Arbeitshilfe zur Umsetzung der „BSI Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ (OH SzA) in der Branche medizinische Versorgung

Motivation

Die „BSI Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung“ (OH SzA), wurde durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) am 29.09.2022[1] in der Version 1.0 veröffentlicht. Dieses Veröffentlichungsdatum von konkreten BSI-Umsetzungsanforderungen gemäß §8a Absatz 1a BSI-Gesetz (BSIG) ist aufgrund der im BSIG festgeschriebenen Terminvorgabe zur Umsetzung bis zum 01.05.2023 eine erhebliche Herausforderung für die Branche „medizinische Versorgung“. Vor dem Hintergrund der Komplexität des vom BSI in der OH SzA geforderten Angriffserkennungsverfahrens und z. B. einzuhaltenden Ausschreibungsfristen bei entsprechenden Beschaffungsprozessen, ist es sehr unwahrscheinlich, dass die betroffene KRITIS-Betreiber in der stationären medizinischen Versorgung in der Zeit von der Veröffentlichung der OH SzA bis zum geforderten Umsetzungstermin alle Kriterien für den vom BSI geforderten SzA-Reifegrad der Stufe „3“ erreichen können. Dies wurde bereits in der Stellungnahme des BAK zum Entwurf der BSI Orientierungshilfe zum Einsatz von Systemen zur Angriffserkennung deutlich dargestellt.

Die OH SzA wurde zudem mit der Perspektive einer übergreifenden Orientierungshilfe für alle KRITIS-Sektoren/Branchen geschrieben. Eine Differenzierung nach den Spezifika der einzelnen Branchen ist bisher nicht erfolgt. Im Ergebnis eines mehrmonatigen Abstimmungsprozesses zwischen Deutscher Krankenhausgesellschaft (DKG, Herausgeber des Branchenspezifischen Sicherheitsstandard), Vertretern des Branchenarbeitskreises (BAK) „Medizinische Versorgung“ und BSI wurden die Anforderungen der OH SzA in Bezug auf die Branche „Medizinische Versorgung“ in den Branchenspezifischer Sicherheitsstandard (B3S) Version 1.2 überführt. Mit Blick auf die erfolgte Eignungsfeststellung des B3S besteht damit die Gewissheit, dass mit der Umsetzung des B3S in der Version 1.2 auch die in der OH SzA definierten Anforderungen vollständig abgebildet werden.

Diese Anforderungen können darüber hinaus auch von Krankenhäusern aufgegriffen werden, die keine kritische Infrastruktur i. S. d. § 8a BSIG sind, jedoch auf Basis der Anforderungen des § 75c SGB V angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen haben. Aktuell ist eine Überarbeitung der hierfür bereitgestellten Arbeitshilfen der DKG in Vorbereitung.

Die vorliegende Arbeitshilfe des BAK „Medizinische Versorgung“ basiert auf dem zum Zeitpunkt der Veröffentlichung aktuellen Stand der Technik und soll Krankenhäusern, insbesondere für die Nachweisphase gemäß § 8a BSIG, im Jahr 2023 eine Hilfestellung bei der konkreten Umsetzung dieser neuen Anforderungen geben. Auch „Prüfenden Stellen“ (Audit-Teams) kann das vorliegende Dokument in Bezug auf ein Einführungskonzept der „Systeme für Angriffserkennung“ eine Orientierung bei der Bewertung der Umsetzung der entsprechenden Anforderungen geben.

Für die kommende Überarbeitung des B3S zu einer Version 2.0 soll im Rahmen einer wissenschaftlichen Begleitung eine umfangreiche Analyse der sich stetig weiterentwickelnden Systeme zur Angriffserkennung im Krankenhausumfeld erfolgen. Die vorliegende Arbeitshilfe soll dann entsprechend angepasst werden.

[1] Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/oh-sza.html (Eing. 16.3.2023)

Rechtlicher Rahmen nach § 8a BSI-Gesetz

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei soll der Stand der Technik eingehalten werden. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.[2]

(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend.[3]

Nicht-KRITIS-Krankenhäuser müssen diesen gesetzlichen Vorgaben bisher noch nicht folgen, sollten aber auf die Verschärfung der rechtlichen Anforderungen, nach „EU NIS-Richtlinie 2.0“ und „EU Cyber Resilience Act“ vorbereitet sein. Zudem sollten sie vorbereitet sein, wenn sich die Fallzahlen eines Krankenhauses in der Nähe des Schwellenwertes nach KritisV bewegen.

Bewertung der OH SzA

Die grundsätzlichen Anforderungsschwerpunkte der OH SzA lassen sich wie folgt zusammenfassen:

1. Es wird ein umfassendes „Angriffserkennungsmanagementsystem“ angestrebt, welches die organisatorischen und technischen Maßnahmen und somit eine Kern-ISMS mit der technischen Systemunterfütterung aus der Perspektive „Detection/Response“ umfasst. Die OH SzA gibt grundsätzlich keinen verbindlichen Umsetzungsweg zur Erfüllung der Anforderungen vor, sondern lässt den Umsetzungsweg offen.
2. Das SzA soll den gesamten Informationsverbund umfassen. Hierzu ist die gezielte Auswahl unterstützender IT-Systeme, eine risikobewertete Logging-Planung mit Konsolidierung der Logging-Inhalte auf ein gemeinsam auswertbares Datenmodell und die schrittweise und zeitlich geplante Umsetzung nach dem Prinzip einer möglichst effizienten Erkennung von Angriffen vorzusehen.
3. Der „Detection/Response“-Prozess soll möglichst automatisiert aber ohne Gefährdung der „kritischen Dienstleistung“ (im Weiteren als kDL abgekürzt) erfolgen. Zudem soll eine möglichst zentrale Auswertung und Koordination der Event-Lage innerhalb einer der Risikoanalyse entsprechend geringen Zeitspanne erfolgen und ein unmittelbarer „Response“ auf vermutliche Angriffe ermöglicht werden.
4. Das Schwachstellenmanagement, welches den präventiven Maßnahmen zuzurechnen ist, wurde im Anforderungskatalog explizit ausgeklammert.
5. Vorgeschlagen wird, sich in Bezug auf die Planung zu Angriffserkennungsmaßnahmen z. B. an der MITRE-Attack-Matrix zu orientieren.

[2] Quelle: § 8a Absatz 1 BSIG - Einzelnorm (gesetze-im-internet.de); eingesehen am 28.02.2023
[3] Quelle: § 8a Absatz 1a BSIG - Einzelnorm (gesetze-im-internet.de); eingesehen am 28.02.2023

6. Die OH SzA definiert den Begriff „Angriff“ wie folgt:
   „Ein Angriff ist eine vorsätzliche Form der Gefährdung, nämlich eine unerwünschte oder unberechtigte Handlung mit dem Ziel, sich Vorteile zu verschaffen bzw. einen Dritten zu schädigen. Angreifer können auch im Auftrag von Dritten handeln, die sich Vorteile verschaffen wollen“.

Bei der Bewertung der OH SzA ist der BAK von folgenden, grundlegenden Thesen ausgegangen:

1. **Im B3S in der Version 1.2 wurden die für die Branche relevanten Anforderungen der OH SzA in Abstimmung mit dem BSI vollständig aufgenommen**. Die OH SzA spezifiziert dabei lediglich die ISMS-Vorgaben in den Bereichen technisch-organisatorische Angriffserkennung und Reaktion („Detection & Response“) aus der Perspektive des BSI.
2. **Die KRITIS-Betreiber im Kontext der Branche med. Versorgung sind keineswegs am Anfang der Entwicklung** bezüglich der IT-Systemabsicherung im Sinne der OH SzA. Die KRITIS-Betreiber verfügen i. d. R. bereits über entsprechende Systeme und Maßnahmen zur Angriffserkennung und sind daher bestenfalls auf dem Weg zu einer übergreifenden Konsolidierung und Optimierung der technisch-organisatorischen Maßnahmen gemäß den Vorgaben der OH SzA.
3. Bei der Anpassungsplanung sind auch die Komplexität der vom BSI in der OH SzA geforderten Angriffserkennungsverfahren und bestehende Rahmenbedingungen bei Beschaffungsprozessen, z. B. einzuhaltende Ausschreibungsfristen, in Bezug auf den § 8a-Nachweis zu berücksichtigen.
4. **Oberstes Ziel jeder Absicherungsmaßnahme in der medizinischen Versorgung ist der „Schutz der kritischen Dienstleistung“** und nicht die „maximale, IT-technische Absicherung“. Absicherungsmaßnahmen müssen sowohl ökonomisch als auch in Bezug auf die potentiell gefährdende Wirkung eines technischen Systems zu Angriffserkennung auf das IT-Gesamtsystem angemessen sein.
5. **Krankenhäuser sind keine „Gesundheitsfabriken“,** bei der es um einen stabilen Output von Produkten geht. Die Fokussierung eines Behandlungsprozesses ist die möglichst optimale medizinische Versorgung eines individuellen Patienten. Besonders wichtig ist daher die Fokussierung auf die Schutzziele: Patientensicherheit und Behandlungseffektivität (siehe B3S V1.2, Kap. 2.2.2 sowie ANF-186). Die Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit, sind somit im Kontext der kDL-Erbringung an den ersten beiden Schutzzielen auszurichten.
6. **Die IT-Infrastruktur eines Krankenhauses muss vielfältigen regulatorischen Vorgaben entsprechen,** die in ihrer Fokussierung und Schwerpunktsetzung teilweise konkurrieren. Die IT-Sicherheitsgesetzgebung ist nur einer von vielen Aspekten. Es müssen weiterhin Datenschutzgesetzgebung (DSGVO/TTDSG/Landeskrankenhausgesetze), Medizinproduktegesetzgebung (EU-MDR), medizinische Leitlinien (AWMF), Vorgaben aus der übergreifenden Krankenhausgesetzgebung, z. B. SGB V (z. B. Telematik-Infrastruktur), KHG, KHZG, Strahlenschutzgesetzgebung, Hygiene- und Infektionsschutzgesetzgebung, ärztlichen Kammervorgaben, Vorgaben im Kontext der Durchführung klinische Studien sowie arbeitsrechtliche Vorgaben berücksichtigt und in Einklang gebracht werden.
7. **IT-Systeme in Krankenhausnetzwerkstrukturen sind äußerst heterogen** und werden, z.T. aus klinischen Gründen aber auch wegen der Besonderheiten des Finanzierungssystems im deutschen Gesundheitswesen, über einen sehr langen Zeitraum betrieben. Die IT-Sicherheit und die Logging-Fähigkeit der IT-Systeme im Krankenhaus sind somit extrem abhängig von der Sicherstellung der IT-sicherheitstechnischen Anforderungen nach dem Stand der Technik durch die Hersteller der IT-Systeme.

8. **Es handelt sich bei IT-Systemen im Krankenhaus oft um IT-Systeme, die vor allem in Bezug auf den medizinischen Nutzen und den hiermit einhergehenden, regulatorischen Anforderungen im nationalen, europäischen oder internationalen Kontext optimiert wurden** (Medizinprodukte, krankenhausspezifische Spezialsoftware). Diese IT-Systeme in kürzester Zeit auf die Anforderungen der neuesten IT-Sicherheitsgesetzgebung bzw. die Anforderungen der OH SzA anzupassen, ist kurzfristig nicht möglich.
9. Technische Angriffserkennungssysteme helfen bei der Erkennung von Angriffsprozessen und referenzieren i.d.R. auf bekannte Angriffsvektoren und Angriffsszenarien. **Wichtig ist daher vor allem die Festlegung von „Anomalie-Erkennungs-Metriken/Anomalie-Erkennungs-Triggern" in der jeweiligen IT-Betriebssituation.** Derartige Metriken/Trigger im jeweiligen IT-Betriebskontext zu definieren, erfordert neben IT-Fachkompetenz insbesondere Branchenkompetenz und sollten durch das Krankenhaus individuell festgelegt werden. Beispielsweise könnte dies in einem ersten Schritt für die IT-Systeme im Krankenhaus am ehesten von den betreuenden Systemadministratoren geleistet werden.
10. **Der Betrieb von IT-Systemen im Krankenhaus erfolgt in unterschiedlichen Betriebs-, Nutzungs- und Knowhow-Domänen (z. B. Office-IT, Medizin-IT, Facility-Management/Versorgungstechnik-IT, Cloud-IT)**. Die Sicherstellung der Funktionsfähigkeit der Systeme zur Aufrechterhaltung der kDL erfordert somit sehr differenzierte Fachkenntnisse im jeweiligen IT-Betriebskontext, um potentielle Anomalie-Ereignisse einordnen oder bewerten zu können. Diese sind nötig, um Abwehrmaßnahmen mit Fokussierung auf die Sicherstellung der kDL bzw. Behandlungseffektivität und Patientensicherheit problemadäquat einordnen zu können. Beauftragte (externe) SOC-Teams (Security Operations Center), müssen das konkrete Geschehen im Netzwerk bzw. auf den IT-Systemen, anhand einer branchenspezifischen Datenlage mit unmittelbaren Betriebsbezug bewerten können, um in Bezug auf die Reaktion auf eine erkannte IT-Anomalie oder ein potentielles Angriffsgeschehen u. U. nicht die Erbringung der kritischen Dienstleistung (kDL) zu gefährden. Sie sollten daher in Bezug auf die Reaktionsprozesse differenziert und mit vom Krankenhaus vorgegeben Handlungsvorgaben in den Angriffserkennungsprozess eingebunden werden. Eine konkrete Reaktion auf erkannte, kritische IT-Anomalien oder ein entsprechendes Angriffsgeschehen sollte somit durch das Krankenhaus nach einer Alarmierung festgelegt werden.
11. **Automatisierte Erkennungs- und Reaktions-Systeme („Detection"/"Response") können unmittelbaren Schaden in Bezug auf die Erbringung der kDL bedingen und sind im Krankenhausumfeld kritisch zu sehen**. Sie sollten daher hinsichtlich des Betriebskontextes (z. B. Office-IT, Medizintechnik, usw.) betrachtet und nur nach einer Risikobewertung bezüglich der Folgen für die kDL zum Einsatz kommen.
12. **Bei der Speicherdauer von angriffserkennungsrelevanten Daten, ist ein sinnvoller Kompromiss zwischen retrospektiver Analysemöglichkeit (Forensik), Datenschutzaspekten und Ressourcen-Anforderungen zu finden.** Es wird eine Aufbewahrungsdauer von Daten, die für die nachträgliche Angriffserkennung (Forensik) von hoher Relevanz sind (z. B. AD-Logs, Firewall-Logs u. ä.), von **einem Jahr**, und für Erkennungssysteme oder Log-Bereiche, die eher einen reaktiven Aspekt (z. B. DDoS-Attacken) abdecken, von **drei Monaten** empfohlen. Hierbei ist insbesondere eine Nutzen-Risiko-Analyse bezüglich der aufbewahrten Logs sinnvoll, um bspw. Ressourcenengpässe zu vermeiden. Die abschließende Festlegung der Speicherdauer sollte in Abwägung der genannten Parameter individuell vom Krankenhaus festgelegt werden, da im Einzelfall auch eine längere Dauer durchaus sinnvoll sein kann.

Fazit der Bewertung durch den BAK:

Die spezifischen Problemstellungen der Branche führen zu einer besonderen Gewichtung der Angriffserkennung am Perimeter (Firewall, Bereichsfirewalls, Router mit ACLs u.ä.) bzw. den Netzübergangspunkten im weiteren Sinne (Arbeitsplatz PCs bzw. Devices mit Außenanbindung), um eine Art „Schutzumgebung für kDL-relevante Systeme“ zu erzeugen. Zudem muss es vor allem das Ziel sein, die Angriffserkennung und Angriffsabwehr im Krankenhaus-IT-Informationsverbund im Sinne des Schutzes der Erbringung und Sicherstellung der „Kritischen Dienstleistung“ zu gestalten.

Die Vorgabe von technisch-organisatorischen Anforderungen muss auf den jeweiligen Branchenkontext angepasst werden. Die potentielle Gefährdung von Patienten durch nicht auf den Anwendungskontext abgestimmte Abwehrsysteme ist kritisch zu betrachten. Ein risikiobasiertes Vorgehen ist daher dringend empfohlen.

Die KRITIS-Betreiber sollten daher ein schlüssiges Konzept im Sinne der geforderten „Systeme zur Angriffserkennung“ in Bezug auf den § 8a-Nachweis im Jahr 2023 vorweisen können, aber durchaus auch die konstruktiven Dialog mit Auditoren, Prüfenden Stellen oder dem BSI in Bezug auf Anforderungen der OH SzA suchen, wenn dies im Sinne der Erbringung der kDL nachvollziehbar begründbar ist. Lassen sich unterschiedliche Interpretationen der Anforderungen nicht in diesem Rahmen klären, wird um Hinweis an die Leitung des BAK gebeten. Nach Möglichkeit werden diese Fragen dann zur Klärung in der weiteren Abstimmung mit dem BSI aufgegriffen.

Beispiel für ein Vorgehensmodell zur Umsetzung der Anforderungen für Angriffserkennung und Angriffsreaktion:

Zugehörige Richtlinien planen, erstellen und pflegen:

- Sicherheitsrichtlinie für die Protokollierung
- Sicherheitsrichtlinie für die Detektion von sicherheitsrelevanten Ereignissen
- Erstellung einer Richtlinie zur Behandlung von Sicherheitsvorfällen
- **…**

Analyse des Informationsverbundes mit der Perspektive der Angriffserkennung- und Angriffsabwehr durchführen:

- Sinnvoll begründbares Absicherungsdomänenkonzept festlegen (s. o.). Hierbei ein Schalenmodell von Perimeter über Netzsegmentierung bis zu Einzelsystemkomplexen fokussieren.

IST-Zustand Angriffserkennung/Angriffsabwehr erfassen:

- Die wichtigsten, in den Schutzdomänen bereits vorhandenen Absicherungssysteme katalogisieren und klassifizieren. Diese Systeme auf ihren bestimmungsgemäßen Gebrauch und das ggf. noch nicht ausgeschöpfte Angriffserkennungspotential prüfen.
- Die Überwachungs- und Logging-Funktionalitäten inkl. des hierfür nötigen Ressourcenbedarfes (Speicherplatz/Rechenleistung), sowie die bisherige Speicherdauer für die Log-Daten bei den bereits betriebenen IT-Absicherungs- und IT-Kernmanagementsysteme (z. B. AD) erfassen.

- Explizit die IT-Betriebsüberwachungssysteme (z. B. IT-Infrastructure Monitoring, System Center Operations Manager, u. ä.) und die dezentralen, administrativen Überwachungslösungen, z. B. Helpdesk-Meldungen, in die Überlegungen einbeziehen.
- Bisherige technisch-organisatorische Reaktionsregelungen und Maßnahmen auf die entsprechende Prozesstreue überprüfen, falls dies im Rahmen des ISMS nicht regelmäßig erfolgt.

Verbesserungs- und Ausbaupotentiale im Kontext der Absicherungsdomänen identifizieren:

- SWOT-Analyse (Stärken-Schwächen-Chancen-Risiken-Analyse) in Bezug auf die bestehende Konzeption der „Systeme zur Absicherung“ vornehmen. Gründe für erkannte Schwächen identifizieren und dokumentieren. Dies ist von einer GAP-Analyse (Lückenanalyse) zu unterscheiden, die z. B. auf Lücken bei der Umsetzung eines Anforderungskataloges, z. B. OH SzA, fokussiert und so gesehen nur ein Teil der SWOT-Analyse sein kann.
- Zentralen, strategischen Nachkaufbedarf für IT-Absicherungssysteme oder fehlender organisatorische Maßnahmen mit einer Risikobewertung für die Absicherungsdomäne identifizieren.
- Logfile-Schnittstellen- und Kapazitätsanalyse mit der Fokussierung auf die möglichst effiziente Erkennung von Angriffen vornehmen.
- Aufbau- und Ausbauplan in technisch-organisatorischer Hinsicht definieren, also ein IT-Sicherheitskonzept mit Fokussierung Angriffserkennung entwickeln, falls noch nicht vorhanden, und Lücken im Angriffserkennungssystem identifizieren.
- Technisch-organisatorisches Erkennungs- und Reaktionsvorgehen definieren und festlegen, soweit hier Schwächen erkannt wurden, und hierbei das SMART-Prinzip des Projektmanagements (spezifisch, messbar, attraktive, realistische und terminierte Ziele) im Blick behalten.

Beispiel für ein koordiniertes Vorgehen zur Verbesserung der Angriffserkennung und Angriffsreaktion am Beispiel einer SIEM-Einführung:

Bereits vor dem Einsatz der erforderlichen Systeme sind umfangreiche Vorarbeiten erforderlich, dazu zählen:

- ein Abgleich der möglichen Protokollquellen mit Medizin- und Gebäudetechnik,
- die Festlegung der Kritikalitätsstufen für alle Protokollquellen zur Identifizierung als für den Versorgungsauftrag maßgeblich,
- die Abstimmung zum Umgang mit datenschutzrechtlichen relevanten Daten,
- die Dokumentation aller Netzbereiche, die Protokoll- und Protokollierungsdatenquellen, deren Beziehungen untereinander,
- die Erarbeitung und Etablierung eines Change-Prozesses bei Veränderungen in der Systemlandschaft des Krankenhauses,
- das Durchführen einer Datenschutzfolgenabschätzung für die Protokollierungslösung.

1. **Schritt:** Definition des konkreten Verbesserungspotential bezüglich der Erkennung von Angriffen mit Hilfe eines SIEMS nach Analyse der bestehenden Verfahren, Maßnahmen und IT-Absicherungssysteme.
2. **Schritt:** Fokussierte Absicherungsdomäne für eine Logfile-Auswertung mit SIEM-System identifizieren. Hierbei berücksichtigen, dass die Reaktion auf eine erkannte Anomalie innerhalb einer Absicherungsdomäne nur mit sehr viel speziellem Fach-Knowhow – auch in Bezug auf die Folgen für die kritische Dienstleistung – erfolgen darf. Eine Absicherungsdomäne wird demnach oftmals einer technisch-organisatorischen Fachknowhow-Domäne entsprechen.
3. **Schritt:** Identifikation von Wissenslücken, Beratungsbedarf, Unterstützungsbedarf im getroffenen Handlungsrahmen.

4. **Schritt:** Identifikation des Personalbedarfs bzw. externen Unterstützungsbedarfs im Betrieb des SIEMs. Absicherungssysteme, die personell nicht adäquat betreut werden können, erhöhen ggf. die Angriffsfläche und sind im Wesentlichen zur Zielerreichung einer besseren Absicherung des Informationsverbundes sinnlos.
5. **Schritt:** Die wichtigsten schon verfügbaren technischen Angriffserkennungssysteme identifizieren und das Logfile-Aufkommen analysieren.
6. **Schritt:** Probleme in Bezug auf Datenschutzregelungen/Arbeitsüberwachungsfragestellungen usw. identifizieren, kommunizieren, diskutieren und lösen, z. B. Datenschutzfolgenabschätzung.
7. **Schritt:** Speicherdauer für Logfiles festlegen.
8. **Schritt:** Integration und Abgleich der Asset-Datenbanken, vom ggf. vorhandenen IPAM-System bis zur Inventarisierungsdatenbanken, in das Projektkonzept einbeziehen. Ein SIEM-System, bei dem Anomalien nicht unmittelbar einem Betriebskontext und den betroffenen Assets zuzuordnen sind, ist bei der Angriffserkennung lediglich eine Scheinsicherheit, aber kein adäquates Absicherungselement. Ein Herzkatheter-Konsolen-PC erscheint für ein SIEM ohne Metadaten, je nach Ausprägung, lediglich als IP-Adresse.
9. **Schritt:** Risikobasierte Kritikalitätsanalyse bezüglich der SIEM-Einbindung von fokussierten IT-Systemen/Assets in der jeweiligen Absicherungsdomäne vornehmen. Potentielle Gefährdungen für die kDL in Bezug auf Anomalie-Erkennung und Reaktion bezüglich der betroffenen Assets und Netzbereiche identifizieren (Kollateralschäden der Angriffserkennung).
10. **Schritt:** Erfassung der Mitarbeiterinformations-, Notfall-Überbrückungs- und Wiederherstellungsmaßnahmen im Falle einer automatisierten Reaktion auf eine Anomalie.
11. **Schritt:** SIEM-Integration z. B. mit Außen-Firewall/Bereichsfirewalls an den Netzübergängen beginnen.
12. **Schritt:** SIEM-Integration mit Systemen zur Endpoint-Protection/Virenscannern u. ä. fortsetzen.
13. **Schritt:** Logfiles zentraler Katalogsysteme, z. B. AD/Azure-AD bzw. Domain-Controller bzw. zentraler Infrastrukturkomponenten, z. B. Virtualisierungsinfrastruktur, Datenbankcluster usw., VPN-Routern, IPS/IDS-Systemen, SPAM-Abwehrsystemen, Ransomware-Erkennungs-Traps und Honeypots usw. integrieren.
14. **Schritt:** SIEM-Integration von NAC & IPAM & Medizinprodukt-Erkennungs- und Absicherungssystemen (z. B. spezialisierte Medizinprodukte-Netzwerk-Scanner o. ä.) & MDM & Netzwerküberwachungstools und, wenn sinnvoll, Zugangsmanagementsystem integrieren. **Achtung:** Aktive Scans auf fragile Infrastrukturen können zu deren Ausfall führen, daher sollte im Vorfeld eine Risikobetrachtung hinsichtlich aktiver oder passiver Scans durchgeführt werden. Grundsätzlich sind bei fragilen Infrastrukturen passive Scans zu bevorzugen.
15. **Schritt:** Logs zentraler Anwendungssysteme, Fileserver, Exchange, Cloud-Anwendungen/DMZ-Server & weitere Infrastruktur-Log-Quellen integrieren.
16. **Schritt:** Log-Integration der primären kDL-prozessrelevanten-IT-Systeme
17. **Schritt:** Log-Integration aller andern als für die Angriffserkennung relevant definierten IT-Systeme.
18. **Schritt:** Erarbeitung und Etablierung eines Change-Prozesses bei Veränderungen in der Systemlandschaft des Krankenhauses

Die sicherlich größte Herausforderung im Rahmen der Optimierung der Angriffserkennung- und der Reaktion auf Angriffe besteht hierbei nicht in der Log-Anbindung und Logfile-Konsolidierung in einem SIEM, sondern in der Definition der „Trigger-Points“ zur Anomalie-Erkennung und Behandlung in jedem Ausbauschritt der SIEM-Umgebung, um adäquat auf eine Angriffssignalisierung reagieren zu können. In diesem Kontext ist externe **Unterstützung durch entsprechende Fachberater** oft sinnvoll und hilfreich. Zudem kann darauf hingearbeitet werden, mit einem Beratungsunternehmen oder eigener Expertise eine sinnvolle Unterstützung in tatsächlichen Angriffsfall abzustimmen und entsprechende Aspekte zur retrospektiven, forensischen Analyse zu berücksichtigen.

IT-Systeme im Kontext der aktiven Angriffserkennung, die mit hohen Systemrechten zur Erfassung von Angriffsanomalien ausgestattet sind und zentrale Angriffserkennungsinformationen an ein SIEM übertragen, können zusammen mit dem **SIEM ggf. selbst einem erheblichen Angriffsrisiko unterliegen** und sollten dann bestmöglich abgesichert werden.

Abkürzungsverzeichnis:

ACL	Access Control List
AD	Active Directory
ANF	Anforderung
AWMF	Arbeitsgemeinschaft der wissenschaftlich Medizinischen Fachgesellschaften e.V.
Azure-AD	Microsoft Azure-Active Directory
B3S	Branchenspezifischer Sicherheitsstandard
BAK	Branchenarbeitskreis
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
DDoS	Distributed Denial of Service
DKG	Deutsche Krankenhausgesellschaft e.V
DMZ	Demilitarisierte Zone
DSGVO	Datenschutzgrundverordnung
ERT	Emergency-Response-Team
EU-MDR	European Medical Device Regulation
GAP-Analyse	Lücken-Analyse
IDS	Intrusion Detection System
IPAM	IP-Adress-Management
IPS	Intrusion Prevention System
ISMS	Informationssicherheitsmanagementsystem
kDL	Kritische Dienstleistung gemäß Kritis-Verordnung
KHG	Krankenhaushausgesetz
KHZG	Krankenhauszukunftsgesetz
KIS	Krankenhausinformationssystem
KAS	Klinisches-Arbeitsplatz-System
KritisV	Kritis-Verordnung
MDM	Mobile-Device-Management
NAC	Network-Access-Control
OH	Orientierungshilfe
SdT	Stand der Technik
SIEM	Security Information and Even Management
SMART	***S**pecific **M**easurable **A**chievable **R**easonable **T**ime-bound*
SOC	Security Operations Center
SPAM	unerwünschte E-Mails
SWOT	**S**trengths, **W**eaknesses, **O**pportunities, **T**hreats
SzA	Systeme zur Angriffserkennung
TTDSG	Telekommunikation-Telemedien-Datenschutz-Gesetz
VPN	Virtual Privat Network