standards (1) mit Fähigkeiten für ein lösungsorientiertes, jedoch branchenspezifisches Architektur- und Prozessdesign (3). Die konsequente Anwendung von Cyber Security Engineering (2) ist die methodische Antwort auf die in der KHSFV [24, §19, Absatz 10] erhobene Umsetzungspflicht von IT-Sicherheit.

Der hohe Anspruch an die digitale Modernisierung und damit an das Transformationsboard entwickelt sich aus komplexen, technologischen, funktionalen und Sicherheitsanforderungen zur Transformation. Gleichzeitig wirken regulierende Rahmenbedingungen auf die funktionale und sicherheitsrelevante Ausrichtung und verpflichten zu einer durchgehenden Compliance-Zusicherung.

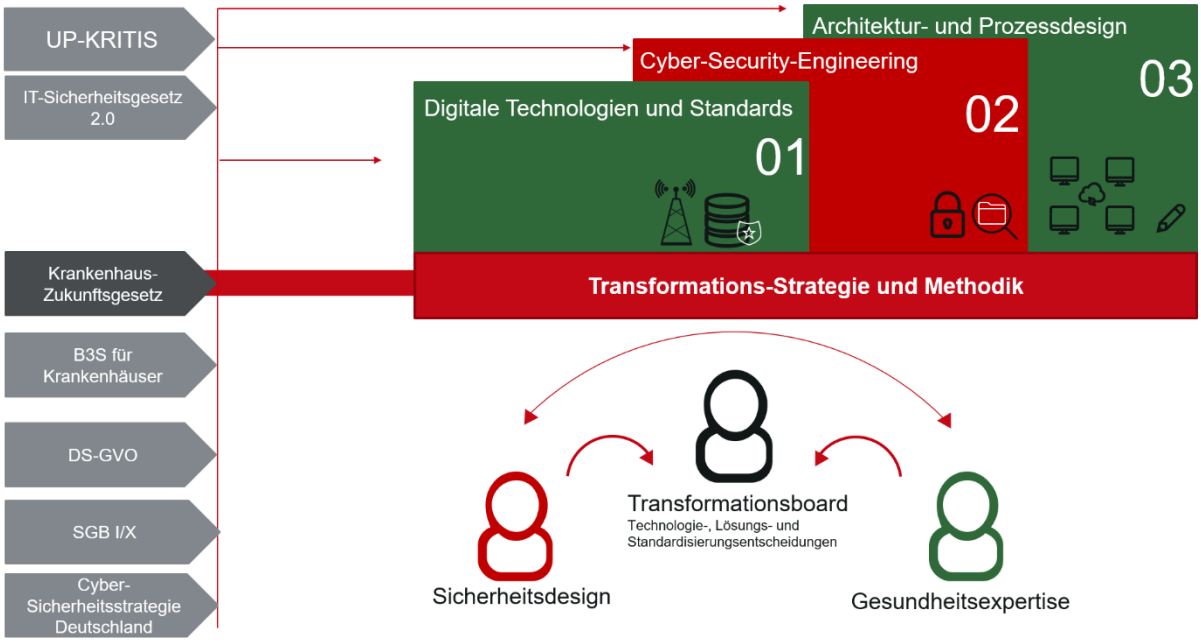

Abbildung 2: Regulative Anforderungen für Krankenhäuser

2.1 Umsetzungsplan KRITIS

Der Umsetzungsplan KRITIS (UP-KRITIS) ist die Initiative zur Zusammenarbeit von Wirtschaft und Staat zum Schutz Kritischer Infrastrukturen in Deutschland. Der Schutz Kritischer Infrastrukturen unterliegt einer nationalen Strategie [27] und bezieht gleichzeitig eine Cyber-Sicherheitsstrategie [13, Handlungsfeld 2] mit ein.

2.2 IT-SiG

Die Kompetenz und die Einflussnahme des BSI wurden mit dem Sicherheitsgesetz gestärkt. Der kooperative Ansatz des UP-KRITIS zum Schutz Kritischer Infrastrukturen wird mit dem IT-Sicherheitsgesetz (IT-SiG) weitergeführt [23].

Mit dem IT-Sicherheitsgesetz liegen Regelungen zur Verbesserung der Verfügbarkeit und Sicherheit der IT-Systeme, speziell im Bereich der Kritischen Infrastrukturen vor.

Wirkungsbereich:

- Technische Anforderungen für BSI-Integration
- Systeme zur Angriffserkennung mit Meldepflicht
- Sicherheitsstandards durch UP-KRITIS

2.3 B3S im Krankenhaus

Die Deutsche Krankenhausgesellschaft hat einen branchenspezifischen Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus herausgegeben. Auf Grundlage des IT-Sicherheitsgesetzes werden mit dem B3S sowohl Methodenbeschreibungen als auch für das Gesundheitssystem zugeschnittene Sicherheitsmaßnahmen vorgelegt.

Der Schwellenwert zur Einstufung als Kritische Infrastruktur wird hier auf 30.000 vollstationäre Behandlungsfälle festgelegt [20, Seite 9].

Wirkungsbereich:

- Maßnahmen zum Design von Sicherheitsarchitekturen
- Prozessmodell für kritische Krankenhaus-Dienstleistungen
- Methodik: Krankenhaus-spezifische Gefährdungsbeschreibungen

2.4 DSGVO

Die DSGVO regelt das Grundrecht von Patienten in Bezug auf ihre Gesundheitsdaten. Patientendaten sind als personenbezogene Daten klassifiziert und unterliegen begründet der Datenschutzverordnung (DSGVO). Rechtmäßigkeit und Zweckbindung sind wesentliche Grundsätze zur Verarbeitung personenbezogener Daten.

Die datenschutzrechtliche Einwilligung des Betroffenen sichert dafür die Rechtmäßigkeit der Verarbeitung [32, Seite 38]. Die DSGVO setzt gleichzeitig Vorschriften zur Anwendung von IT-Sicherheit [14, Art.32].

Wirkungsbereich:

- Anforderungen an eine digitale Willensbekundung
- Prozesse unter Einbeziehung von Betroffenen
- Nachweisgeführte und vertrauliche Datenweitergabe

2.5 SGB I/X

Für Gesundheitsdaten stehen die Bestimmungen der DSGVO im Vordergrund. Darüber hinaus sind die Bestimmungen des SGB I und X zu berücksichtigen und anzuwenden [25].

Mit §38 SGB I wird das Sozialgeheimnis definiert, welches Leistungsträger sicherstellen müssen. Die Sozialdaten im Gesundheitswesen werden im §67 Absatz 2 SGB X definiert und stellen erweiterte Sicherheitsanforderungen im Austausch von Patientendaten zwischen unterschiedlichen verantwortlichen Stellen.

Ein Lösungsansatz zur sicheren Verteilung von Gesundheitsdaten wird in Abschnitt 5 vorgestellt.

3 Baustein: strukturierte Sicherheitsanalyse

3.1 Problem: Sicherheitsbewertung komplexer IT-Systeme

Digitale Systeme für die stationäre Versorgung in einem Krankenhaus bilden eine komplexe IT-Architektur, bestehend aus verschiedenen Technologiebausteinen und Systemkomponenten.

Ein Verbund aus Systemkomponenten realisiert digitale Krankenhaus-Fachanwendungen zur Sicherstellung einer digitalen, stationären Versorgung.

Sensible, medizinische Informationswerte bilden digitale Assets in einem Krankenhaus und durchlaufen in der Verarbeitung einzelne Krankenhaus-Fachanwendungen (Abbildung 3).

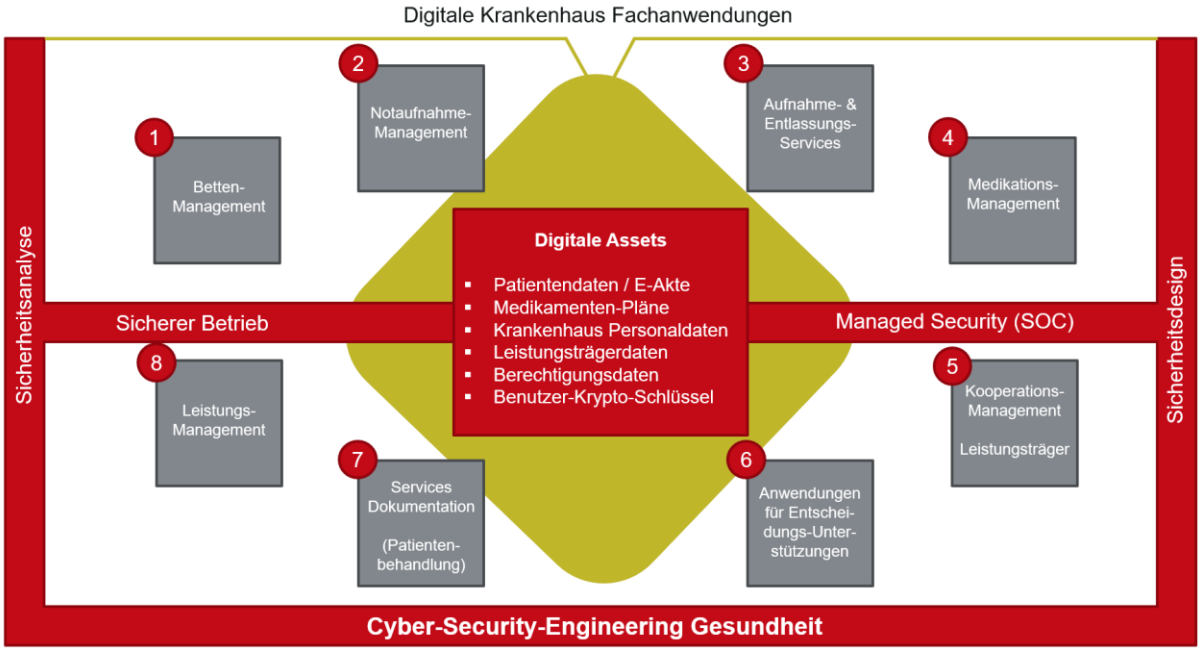

Abbildung 3: Cyber-Security-Engineering Strategie

Über Schnittstellen zur Kopplung einzelner Krankenhaus-Fachanwendungen erfolgt der Informationsaustausch zwischen den Dienstleistungen. Kopplungskonzepte bilden die Grundlage für notwendige kooperative Prozessstrukturen.

Das Kernproblem besteht darin, dass sich ein Sicherheitszustand in gekoppelten und komplexen IT-Architekturen, selbst unter Anwendung von IT-Administrationswerkzeugen, nur schwer oder gar nicht beschreiben lässt.

Für die Ableitung des Sicherheitszustandes sind überprüfbare Zusicherungen aus den Krankenhaus-Fachanwendungen (1)..(8) erforderlich. Zusicherungen darüber, wie und ob eine aufgestellte Sicherheitsstrategie durch angemessene Sicherheitsmaßnahmen die digitalen Assets und IT-Systemressourcen eines Krankenhauses wirksam schützen.

In Abbildung 3 wird deutlich, dass sich eine wirksame IT-Sicherheit auf alle Prozessbereiche erstrecken muss. Das verbindende Element sind zu schützende digitale Assets, denn Kopplungskonzepte öffnen Prozessketten und verteilen diese in alle Bereiche der IT-Architektur eines Krankenhauses.

Wie lässt sich ein Sicherheitszustand strukturiert erfassen und beschreiben? Mit welchen Methoden unterziehen sich einzelne IT-Architektur-Bereiche einer Bewertung?

Gibt es eine strukturierte Vorgehensweise, um Auswirkungen von Sicherheitsdefiziten kontrolliert einzugrenzen?

3.2 Lösung: Architekturbezogene Sicherheitsbewertung

Die Sicherheitsanalyse ist der Bereich im Cyber-Security-Engineering, der Sicherheitsprobleme nach einem methodischen Vorgehen identifiziert. Die Sicherheitsanalyse entwickelt für IT-Architekturbereiche in einem Krankenhaus-System eine begründete Sicht auf eine bestehende Gefährdungssituation.

Aus den Ergebnissen der Analyse leiten sich quantitative und qualitative Beschreibungen über den aktuellen Sicherheitszustand ab.

3.2.1 Methodische Ausrichtung

Für die Entwicklung einer Gefährdungsbeschreibung haben sich unterschiedliche standardisierte und branchenorientierte Vorgehensweisen etabliert (siehe Abbildung 4). Ausgehend von den B3S-Empfehlungen [20] sind in Krankenhaus-Systemen die Methoden nach dem Standard für Sicherheitsmanagement ISO-2700x anzuwenden.

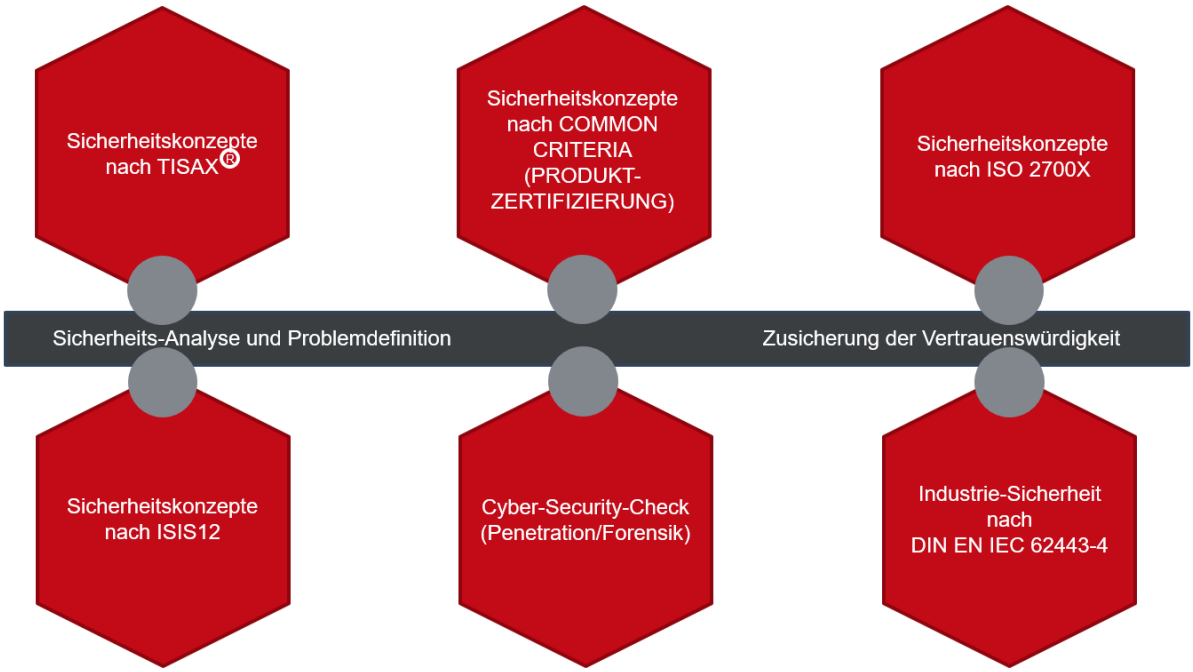

Abbildung 4: Methodenkonzepte – Sicherheitsanalyse

Die Vorgehensweise legt die Grundlage für den Aufbau eines Managements für Informationssicherheit (ISMS), konform zu den Maßnahmen nach ISO 27001 [21]. (Die Zertifizierung nach ISO 27001 ist optional.)

Penetrationsverfahren und forensische Methoden untersuchen IT-Architekturen in Bezug auf bestehende Schwachstellen.

3.2.2 Strukturelle Ausrichtung

Für die Sicherheitsbewertung sind Strukturbereiche des Krankenhauses auszuwählen. Die B3S-Empfehlungen stützen sich dabei auf die DIN-Norm 13080 [16]. Ein Krankenhaus lässt sich darüber mit seinen krankenhausspezifischen Funktionen und Dienstleistungen strukturieren.

Die Versorgungsprozesse (2) in Abbildung 5 erweitert den kritischen Kernprozess (1) um Services, die den Kernprozess einleiten (Aufnahme, Notaufnahme) und um Services, die einen definierten Abschluss bilden (Entlassung, Verteilung).

Die Zielbereiche für eine Sicherheitsanalyse sind mit ihren Einstiegspunkten (1)..(4) hervorgehoben. Die Schnittstellen zu digitalen Ressourcen (3) und zur Telematik-Infrastruktur (4) stellen für den Gesamtprozess unterstützende Dienstleistungen bereit. Die gekennzeichneten Bereiche bilden Sicherheitszonen (Partitionen), die sich separiert und einzeln analysieren lassen.

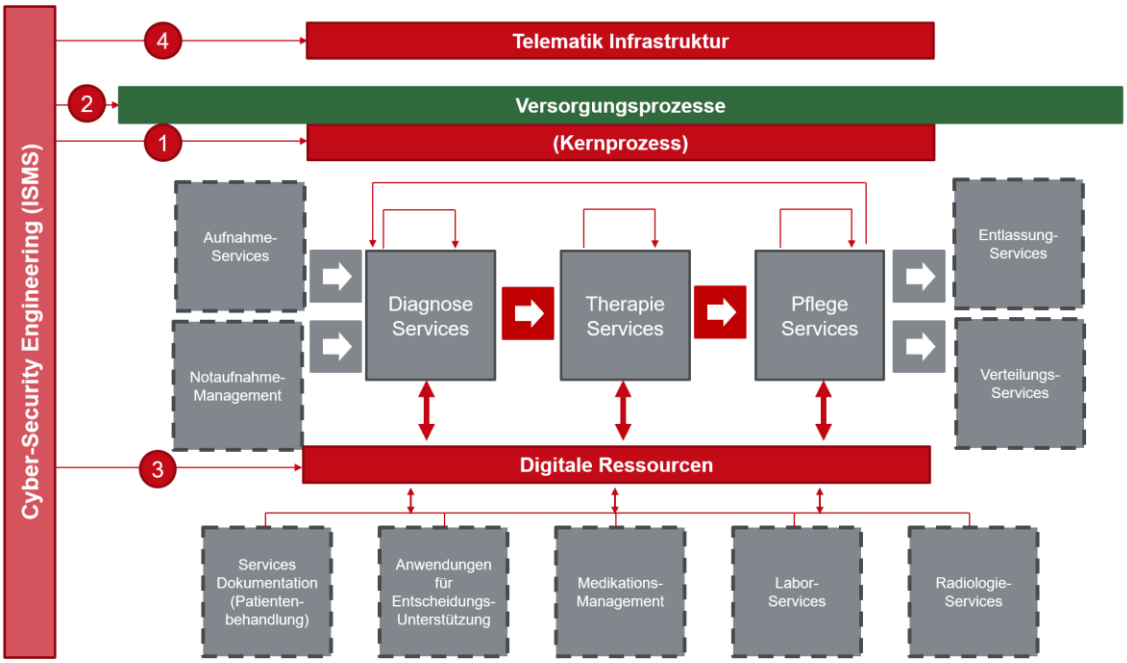

Abbildung 5: Ziele der Sicherheitsanalyse

3.3 Sicherheits-Dienstleistungen

Sicherheitsanalyse: Strukturierte und formalisierte Sicherheitsanalyse von ausgewählten IT-Architekturbereichen nach ISO 27001 Standard. Unterstützung bei der Einführung eines ISMS mit angemessenem Risikomanagementsystem. Erarbeitung von Sicherheitsleitlinien und Sicherheitskonzepten.

BSI-Grundschutz: Strukturierte und formalisierte Sicherheitsanalyse von IT-Architekturbereichen nach BSI-Grundschutz. Struktur- und Schutzbedarfsanalyse, Modellierung von Maßnahmenbausteinen, Basis-Sicherheits-Prüfungen, Realisierungsplanung, Sicherheitsanalyse für hohen Schutzbedarf.

Schwachstellenbewertung: Bewertung der Verletzbarkeit für IT-Systembereiche durch selektive Penetrationsverfahren. Die Untersuchungen richten sich auf verschiedene Ebenen (Netzwerk, Betriebssystem, Fachanwendung) der IT- Infrastruktur. Die Bewertung bestehender Schwachstellen erfolgt im Abgleich mit einer Common-Vulnerabilities and Exposures CVE-Datenbank [12].

Sicherheitszulassung: Bewertung der Vertrauenswürdigkeit von IT-Sicherheitsprodukten nach Common Criteria. Erarbeitung von Zulassungsnachweisen inklusive Security Target. Koordinierung des Zulassungsprozesses mit dem BSI und der entsprechenden Prüfstelle.

Strategie und Transformation: Begleitung von Transformationsprojekten zur Digitalisierung von Krankenhausprozessen. Entwicklung von Sicherheitsstrategien und Ableitung von Sicherheits-Policies. Entwurf von Transformationsmodellen zur technischen und kontrollierten Umsetzung definierter Sicherheitsziele.

4 Baustein: Sicherheitsarchitektur – Sicherheitsentwicklung

4.1 Problem: Softwareentwicklung – Security-By-Design

Die Umsetzung von Informationssicherheit (Cyber Security) als strukturierte Disziplin wird in der gegenwärtigen Digitalisierungs- und speziell in der Entwicklungspraxis oft noch als zusätzliche und herausfordernde Notwendigkeit empfunden. Sicherheitsqualität ist noch nicht überall ein inhärentes Paradigma einer digitalen Entwicklungs- und Fertigungsstrategie.

Der Begriff Security-by-Design formuliert die Forderung, getrennte Betrachtungsweisen über Funktion, Fachverfahren und Geschäftsmodelle auf der einen Seite, sowie Sicherheit und Datenschutz auf der anderen Seite, in ein geschlossenes Praxismodell zu überführen.

In der gültigen Verordnung zur Verwaltung des Strukturfonds im Krankenhausbereich (KHFSV) [24, §19, Absatz 10] wird lösungsübergreifend eine Anforderung nach Informationssicherheit gesetzt. Die Digitalisierung von Verwaltungs- und Behandlungsprozessen ist ohne die Entwicklung einer verteilten Sicherheitsarchitektur nicht zu anzuraten.

In der Software-Entwicklung folgt man bereits ganzheitlichen Vorgehensmodellen wie Scrum [26], Kanban [8], Continuous Delivery bzw. Continuous Deployment (CD) [36]. Jedoch gibt es bis heute keine vergleichbaren Prozesse für eine vollständige Integration der Prinzipien von Cyber Security Engineering in diese Entwicklungsprozesse.

Die Risiken einer solchen Praxis können im Nachhinein zu Qualitäts- und Sicherheitsbewertungsproblemen führen. Das Prinzip zur Verwendung sicherer und vertrauenswürdiger Softwarebausteine ist bereits bei der Beschaffung zu berücksichtigen und setzt sich in der späteren technischen Integration als Teile einer Sicherheitsarchitektur fort.

4.1.1 Schwer nachvollziehbares IT-Architekturdesign

Cyber Security Engineering ist durch einen fortlaufenden Entscheidungsprozess für den Entwurf einer Sicherheitsarchitektur geprägt. Regulative Anforderungen, nicht funktionale Anforderungen, z. B. die Verfügbarkeit, aber auch fachlich definierte Sicherheitsziele konstituieren eine Sicherheitsarchitektur.

Speziell im Krankenhausbereich entwickeln sich IT-Architekturen aus verschiedenen Richtungen. Erst steigende Integrationsanforderungen erhöhen die Priorität für spezifische Sicherheitsanforderungen. Die Komplexität der vollständigen IT-Architektur eines Krankenhauses entzieht sich meist, da in den IT-Projekten eine Sicht auf digitale Einzelaspekte vorherrscht. Idealerweise existiert ein Architektur-Board, mit einem ganzheitlichen Fokus auf die Umsetzung einer Sicherheitsstrategie, gekoppelt an eine fortlaufende Architekturbeschreibung.

Die durch Formalismen künstlich differenzierte Entwicklungspraxis führte zu einem Defizit in der Nachvollziehbarkeit von Architekturentscheidungen. Die fehlende Verknüpfung zwischen einer Sicherheitsstrategie, ihren Sicherheitsanforderungen und dem eigentlichen Architekturdesign ist meist Ursache für IT-Lösungen, deren Funktionen oft noch unzureichende Schutzfunktionen anbieten.

4.1.2 Aufwändige Sicherheitsbewertung

Die Bereitstellung notwendiger Nachweise zur Erlangung einer Sicherheitszulassung ist formal aufwändig, komplex und mit einem hohen Personalaufwand verbunden.

Die Überprüfung und Bewertung durch autorisierte Prüfstellen vollziehen sich als aufwändiger und vergleichender Überprüfungsprozess. Die Bewertungsgrundlage bestimmt sich allein über eine Papierlage und kann sich nicht direkt an einer elektronischen, semantischen Modellgrundlage für die Sicherheitsarchitektur orientieren.

Die Zusicherung von Sicherheitseigenschaften für neue Software-Releases bleibt mit einem schwer zu kalkulierenden formalen Bewertungsaufwand konfrontiert.

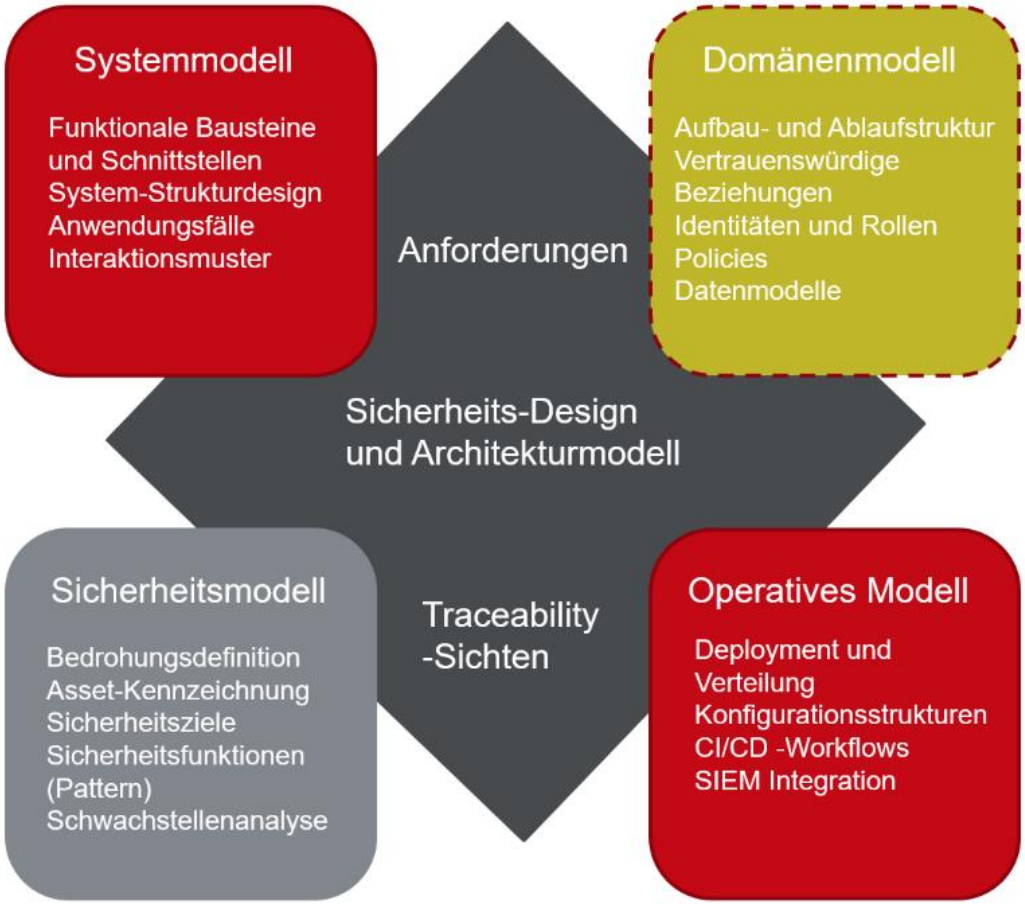

Abbildung 6: Modellbasiertes Architektur- und Lösungsdesign

4.2 Lösung: Strukturiertes Funktions- und Sicherheitsdesign

Materna analysiert in einem ersten Schritt bestehende IT-Architekturen und erstellt dabei eine Art „digitale Bestandsaufnahme“, um erforderliches Wissen über den aktuellen Zustand und geltende operative und regulative Rahmenbedingungen der IT-Architektur ableiten und aufbauen zu können.

Materna repräsentiert und entwickelt modellbasiert Sicherheitsarchitekturen. Modelle sind Abbild der aktuellen und der zu gestaltenden Sicherheitslösung. Ein fest mit dem Modell verankertes Management für Anforderungen [31] legt den Grundstein für das Prinzip begründeter Design-Entscheidungen (Requirement Engineering). Aus begründeten Anforderungen entwickelt sich eine aus verschiedenen Sichten bestehende Sicherheitsarchitektur. Digitalisierungsziele bleiben jederzeit nachvollziehbar:

Domänenmodell: Die Sicht greift fachliche und strukturelle Aspekte einer Krankenhaus-Organisation auf und beschreibt sicherheitsrelevante Beziehungen der Fachebene.

Kernkonzepte (Terminologie), strukturelle Verteilungen (Aufbaustruktur) mit ihren Abgrenzungen und Übergängen, fachliche Rollen für Zuständigkeit, Entscheidungskompetenz und Prozessverantwortung

(Ablaufstruktur) werden formalisiert. Die strukturierte Abbildung von Identitäten, von Policies (Regelwerken) und von Klassifikationen für Datenstrukturen bilden Grundlagen für erste Entwürfe regulierter Prozesse und einer begleitenden Sicherheitsbewertung.

Systemmodell: Im Systemmodell vollzieht sich eine schrittweise und technische Transformation des Domänenmodells in eine konkrete IT-Implementierung. Das Systemmodell entwickelt sich auf Ebene der IT-System-Konzepte.

Bausteinsichten mit ihren Schnittstellen formen eine Spezifikationssicht durch ein interpretierbares Beziehungsmodell. Anwendungsfälle und Interaktionsmuster repräsentieren den Lösungsansatz und stellen die fachlichen Zielstellungen der Sicherheitsarchitektur heraus.

Sicherheitsmodell: Im Sicherheitsmodell fließen über Profilerweiterungen Sicherheitsbegriffe, Beziehungen und Pattern der Informationssicherheit ein [19].

Das Systemmodell wird um eine konkrete Gefährdungsbewertung verlinkt. Die Verknüpfung von Signaturen der Systemschnittstellen mit konkreten Bedrohungen kennzeichnen Sicherheitsprobleme.

Eine systematische Attack-Tree-Analyse [3] visualisiert mögliche Gefährdungsketten über Schnittstellen hierarchischer Systemkomponenten.

Das Sicherheitsmodell beschreibt Sicherheitsziele, Sicherheitsfunktionspattern [17] und setzt Beziehungen zu konkreten Klassen formaler Sicherheitsanforderungen [11].

Operatives Modell: Es liefert eine vollständige Sicht auf die operative, sichere Einsatzumgebung. Das Modell beschreibt vertrauenswürdige Rahmenbedingungen, unter denen eine Sicherheitsarchitektur aufgebaut, konfiguriert und betrieben werden kann.

Im Mittelpunkt stehen Konzepte für eine automatisierte und kryptografisch überprüfbare Sicherheitskonfiguration und für das zyklische Release-Management von Architektur-Bausteinen. Das Modell spezifiziert die Integration in ein ISM-System für Überwachungs- und Steuerungsaufgaben (siehe Abschnitt 7).

4.3 Sicherheits-Dienstleistungen

Requirement Engineering: Für die Entwicklung einer Sicherheitsarchitektur als Sicherheitslösung wird ein durchgehender Prozess zur Anforderungserhebung, Verwaltung und Nachvollziehbarkeit aufgesetzt.

Ein Requirement Engineering sichert in allen Projektphasen eine konsequente Transparenz von Anforderungen für die Entwicklung und für ein begründetes Sicherheitsdesign der Gesamtlösung.

Sicherheitsmodellierung: Die funktionale Modellierung im Bereich der Software- und Architektur-Entwicklung stützt sich auf Standards wie UML [35], SysML [28] und für die Prozessmodellierung auf BPMN [9] und DNN [15].

Sicherheitsorientierte UML-Profile erweitern die funktionale Modellierung um Konzeptklassen für ein Security- Engineering und für die Anwendung kryptografischer Funktionen. Die Methodik ist auf die Entwicklung von Sicherheitsarchitekturen und/oder Produkten mit hohen Sicherheitsanforderungen ausgerichtet.

Zulassungsorientierte Entwicklung: Die Entwicklung von IT-Sicherheitsprodukten mit einer BSI-Zulassung benötigt spezifische Vorgehensweisen für die Sicherheitsarchitekturentwicklung.

Es bestehen Auflagen zur Erzeugung formaler Evaluierungsnachweise (z. B. Entwicklung eines Security Targets [10, Seite 64]). Prozesse zum Nachweis von Sicherheitseigenschaften und einer spezifizierten Testabdeckung erweitern den Gesamtentwicklungsprozess.

Sichere Entwicklung und Awareness: Methoden und Prinzipien zur sicheren Anwendungsentwicklung erhöhen Softwarequalität. Die Prinzipien setzen ein strukturiertes, sicherheitsorientiertes und nachweisgeführtes Vorgehen voraus.

Die Vorgehensweise wird auf konkrete Projekte zur Entwicklung kritischer Lösungen übertragen. Zusätzliche Awareness-Programme dienen der Qualifizierung bestehender Entwicklungsteams.

5 Baustein: gesetzeskonforme Datenverteilung

5.1 Problem: Überlagerte Regulierungsziele

Gesundheitsdaten bilden ein wesentliches digitales Asset im stationären Versorgungsprozess. Gesundheitsdaten fallen prinzipiell in die besondere Kategorie personenbezogener Daten (früher Sensible Daten) [14, Art. 9] und sind in der DSGVO definiert [14, Art. 4].

Die Verteilung medizinischer Daten zwischen Trägern von Sozialleistungen, Leistungserbringern (z. B. Krankenhäuser oder Betreuungseinrichtungen) und niedergelassenen Vertragsärzten führt dazu, dass unterschiedliche gesetzliche Regelungen zum Schutz der Gesundheitsdaten im Gesamtverteilungsprozess berücksichtigt werden müssen.

Mit Art. 20 der DSGVO haben Patienten ein Recht auf Datenübertragbarkeit (z. B. Übermittlung der Daten zu einem anderen Arzt). Diese Regelung steuert eine begründete Weitergabe von Patientendaten durch eine freiwillige Einwilligung des Patienten.

Der Umgang mit personenbezogenen Daten im Rahmen der Sozialverwaltung (Leistungsträger) ist dem Sozialdatenschutz untergeordnet (SGB I, SGB X). Das Sozialdatum zeichnet sich durch einen Personen- und durch einen Sachbezug aus und unterliegt dem Sozialgeheimnis [33, §35 Abs.1].

Gesundheitsdaten der Leistungserbringer unterliegen anderen gesetzlichen Regeln. Auch Behandlungsdaten niedergelassener Ärzte unterliegen nicht dem Sozialdatenschutz, sondern dem Bundesdatenschutzgesetz (BDSG) [4] bzw. der europäischen Datenschutzverordnung (DSGVO).

Im Bereich der Krankenhäuser kommt zum Schutz personenbezogener Daten nicht allgemein das BDSG oder die DSGVO zur Anwendung. In Abhängigkeit vom Rechtsträger oder Bundesland eines Krankenhauses wird das Datenschutzgesetz weiter differenziert.

Handelt es sich um ein kommunales oder universitäres Krankenhaus, müssen entweder das Landeskrankenhausgesetz oder das Landesdatenschutzgesetz herangezogen werden. Mit einer kirchlichen Trägerschaft sind zusätzliche rechtliche Rahmenbedingungen einzubeziehen.

Eine weitere Überlagerung gesetzlicher Regelungen zum Datenschutz entwickelt sich mit der Einführung der elektronischen Patientenakte (ePA-01/2021). Das Patientendaten-Schutz-Gesetz (PDSG) [7] und das Terminservice- und Versorgungsgesetz (TSVG) [6] bilden dafür den gesetzlichen Rahmen.

Die ePA verknüpft digitale Informationen, die während eines Behandlungszeitraumes über Patienten erhoben (z. B. Medikamente, Vorerkrankungen oder Blutwerte) und diesen eindeutig zugeordnet werden. Mit der ePA erfolgt die Dokumentation über Behandlungsplanung, chronologischen Ablauf, medizinische Zuständigkeiten und behandlungsrelevante Entscheidungen.

Die hohe ePA-Akkumulationsdichte an personenbezogenen Daten nach Art.9 der DSGVO setzt eine eigenständige, zugelassene Sicherheits-Architektur zur Verteilung und Zugriffssteuerung auf die Tagesordnung.

5.2 Lösung: Sichere Kooperation mit Gesundheitsdaten

Die Verwaltung und Anwendung gesundheitsbezogener Informationen auf Grundlage von KIS-Systemen oder der ePA erfordert einen sicheren und datenschutzkonformen Informationsaustausch zwischen Leistungserbringern, Leistungsträgern, Pflege- und auch Rehabilitationseinrichtungen.

Die Datenschutzkonformität reduziert sich nicht allein auf Kommunikationstechnologien (z. B. DE-Mail, E-Postbrief, Konnektor-basierte Übertragung), sondern bezieht die fachliche Ebene für Zusammenarbeit mit ein.

5.2.1 Sicherheitsarchitektur

Kooperation und Verteilung: Materna entwickelte bereits für den behördlichen Bereich, in Kooperation mit Sicherheitsfirmen aus dem Hochsicherheitsbereich und dem BSI, eine Sicherheitsarchitektur als Lösung: Sichere E-Akte.

Die Lösung: Sichere E-Akte basiert auf dem Konzeptansatz E-Akte-Sicherheitsraum (siehe Abbildung 7). Der E-Akte-Sicherheitsraum bildet einen separierten und regulierten Informationsraum innerhalb der Telematikinfrastruktur.

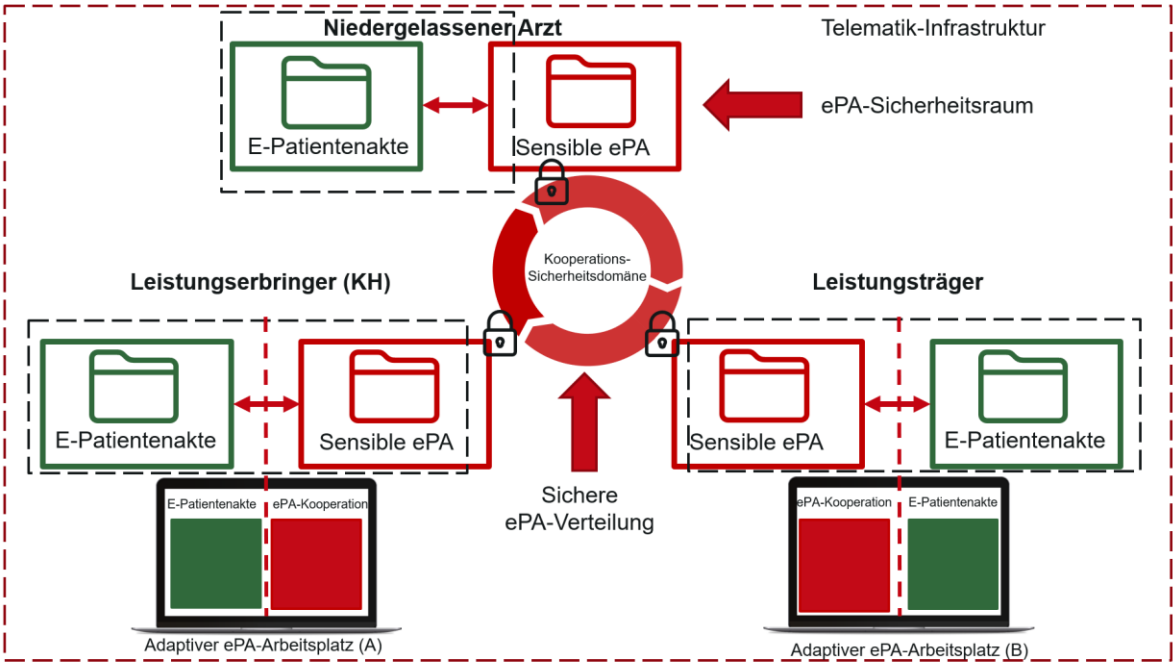

Abbildung 7: Lösung: Sichere ePA-Kooperation

Im Zuge der Verarbeitung sensibler Gesundheitsdaten lassen sich unterschiedliche Sicherheitsbedingungen und Regulierungsanforderungen sicherstellen, die durch ein KIS- oder ePA-System nicht erfüllt werden können.

Der E-Akte-Sicherheitsraum ist eine Integrationslösung und erweitert bestehende Verwaltungssysteme für Gesundheitsdaten um eine zertifizierte Sicherheitsumgebung. Eigene Regelwerke des E-Akte-Sicherheitsraumes steuern die Prozesse zur Kenntnisnahme, Nachweisführung und einer gesicherten, digitalen Zusammenarbeit.

5.2.2 Sicherheitsziele

Die fachliche Zusammenarbeit zwischen verantwortlichen Stellen (Verantwortlicher nach SGB V §307 [1]) unter Verwendung sensibler ePA-Daten erfordert Sicherheitsbedingungen für die interdisziplinäre, gesetzlich verbindliche, nachvollziehbare und geregelte Kooperation.

Folgende Sicherheitsziele sind Grundlage für die Umsetzung unterschiedlicher gesetzlicher Vorgaben:

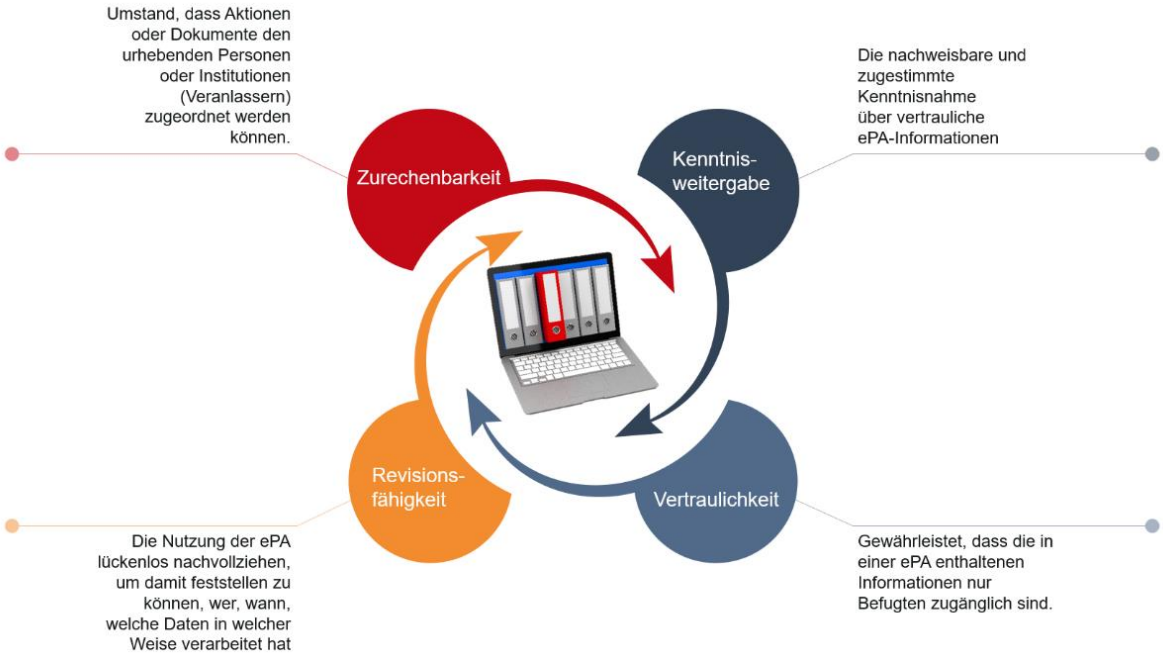

Abbildung 8: Sicherheitsziele für ePA-Prozesse

Verwaltungssysteme für sensible Gesundheitsdaten werden bedarfsorientiert in eine zertifizierte Kooperations-Sicherheitsdomäne eingebunden und erweitern das bestehende Sicherheitsniveau durch Umsetzung der oben genannten Sicherheitsziele.

5.3 Sicherheits-Dienstleistungen

Technische-Integration: Bestehende KIS- und ePA-Systeme sind in eine zertifizierte Verteilungs-Sicherheitsarchitektur einzubinden. Die Verteilung von Gesundheitsdaten kann als Teil eines stationären Versorgungsprozesses (siehe Abbildung 5 – Verteilungs-Service) ausgebaut werden.

Prozess-Integration: Für bestehende KIS- und ePA-Systeme sind Anwendungsfälle zur Einbindung von Verteilungsprozessen zu entwickeln. Die Anwendungsfälle erfüllen dabei Sicherheitsanforderungen für eine revisionsfähige Prozessausführung.

IAM-Verbund: Die Verteilung von Gesundheitsdaten zwischen Verantwortlichen benötigt ein übergreifendes Identity- und Access-Management. Das Konzept IAM-Verbund setzt Grundlagen für die Etablierung vertrauenswürdiger Beziehungen und Verfahren unter Anwendung qualifizierter, digitaler Identitäten.

Sicherheits-Policies: Policies steuern eine gesetzeskonforme Verteilung von Gesundheitsdaten. Der Entwurf von Policies erfolgt in Abstimmung mit den Aufgaben für Leistungsträger, Leistungserbringern bzw. weiteren eingebundenen Verantwortlichen.

Sichere Nachweisführung: Revisionsfähigkeit im Austausch von Gesundheitsdaten benötigt abgesicherte Nachweisprotokolle. Die Nachweisführung wird durch Konzepte zur sicheren Attestierung erweitert.

Sichere Workflows: Es werden Maßnahmen zur sicheren Einbindung von Sicherheits-Policies in Workflows umgesetzt. Im Mittelpunkt steht der Aufbau eines Management-Prozesses für die Konfiguration, Umsetzung und für das Update und den Nachweis sicherer Workflows.

6 Baustein: Krankenhaus Anwendungsschutz

6.1 Problem: Bedrohte Web-Anwendungs- und Serviceebene

Eine große Anzahl zentraler Schnittstellen zur Interaktion mit IT-Systemen eines Krankenhauses basieren auf Web-Technologien. Web-Portale bieten z. B. für unterschiedliche Akteure einen zentralen, personalisierten Zugangspunkt zur Nutzung digitaler Anwendungen eines Krankenhauses (Business-to-Consumer).

Mit nur einem Webbrowser können Benutzer einfach auf Anwendungen bzw. Prozesse des Gesundheitswesens zugreifen, ohne eine Installation spezifischer Client-Programme (z. B. Apps) vornehmen zu müssen.

Auch im Bereich digitaler Verbundkonzepte zwischen Krankenhäusern oder mit anderen digitalen Dienstleistern (Business-to-Business) bilden webbasierte Protokolle und Technologien die kommunikative Grundlage.

Die strukturelle Einbindung und die Positionierung von Web-Anwendungen mit ihren Protokollen in eine IT-Sicherheitsarchitektur bilden die Ursache, dass die häufigsten Cyber-Angriffe erfolgreich auf diese Ebene ausgerichtet sind. Das Sicherheitsproblem entwickelt sich aus den besonderen Prinzipien der Web-Anwendungsebene:

Öffentliche Schnittstellen: Web-Systeme interagieren direkt mit Akteuren der Außenwelt und bieten dafür eine öffentliche Benutzerschnittstelle an. Beliebige Anwender entwickeln dabei unterschiedliche Verhaltensmuster in der direkten Kommunikation mit offenen Web-Benutzerschnittstellen.

Offene Service Ports: Der Schutz der Web-Anwendungsebene kann nicht mit zentralen Sicherheitsinstrumenten erfolgen, die für die Netzwerksicherheit (z. B. Firewall, VLAN-Sicherheit, VPN) vorgesehen sind. Eine Firewall z. B. öffnet standardmäßig Serviceports für webbasierte Protokolle (z. B. Port 80, Port 443).

Auch die kryptographische Absicherung der HTTP-Kommunikation über ein TLS/SSL-Protokoll [34] (https), z. B. unter Anwendung von X.509 Zertifikaten [22], hat nur begrenzten Einfluss auf die Sicherheit von Funktionen und Daten einer Web-Anwendung.

Mehrstufige Sicherheit: Das Sicherheitsniveau einer Web-Anwendung wird allein durch ihr eigenes und ganzheitliches Sicherheitsdesign bestimmt.

Die Umsetzung von Sicherheitszielen in Web-Anwendungen ist mehrstufig und komplex (siehe dazu OWASP TOP 10 [30]). Entwickler benötigen ein umfassendes Sicherheitsbewusstsein und eine qualifizierte Entwicklungsmethodik nach dem Prinzip Security-by-Design.

Nicht-vertrauenswürdige Arbeitsplätze: Das Sicherheitsniveau von Computersystemen der Endanwender, inklusive ihrer Betriebssysteme, Anwendungen und Webbrowser ist aus Sicht eines Krankenhauses nur begrenzt bestimmbar.

Arbeitsplatzsysteme, die nicht unter dem Sicherheitsmanagement eines Krankenhauses verwaltet werden, müssen grundsätzlich als unsicher eingestuft werden und stellen ein Bedrohungspotenzial dar.

6.2 Lösung: Entkoppelte Web-Sicherheitsarchitektur

Materna konzipiert und betreibt eine geschlossene Web-Sicherheits-Infrastrukturlösung (siehe Abbildung 9), um das komplexe Thema Cyber-Security aus fachlichen Web-Verfahren herauszulösen.

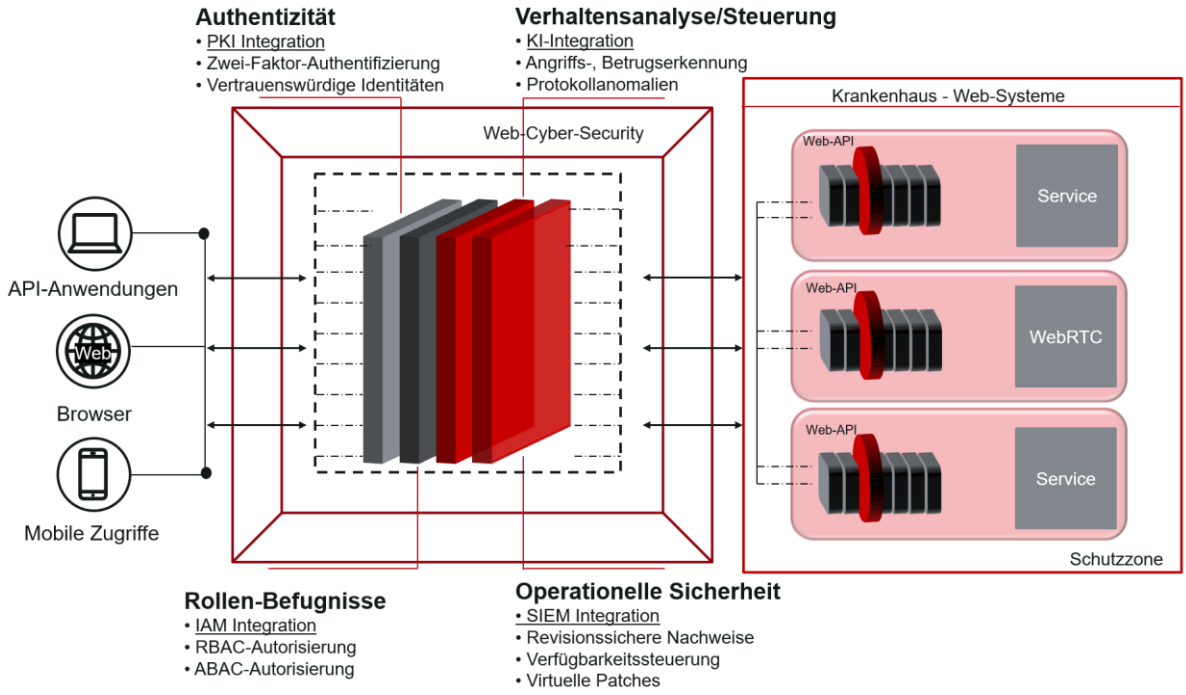

Abbildung 9: Web-basierte Sicherheitsstrategie

Die architekturelle Entkopplung von Cyber-Security bietet ein modulares, mehrstufiges Sicherheitskonzept zur Durchsetzung verschiedener Sicherheitsziele an. Jedes Sicherheitsmodul stellt sich als Integrationsansatz mit ergänzenden Sicherheitstechnologien dar.

Kritische Web-Anwendungen sind nicht mehr direkt mit den Interaktionen aus einer nicht-vertrauenswürdigen Umgebung konfrontiert.

Web-Schutzzonen: Die vorgestellte Web-Sicherheitsarchitektur bietet Kontrollinstrumente für die bedarfsgerechte Gestaltung eines Web-Sicherheitsniveaus. Die Separierung schafft Krankenhaus-Schutzzonen und gewährleistet die Aufteilung in differenzierte Zuständigkeiten für Web-Anwendungssicherheit.

Verhaltensanalyse: Herzstück der Analyse bildet die Integration einer KI-basierten Protokollanalyse. Das Benutzerverhalten mit Anwendungssystemen innerhalb der Krankenhaus-Schutzzone wird kontinuierlich beobachtet.

Unter Echtzeitbedingungen analysiert ein Pattern-definiertes Regelwerk ausgewählte Datenprotokolle nach bekannten Angriffsmustern. Konkrete Muster triggern Abwehrmechanismen und protokollieren das Verhalten.

Verhaltenssteuerung: Während der Analyse lassen sich Protokollinformationen gezielt verändern (z. B. Header-Umschreibungen) bzw. für spezifische Web-Ressourcen anpassen.

Es stehen Methoden zur Behebung bekannter Anwendungs-Schwachstellen zur Verfügung (Virtual Patches), ohne einen Bugfix direkt an der Web-Anwendung vornehmen zu müssen.

Authentizität: Die Überprüfung vertrauenswürdiger Identitäten von Web-Benutzern erfolgt im Zusammenspiel mit einer PKI-Integration. Eine Sicherheitspolicy regelt die Authentifizierungsstärke für

Benutzer/Benutzergruppen in Abhängigkeit von der Sicherheitsklassifikation der zugeordneten Web-Anwendung.

Das Management vertrauenswürdiger Identitäten bestimmt das Sicherheitsniveau aller nachgeordneten Sicherheitsmechanismen.

Rollen und Befugnisse: Das Berechtigungsmanagement verlangt ein integratives Zusammenspiel von Cyber Security Engineering und technologischer Fachkompetenz und verteilt sich auf beide Bereiche.

Im Kern erfolgt die Berechtigungssteuerung über ein integriertes RBAC-Sicherheitsmodell (Role-Base-Access-Control) [18].

Operationelle Sicherheit: Der Schutz von Web-Ressourcen benötigt Instrumente zur Überwachung der Verfügbarkeit, Performance, Auslastung und Lastverteilung (siehe Abschnitt 7-B – SIEM Integration).

Die operationelle Sicherheit steuert z. B. gezielt die Abwehr von DoS-Attacken (Denial of Service), um eine geforderte Verfügbarkeit der medizinischen Produktivsysteme zu garantieren.

6.3 Sicherheits-Dienstleistungen

Web-Sicherheitskonzept: Für Web-Anwendungen werden die Sicherheitsziele definiert. Als Orientierung dienen die Grundsätze der OWASP [29] zur sicheren Entwicklung und Zertifizierung von Web-Anwendungssystemen. Das Sicherheitskonzept beschreibt Verfahren zur Sicherstellung der Verfügbarkeit und der Lastverteilung.

Sicherheitspolicies: Policies enthalten Regeln zur Steuerung des Interaktionsverhaltens zwischen Web-Akteuren und den Krankenhaus Web-Anwendungen. Sicherheitspolicies bilden die Grundlage für eine spätere System-Akkreditierung.

IAM-Integration: Zentrale Verfahren für eine Mehrfaktor-Authentifizierung benötigen ein technisches Integrationskonzept. Ein erweitertes PKI-Integrationskonzept unterstützt Prozesse für das Management vertrauenswürdiger Identitäten.

Autorisierung: Für Krankenhaus Web-Anwendungen lassen sich Anwenderbefugnisse über ein verteiltes Rollen- und Berechtigungsmanagement prüfen und freigeben. Die Autorisierung ist Teil einer zentralen Sicherheitspolicy.

SSO-Verfahren: Über Schnittstellen und Credential-Verteilungskonzepte verbinden sich Web-Anwendungen der Krankenhaus-Schutzzone transparent mit der zentralen Web-Sicherheitsarchitektur. Web-Anwender müssen sich nicht mehrfach authentisieren (Single-Sign-On).

Inbetriebnahme: Die Web-Sicherheitsarchitektur wird mit allen erforderlichen Schnittstellen konzipiert, integriert und in Betrieb genommen. Testprozesse aus der Konzeptionsphase steuern die Inbetriebnahmephase.

7 Baustein: sicherer Betrieb – Managed Security

7.1 Problem: Sicherheit braucht durchgehende Kontrolle

Sicherheitsrelevante Prozesse in einem Krankenhaus sind fest an ein operatives und zuverlässiges Umsetzungskonzept gebunden. Der hohe Stellenwert an ein funktionierendes Informations-Sicherheitsmanagementsystem (ISMS) entwickelt sich durch die folgenden Anforderungen:

Sicherheitsstrategie: Für die IT-Infrastruktur eines Krankenhauses sind eine durchgehende Sicherheitsstrategie umzusetzen und der operative Betrieb zu gewährleisten. Die Sicherheitsziele sind Ergebnis einer durchgehenden Sicherheitsanalyse (siehe Baustein „strukturierte Sicherheitsanalyse“ in Abschnitt 3).

Operative Managementfunktionen für ein Life-Cycle-Sicherheitsmanagement sind erforderlich. Beispiele sind:

- Identity und kryptografisches Credential-Management
- Sicherheitskonfiguration
- Deployment-Management (Continuous Deployment)
- Software-Überprüfung, Freigabe und Update (Continuous Integration, Continuous Delivery)
- Datensicherheits- und Policy-Management
- Nachweisführung und Monitoring.

Die Sicherheitsstrategie ist Ausgangspunkt zur Planung und Entwicklung notwendiger Prozesse zur Aufrechterhaltung betrieblicher digitaler Prozesse (Business Continuity Management). Im Fall, dass die Verfügbarkeit sicherheitsrelevanter Ressourcen nicht gewährleistet ist, sind Strategien zur Behebung solcher Ereignisse vorzubereiten (Disaster Recovery Plan).

Der Umfang der Maßnahmen sollte die vollständige IT-Infrastruktur eines Krankenhauses einbeziehen. Ziel ist es, unter Echtzeitbedingungen eine Bilanz über den aktuellen Betriebs- und Sicherheitsstatus vornehmen zu können.

Sicherheitsbeobachtung: Eine Krankenhaus-Sicherheitsarchitektur besitzt Schnittstellen zur Außenwelt. Die Wirksamkeit von bestehenden Sicherheitsmaßnahmen in Konfrontation mit äußeren und inneren Bedrohungen ist auszuweisen.

Nicht bekannte Systemschwachstellen können zu Sicherheitsvorfällen führen. Ziel ist es, frühzeitig die Kenntnis über Verletzungen eines gesetzten Sicherheitsstatus zu erhalten und mit einer angemessenen Handlungsstrategie (Incident Management) mögliche Auswirkungen zu beheben.

Koordinierte und gesetzeskonforme Prozessstrukturen sind als kontrollierte Reaktion darauf zu aktivieren (Incident Response) und nachzuweisen.

Gesetzliche Meldepflicht: Mit dem IT-Sicherheitsgesetz (siehe Abschnitt 2-B) besteht eine unternehmerische Vorsorgepflicht. Der Betrieb von Technologien zur Erkennung von Sicherheitsvorfällen ist für kritische Infrastrukturen vorgeschrieben.

Sicherheitsvorfälle sind an das BSI zu melden. Dazu ist eine technische und abgesicherte Integration von IT-Systemen zur Sicherheitsbeobachtung mit Infrastrukturen des BSI zur Sammlung und Auswertung von Sicherheitsvorfällen erforderlich.

7.2 Lösung: Security Operation Center (SOC)

Materna unterstützt mit einem Leitstand für Cyber-Security (siehe Abbildung 10) den operativen Betrieb kritischer Infrastrukturen zur Durchsetzung und Einhaltung gesetzter Sicherheitsziele.

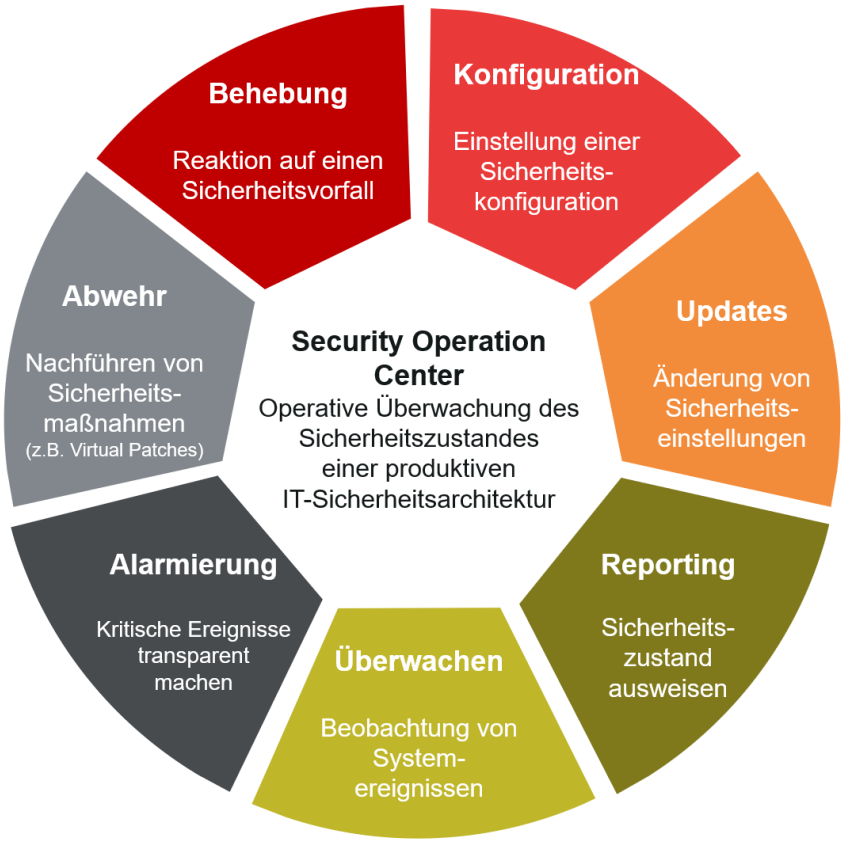

Abbildung 10: Aufgaben Cyber-Sicherheitsleitstelle

Herzstück der Cyber-Security-Leitstelle für das Sicherheitsmanagement bildet ein SIEM-System (Security-Information-Event-Management).

Die SIEM-Integration stellt Funktionen bereit, um unter Echtzeitbedingungen Ereignisse an den Schnittstellen des zu überwachenden IT-Systems (Target-System) vollständig zu erfassen, zu beobachten, zu bewerten und im Bedarfsfall entsprechend beeinflussen zu können.

Konfiguration: Die Sicherheitskonfiguration initialisiert ein Target-System und definiert einen Sicherheitszustand. In der Sicherheitskonfiguration befinden sich z. B. Identitätsdaten mit zugehörigen Credentials, Zugriffskontrollinformationen oder Sicherheitsparametern.

Updates: Änderungen an den Sicherheitseigenschaften unterliegen einer eigenen Sicherheitspolicy. Der Systemzustand des Target-Systems wird zielgerichtet verändert.

Beispiele für Updates sind der Austausch von Benutzer-Zertifikaten oder die Anpassung von Zugriffsberechtigungen von Systemrollen.

Reporting: Die Nachweisführung ist ein vertrauenswürdiger Hintergrundprozess, der die Anwendung von Sicherheitsfunktionen im Target-System überwacht und die Ergebnisse qualifiziert protokolliert. Qualifiziert bedeutet, dass sich die Authentizität der Protokolldaten bestimmen lässt, um den aktuellen Systemzustand des Target-System ausweisen zu können.

Überwachen: Die Schnittstellen des Target-Systems mit der Außenwelt unterliegen einer kontinuierlichen Interaktion mit externen Entitäten. Ereignisse lassen sich im Vorfeld filtern und kategorisieren. Die Ereignismengen werden mit gesetzten Soll-Ereignissen unter Echtzeitbedingungen verglichen.

Alarmierung: Vergleichende Prozesse kennzeichnen Abweichungen des Systemverhaltens mit der Außenwelt. Je nach Art des Sicherheitsereignisses reagiert das Target-System angemessen.

Das Auftreten von Sicherheitsereignissen führt in der Cyber-Sicherheitsleitstelle zur internen Kennzeichnung und Signalisierung.

Abwehr: Eine sich ändernde Bedrohungssituation führt zur Suche nach angemessenen Gegenmaßnahmen, um der zunehmenden Gefährdung des Target-Systems kontrolliert entgegenzuwirken. Ein Aufkommen spezifischer Web-Attacken lässt sich durch das Einspielen von Virtual Patches dynamisch unterbinden.

Behebung: Sicherheitsvorfälle (Security Incidents) erfordern eine Bewertung und die Aktivierung gezielter Behebungsoperationen (Incident Responses). Ziel ist, den Schaden festzustellen und das Target-System in einen stabilen Sicherheitszustand zu überführen.

7.3 Sicherheits-Dienstleistungen

SOC Integration: Planung und technische Konzeption für den Aufbau eines Leitstandes für Cyber-Security. Die Konzeption umfasst Integrationskonzepte zur Einbindung von Teilen der IT-Architektur eines Krankenhauses.

SOC Aufbau und Implementierung: Aufbau und Konfiguration einer ausgewählten SOC-Plattform. Umsetzung von technischen Integrationskonzepten auf Grundlage einer bestehenden SOC-Konzeption.

SIEM-Beratung: Die Einführung eines SIEM erfordert Erfahrungen im Bereich der Beobachtung, Angriffs-Erkennung, Abwehr und Analyse in einem strukturierten Vorgehen. Die SIEM-Beratung erhebt Anforderungen für einen effektiven SIEM-Einsatz zur Abbildung eines Sicherheitszustandes bzw. einer bestehenden Gefährdungssituation.

Incident Response: Die Reaktion auf Sicherheitsvorfälle muss strukturell geplant werden (z. B. Bildung von Incident Response Teams). Maßnahmenpläne sind zu erarbeiten und zu erproben. Im Ergebnis stehen Handlungsmuster und Konzepte zur Nachweisführung zur Verfügung.

Konfiguration von Angriffsmustern: Planung und Einrichtung von Systemen für Intrusion Detection (IDS) oder Intrusion Prevention (IPS). Die Konfiguration umfasst Strukturen zur Angriffserkennung und für IPS als Maßnahmen zur Abwehr. Die Konfigurationen sind Teil einer Sicherheitspolicy.

Analytik-Konzeption: Zur Auswertung gesammelter Informationen (Ereignisse) sind Analytik-Konzepte erforderlich. Entwicklung zugeschnittener Darstellungen, um sicherheitsrelevante Aussagen über das Interaktionsverhalten mit ausgewählten IT-Architektur-Bereichen treffen zu können. Die Analyse erfolgt mit KI-Elementen unter verschiedenen Aspekten: Was hat sich ereignet? Warum konnte es sich ereignen? Was kann sich ereignen? Was muss sich ereignen?

8 References

[1] §307 SGB5-Datenschutzrechtliche Verantwortlichkeiten. URL: https://www.gesetze-im-internet.de/sgb_5/307.html

[2] §341 SGB 5 - Elektronische Patientenakte. URL: https://www.gesetze-im-internet.de/sgb_5/341.html

[3] Academic: Attack Trees - Schneier on Security. URL: https://www.schneier.com/academic/archives/1999/12/attack_trees.html

[4] Bundesdatenschutzgesetz. URL: https://www.gesetze-im-internet.de/bdsg_2018/

[5] Bundesgesundheitsministerium. Krankenhauszukunftsgesetz (KHZG). 2021. URL: https://www.bundesgesundheitsministerium.de/krankenhauszukunftsgesetz.html

[6] Bundesgesundheitsministerium. Terminservice- und Versorgungsgesetz. 2021. URL: https://www.bundesgesundheitsministerium.de/terminservice-und-versorgungsgesetz.html

[7] Deutscher Bundestag. “Patientendaten-Schutz-Gesetz – PDSG: Entwurf eines Gesetzes zum Schutz elektronischer Patientendaten in der Telematikinfrastruktur”. In: (2020). URL: https://www.bundesgesundheitsministerium.de/fileadmin/Dateien/3_Downloads/Gesetze_und_Verordnungen/GuV/P/PDSG-Bundestag_Drs-18793.pdf

[8] Mike Burrows. Kanban: Verstehen, einführen, anwenden. 1. Aufl. s.l.: dpunkt, 2015. ISBN: 978-3-86490- 253-6. URL: http://gbv.eblib.com/patron/FullRecordaspx?p=4350075

[9] Business Process Model and Notation Specification Version 2.0.2. 2014. URL: https://www.omg.org/spec/BPMN

[10] Common Criteria. “Part 1: Introduction and general model: Common Criteriafor Information Technology Security Evaluation”. In: 2017 (). URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf

[11] Common Criteria. “Part 2: Security functional components: Common Criteriafor Information Technology Security Evaluation”. In: (). URL: https://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf

[12] CVE: Common Vulnerabilities and Exposure. URL: https://cve.mitre.org/

[13] “Cyber-Sicherheitsstrategie für Deutschland”. In: Bundesministerium des Innern, für Bau und Heimat 2017 (). URL: https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/cyber-sicherheitsstrategie/cyber-sicherheitsstrategie-node.html

[14] Datenschutz-Grundverordnung. DatenschutzGrundverordnung: DSGVO als übersichtliche Seite. URL: https://dsgvo-gesetz.de/

[15] Decision Model and Notation Specification Version 1.3.2021. URL: https://www.omg.org/spec/DMN/

[16] DIN 13080: Gliederung des Krankenhauses in Funktionsbereiche und Funktionsstellen. URL: https://www.din.de/de/mitwirken/normenausschuesse/nabau/veroeffentlichungen/wdc-beuth:din21:252635669

[17] Eduardo B. Fernandez. Security patterns in practice: Designing secure architectures using software patterns. 1. ed. Wiley Software Patterns Series. Chichester: Wiley, 2013. ISBN: 9781119970484. URL: http://proquest.safaribooksonline.com/9781119970484

[18] David Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli. Role-based access control. Artech House computer security series. Boston: Artech House, 2003. ISBN: 1580533701. URL: http://search.ebscohostcom/login.aspx?direct=true&scope=site&db=nlebk&db=nlabk&AN=87740

[19] Felix Freiling et al. “Technische Sicherheit und Informationssicherheit”. In: Informatik-Spektrum 37.1 (2014), pp. 14–24. ISSN: 0170-6012. DOI: 10.1007/s00287-013-0748-2. URL: https://fb-sicherheit.gi.de/fileadmin/FB/SICHERHEIT/AKBegriffsbildungIS-1-2014.pdf

[20] Informationssicherheit im Krankenhaus | Deutsche Krankenhausgesellschaft e. V. 2019. URL: https://www.dkgev.de/fileadmin/default/Mediapool/2_Themen/2.1_Digitalisierung_Daten/2.1.4._IT-Sicherheit_und_technischer_Datenschutz/2.1.4.1._IT-Sicherheit_im_Krankenhaus/B3S_KH_v1.1_8a_geprueft.pdf

[21] ISO. ISO/IEC 27001:2013. URL: https://www.iso.org/standard/54534.html

[22] ISO. ISO/IEC 9594-8:2017. URL: https://www.iso.org/standard/72557.html

[23] "Kabinettfassung des IT-Sicherheitsgesetzes 2.0". In: (). URL: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/it-sicherheitsgesetz.pdf;jsessionid=4508159A8688D085AB7CE5E543D1793D.1_cid364?blob=publicationFile&v=2 (visited on)

[24] KHSFV - Verordnung zur Verwaltung des Strukturfonds im Krankenhausbereich. 2015. URL: https://www.gesetze-im-internet.de/khsfv/BJNR235000015.html

[25] Dennis-Kenji Kipker and Friederike Voskamp, eds. Sozialdatenschutzrecht in der Praxis. 1. Auflage. Baden-Baden: Nomos, 2021. ISBN: 9783848758432.

[26] Don McGreal and Ralph Jocham. The professional product owner: Leveraging Scrum as a competitive advantage. The professional scrum series. Boston, Amsterdam, and London: Addison-Wesley, 2018. ISBN: 0134686470

[27] "Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie)". In: Bundesministerium des Innern, für Bau und Heimat 2017 (). URL: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/bevoelkerungsschutz/kritis.html

[28] OMG System Modeling Language Specification Version 1.6. 2019. URL: https://www.omg.org/spec/SysML/1.6/

[29] OWASP Security Knowledge Framework. URL: https://owasp.org/www-project-security-knowledge-framework/

[30] OWASP Top Ten Web Application Security Risks | OWASP. URL: https://owasp.org/www-project-top-ten/

[31] Klaus Pohl and Chris Rupp. Basiswissen Requirements Engineering: Aus- und Weiterbildung nach IREB-Standard zum Certified Professional for Requirements Engineering : foundation level nach IREB-Standard. 4., überarbeitete Auflage. Heidelberg: dpunkt, 2015. ISBN: 9783864902833. URL: https://ebookcentral.proquest.com/lib/subhh/detail.action?docID=2029882

[32] Andreas Sachs, Thomas Kranig, and Markus Gierschmann. Datenschutz-Compliance nach der DSGVO: Handlungshilfe für Verantwortliche inklusive Prüffragen für Aufsichtsbehörden. Unternehmen und Wirtschaft. Köln: Bundesanzeiger Verlag, 2017. ISBN: 9783846207604

[33] SGB I Sozialgesetzbuch - SGB I Allgemeiner Teil. URL: https://www.sozialgesetzbuch-sgb.de/sgbi/1.html

[34] Tools.ietf.org, Rfcmarkup Version 1.129d On. RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3. URL: https://tools.ietf.org/html/rfc8446

[35] Unified Modeling Language Specification Version 2.5.1 2017. URL: https://www.omg.org/spec/UML/

[36] Was ist CI/CD? 2021. URL: https://www.redhat.com/de/topics/devops/what-is-ci-cd

MATERNA
Information & Communications

marketing@materna.de
www.materna.de

© Materna 2021