Allianz für Cyber-Sicherheit

**EMPFEHLUNG: Hersteller und Betreiber von Medizinprodukten**

# Sicherheit von Medizinprodukten

Leitfaden zur Nutzung des MDS2 aus 2019

Expertenkreis CyberMed

# Inhaltsverzeichnis

# 1 Präambel

Das vorliegende Dokument ist ein Leitfaden zur Anwendung des Manufacturer Disclosure Statement for Medical Device Security (MDS2) und soll als Hilfestellung dienen, um das MDS2 bestmöglich ausfüllen und verwenden zu können. Das MDS2 ermöglicht Herstellern die Informationen zu (cyber-)sicherheitsrelevanten Merkmalen und Funktionen ihrer Produkte in strukturierter Form an Betreiber zu übermitteln. Es beschreibt Eigenschaften des Standardprodukts im Rahmen der vom Hersteller vorgesehenen Konfigurationsmöglichkeiten.

Der Expertenkreis CyberMed[1], bestehend aus Vertretern von Systembetreibern, Anwendern und Industrie sowie Behörden, empfiehlt, das MDS2 als Kommunikationsinstrument und als Grundlage für weitere Diskussion rund um den Bereich Cyber-Sicherheit zu nutzen.

Die Vorteile des MDS2 im Überblick:

- Als maschinenlesbares und standardisiertes Dokument erleichtert das MDS2 die Kommunikation zwischen Herstellern und Betreibern.
- Das MDS2 ist auf freiwilliger Basis auszufüllen und nicht als Teil der gesetzlich verpflichtenden Unterlagen (Nutzerdokumentation) und nicht als Begleitdokument im Sinne des Medizinprodukterechts zu verstehen.
- Der umfangreiche Fragenkatalog zu Cyber-Sicherheitsfragen von Medizinprodukten bietet eine bisher nicht dagewesene Vergleichbarkeit von Sicherheitseigenschaften verschiedener Produkte unterschiedlicher Hersteller einer Geräteklasse.
- Das MDS2 ermöglicht die Beurteilung von Schwachstellen und Risiken bereits im Vorfeld des eigentlichen Beschaffungsprozesses.
- Das MDS2 beinhaltet insbesondere auch Informationen zum Schutz von sensiblen Daten, z. B. Patientendaten, die als Grundlage für eine Risikoanalyse für den Betrieb des Systems herangezogen werden können.
- Das MDS2 unterstützt Hersteller und Betreiber bei der Erfüllung anwendbarer Standards und regulatorischer Vorgaben.

# 2 Einleitung

Der Trend zur Digitalisierung und Vernetzung gewinnt im Bereich der Medizinprodukte zunehmend an Bedeutung. Bedingt durch die heterogenen Einsatzumgebungen in sicherheitskritischen Bereichen, vor allem in Krankenhäusern, und die oftmals lange Produktlebensdauer, müssen besondere Anforderungen an die Cyber-Sicherheit von Medizinprodukten gestellt werden.

In den USA wurde aus diesen Gründen bereits 2004 ein Vorläufer des aktuellen MDS2[2] (Manufacturer Disclosure Statement for Medical Device Security), im Folgenden nur als das MDS2 bezeichnet, welches bereits standardisierte Informationen zu Cyber-Sicherheitseigenschaften von vernetzten Medizinprodukten aufführte, von der NEMA (National Electrical Manufacturers Association) veröffentlicht. Vier Jahre später konnte das MDS2 in überarbeiteter Version als Standard (HN 1-2008) etabliert werden. Hersteller in den USA sind seitdem dazu angehalten ihre Medizinprodukte mit dem zugehörigen MDS2 an die Betreiber der Systeme auszuhändigen. Das aktuelle Formular listet, als standardisierte und maschinenlesbare Tabelle, Sicherheitsattribute eines Produkts oder von einzelnen Gerätekomponenten auf und dient als Hilfestellung für die Risikobewertung eines Medizinprodukts schon im Vorfeld des eigentlichen Beschaffungsprozesses durch die Systembetreiber.

Um auch in Deutschland die Cyber-Sicherheitslage von Medizinprodukten durch mehr Transparenz nachhaltig und dauerhaft zu verbessern, wird empfohlen, das MDS2 als umfangreiche, standardisierte Informations- und Kommunikationsgrundlage, zu nutzen. Auf lange Sicht harmonisiert die Verbreitung des MDS2 die Informationen zu IT-sicherheitsrelevanten Eigenschaften von IT-gestützten medizinischen Systemen und dient somit der vertrauensvollen Zusammenarbeit aller Beteiligten im Kommunikations- und Beschaffungsprozess derartiger Produkte. Das MDS2 fasst die wichtigsten Kriterien, im Hinblick auf die Anforderungen von „privacy-by-design“ und „security-by-design“ eines IT-gestützten Medizinprodukts auf. Daher sollte es als Unterstützung zur Umsetzung der Cyber-Sicherheit bei der Herstellung von Medizinprodukten sowie beim Risikomanagement gemäß der IEC 80001 beim Betreiber verstanden werden. Es kann sowohl als Grundlageninformation zur kontinuierlichen Risikominimierung, als auch für das gesetzlich geforderte Risikomanagement im Bereich der Kritischen Infrastrukturen verwendet werden.

Die Nutzung von MDS2-Formularen stellt für den Hersteller einen einfachen Weg dar, technische, produktspezifische und übliche Informationssicherheitsattribute an Betreiber zu übermitteln. In Deutschland steht Herstellern die Verwendung des MDS2 frei. Durch die Übermittlung des MDS2 können Hersteller deutlich machen, dass sie Transparenz gewährleisten und sichere Lösungen nach Industriestandards entwickeln, indem sie alle notwendigen Informationen teilen. Das Formular sollte, wenn erforderlich, z. B. bei Software-Updates oder generellen Änderungen an der Gerätekonfiguration, durch den Hersteller überarbeitet werden. Der tabellarische Aufbau des Formulars erlaubt es, dass neue Informationen oder sogar komplexe Änderungen der Sicherheitsinformation zu einem System, schnell eingepflegt und an die Betreiber von Medizinprodukten kommuniziert werden können. Die Verwendung des MDS2 entbindet den Hersteller nicht von seinen generellen Anforderungen und Verpflichtungen. Das MDS2 ist weder eine Betriebs- oder Bedienungsanleitung, noch ersetzt es die technische Dokumentation oder die Spezifikation eines Medizinprodukts.

Zu beachten ist, dass sich Informationen zu einem Medizinprodukt immer auf das spezifische Design, die verwendete Software und die Produktcharakteristika beziehen müssen. Das bedeutet, dass jedes Produkt individuell betrachtet werden muss, um festzulegen, welche sicherheitsrelevanten Merkmale implementiert sind. Dazu zählt u. a. auch, welche Zweckbestimmung für das Produkt vom Hersteller definiert wurde und wie es mit der Umgebung in Wechselwirkung steht. In den wenigsten Fällen werden alle gelisteten Sicherheitsmerkmale des MDS2 für das zu betrachtende Medizinprodukt gelten, so dass im MDS2 klar zu erkennen sein muss, welche vorgegebenen Merkmale nicht betrachtet, beziehungsweise nicht auf das jeweilige Produkt anwendbar sind.

Betreiber können, zusätzlich zu verfügbaren Referenzen (White Paper, Standards, etc.), mithilfe von Informationen aus dem MDS2 ihr Risikomanagement für einen sicheren Betrieb optimieren, da sie die möglichen Cyber-Risiken von vernetzten Medizinprodukten in Bezug auf Informationssicherheit besser beurteilen können. In ihrer standardisierten und maschinenlesbaren Form können MDS2-Formulare verschiedener Hersteller für einen Gerätetypen besser verglichen werden und Änderungen

der IT-Sicherheitskonfiguration einfacher kommuniziert werden.

Das MDS2 erlaubt insbesondere die verschiedenen Aspekte der Informationssicherheit von vernetzten Produkten im Vorfeld der eigentlichen Anschaffung abzuschätzen und in eine Kaufentscheidung einfließen zu lassen. Mit den gelisteten Attributen ist es der Startpunkt, um beim Betreiber administrative, physikalische und technische Maßnahmen für einen sicheren Betrieb diskutieren und planen können.

# 3 Ausfüllanleitung

Ziel dieses Abschnitts ist es, dem Hersteller Anleitungen an die Hand zu geben, wie die Attribute des MDS2 zu verstehen und bestmöglich auszufüllen sind. Das Formular gibt die Systemeigenschaften in Bezug auf Informationssicherheitsmerkmale eines Medizinprodukts in Form von definierten Systemattributabfragen wieder. Hierbei werden zum einen knappe Antwortalternativen, die einen maschinenlesbaren Vergleich mit anderen Produkten und die Charakterisierung des Produktes ermöglichen, verwendet. Zum anderen bietet das Formular Freitextfelder für ergänzende Angaben.

- Die Fragen nach Sicherheitsattributen im MDS2-Formular werden im ersten Schritt nur mit „yes“ für „ja“, „no“ für „nein“ oder „n/a“ für „nicht anwendbar“ ausgefüllt.
- Die einfache Attribut-Eingabe mit den Ausfülloptionen „yes“, „no“ und „n/a“ ist in der Regel nicht ausreichend, sondern gibt eine erste Orientierung.
- Die den Attributen zugeordneten Freitextfelder erlauben es dem Hersteller, zusätzliche, erklärende Informationen bereitzustellen. Es wird empfohlen, dass diese Freitextfelder zur Weitergabe kritischer und übergeordneter Informationen genutzt werden (Referenzen auf White Paper, Literaturreferenzen).
- Falls einige Punkte nicht auf das Produkt zutreffen, so ist mit „no“ oder „n/a“ zu antworten. „n/a“ hat hierbei die Bedeutung, dass das Attribut aufgrund der Zweckbestimmung, des Designprinzips oder der vorgesehenen Anwendungsumgebung nicht anwendbar ist. Dies kann z. B. der Fall sein, wenn es sich nicht um ein Gerät, sondern um eine Software handelt, die beschrieben werden soll. „no“ bedeutet, dass das Produkt dieses Attribut auch dann nicht aufweist, wenn diese Sicherheitseigenschaft im Anwendungskontext des Produkts gegebenenfalls sinnvoll sein könnte.
- Falls die Antwort aufgrund von Zusatzoptionen oder Zubehör bei einem Produkt nicht eindeutig ausfällt, kann der Hersteller dies ebenfalls im Freitextfeld erklären.
- Falls erweiterte Antworten für mehrere Fragen des MDS2 gelten, so sollte auch dies kenntlich gemacht werden.
- Es darf auf andere Dokumente referenziert werden (Hyperlink, Referenzen, White Paper), soweit diese öffentlich zugänglich sind oder im Anhang des MDS2 mit ausgeliefert werden. Idealerweise sollte im Freitextfeld eine kurze Zusammenfassung dieser verwendeten Referenzen zur Verfügung gestellt werden.

## 3.1 Beschreibung des Medizinprodukts (DOC)

Geben Sie hier bitte alle notwendigen Daten zur Beschreibung des Medizinprodukts an.

| FragenID | Frage | Empfehlung |
|---|---|---|
| DOC-1 | Name des Herstellers/Legal manufacturer | |
| DOC-2 | Beschreibung des Produkts | Bitte geben Sie hier die Produkt- und/oder Versionsinformationen an. |
| DOC-3 | Modellnummer des Produkts | Hier ist es empfehlenswert, die Modellnummer, mit der das Produkt in Verkehr gebracht wurde, zu verwenden. |
| DOC-4 | Dokumenten ID | Es wird empfohlen die Dokumentennummer dieses MDS2-Dokuments einzufügen, so dass klar ist, auf welches Dokument und welchen Versionsstand sich eventuelle Rückfragen beziehen. |
| DOC-5 | Kontaktinformationen des Herstellers | Es wird empfohlen, einen Ansprechpartner, in Form einer Telefonnummer, Mailadresse oder durch persönlichen Kontakt zu nennen. Um den unterschiedlichen Firmenstrukturen gerecht zu werden, sollte bei Fragen zum Produkt das Produktmanagement angegeben werden, bei IT-Sicherheitsfragen sollte ein technischer Experte und bei Fragen zum Datenschutz eine entsprechend verantwortliche Person benannt werden. |
| DOC-6 | Zweckbestimmung des Produkts in vernetzten Umgebungen | Hier ist empfehlenswert, dass auf die Formulierungen im Benutzerhandbuch oder in anderen bestehenden Dokumenten verwiesen wird. |
| DOC-7 | Veröffentlichungsdatum des Dokuments | Es wird empfohlen, dass neben dem Dokumentendatum auch das Datum des MDS2-Formulars angegeben wird. |
| DOC-8 | Koordiniertes Offenlegungs-Programm des Herstellers | Gibt es ein herstellereigenes koordiniertes Offenlegungs-Programm (Disclosure-Programm) für Schwachstellen? Wo kann man dieses finden (Web)? |
| DOC-9 | ISAO | ISAO steht für „Information Sharing and Analysis Organization“. Der Hersteller kann hier angeben, ob und in welcher ISAO er Mitglied ist. Die Allianz für Cyber-Sicherheit (ACS) kann durchaus als solche betrachtet werden. |

| FragenID | Frage | Empfehlung |
|---|---|---|
| DOC-10 | Gibt es ein Netzwerk- oder Datenfluss-Diagramm, das die Verbindung zu anderen Systemkomponenten oder externen Ressourcen darstellt? Wenn ja, stellen Sie bitte Details oder entsprechende Referenzen im Freitextfeld zur Verfügung. | Hier ist zu empfehlen, dass ein Verweis z. B. auf ein Netzwerkdiagramm in der Kundendokumentation, aufgeführt wird. |
| DOC-11 | Handelt es sich bei dem Produkt um Software as a Medical Device (SaMD)? | Hier ist zu empfehlen, dass wenn die Antwort „no“ lautet, bei den folgenden Fragen 11.1 bis 11.4 „n/a“ angegeben wird. |
| DOC-11.1 | Beinhaltet die SaMD ein Betriebssystem? Wenn ja, stellen Sie bitte Details oder entsprechende Referenzen im Freitextfeld zur Verfügung. | |
| DOC-11.2 | Läuft die SaMD auf einem vom Betreiber gestellten Betriebssystem? Wenn ja, stellen Sie bitte Details oder entsprechende Referenzen im Freitextfeld zur Verfügung. | |
| DOC-11.3 | Wird die SaMD vom Hersteller betrieben? Wenn ja, stellen Sie bitte Details oder entsprechende Referenzen im Freitextfeld zur Verfügung. | |
| DOC-11.4 | Wird die SaMD vom Kunden betrieben? Wenn ja, stellen Sie bitte Details oder entsprechende Referenzen im Freitextfeld zur Verfügung. | |

## 3.2 Verwaltung von personenbezogenen Daten (MPII)

Geben Sie bitte an, wie personenbezogene Daten vom Produkt verarbeitet werden.

| FragenID | Frage | Empfehlung |
|---|---|---|
| MPII-1 | Kann das Produkt personenbezogene Daten anzeigen, übertragen, speichern oder verändern (inklusive elektronischer Akten)? | Hier ist die nationale/lokale Gesetzgebung bzw. Auslegung von PII (personenbezogene Daten) oder die Verarbeitung dieser Daten gemeint. Hierzu zählen beispielsweise: Patientenname, Krankenversicherung und Versicherungsnummer, biometrische Daten, etc. |
| MPII-2 | Welche Arten von personenbezogenen Daten können von dem Produkt vorgehalten werden? Listen Sie diese bitte in einem Freitextfeld auf. | Hier ist es sinnvoll, dass alle Arten von personenbezogenen Daten aufgezählt werden oder auf deren Dokumentation verwiesen wird. Wenn bei MPII-1 mit „no“ geantwortet wurde, so sollte auch hier mit „no“ geantwortet und das Kommentarfeld freigelassen werden. |

| FragenID | Frage | Empfehlung |
|---|---|---|
| MPII-2.1 | Werden im Produkt personenbezogenen Daten temporär oder in einem flüchtigen internen Speicher vorgehalten (z. B. bis zum Ausschalten oder Zurücksetzen des Produkts)? | Wenn bei MPII-1 mit „no“ geantwortet wurde, so sollte auch hier mit „no“ geantwortet und das Kommentarfeld freigelassen werden. Ansonsten sollte diese Frage mit „yes“ beantwortet und die Details, wie das Halten der Informationen bis zum Ausschalten des Produkts (embedded device) oder bis zum Beenden der Applikation (SaMD, medizinische Apps) im Kommentarfeld angegeben werden. |
| MPII-2.2 | Werden personenbezogene Daten dauerhaft in internem Speicher gesichert? | Bitte geben Sie hier Informationen zur Art der Speicherung, z. B. Datenbank oder Dateisystem, an. |
| MPII-2.3 | Werden personenbezogene Daten auf nicht flüchtigen Datenspeichern aufbewahrt, bis diese explizit gelöscht werden? | Bitte geben Sie hier Informationen zur Art des Auslösens der Löschung, z. B. automatisch oder manuell, an. |
| MPII-2.4 | Werden personenbezogene Daten dauerhaft in Datenbanken gespeichert? Wenn ja, liefern Sie bitte Details zur Architektur der Datenbank im Freitextfeld. | Wenn bei MPII-1 mit „no“ geantwortet wurde, so sollte auch hier mit „no“ geantwortet und das Kommentarfeld freigelassen werden. Diese Frage sollte nur mit „yes“ beantwortet werden, wenn die Daten tatsächlich in einer Datenbank abgelegt werden. Geben Sie bitte an, ob die Daten in einer externen oder lokalen Datenbank gespeichert werden. Bei Informationen zur Datenbank sollte sich die Erklärung nur auf die für den Datenschutz relevanten Daten beschränken. |
| MPII-2.5 | Bietet das Produkt die Möglichkeit, dass lokal gespeicherte, personenbezogene Daten nach deren Ablage auf einem Langzeitspeicher automatisch gelöscht werden? | |
| MPII-2.6 | Können personenbezogene Daten von anderen Systemen importiert oder dorthin exportiert werden? Z. B. ein tragbares Überwachungsgerät könnte personenbezogene Daten an einen Server liefern. | Hier ist das Importieren und Exportieren von personenbezogenen Daten zur weiteren Verarbeitung, als Teil der Zweckbestimmung und des normalen Betriebs, gemeint. Die Frage bezieht sich nicht auf Backup-Lösungen. |
| MPII-2.7 | Werden personenbezogene Daten vorgehalten, wenn das Produkt ausgeschaltet wird oder die Stromzufuhr unterbrochen wird? | |

| FragenID | Frage | Empfehlung |
|---|---|---|
| MPII-2.8 | Können die internen Datenspeicher durch einen Wartungsmitarbeiter entfernt werden, z. B. um diese separat zu vernichten oder beim Kunden vorzuhalten? | Hier kann zusätzlich angegeben werden, ob es sich um einen Mitarbeiter des Kunden handelt oder ob nur ein Mitarbeiter des Herstellers berechtigt ist. |
| MPII-2.9 | Können personenbezogene Daten auf einem separaten System, getrennt vom Betriebssystem des Produkts oder der Gerätesoftware, gespeichert werden? Z. B. auf einem zweiten internen Laufwerk, auf alternativen Partitionen auf der Festplatte oder auf einem externen Speicherplatz. | |
| MPII-3 | Erlaubt die Zweckbestimmung des Produkts, dass Mechanismen für die Übertragung (Importieren/Exportieren) von personenbezogenen Daten genutzt werden? | Bitte geben Sie hier an, ob diese Mechanismen, im Rahmen der Zweckbestimmung, möglich und ob sie optional sind. |
| MPII-3.1 | Ist es möglich auf dem Produkt personenbezogene Daten anzuzeigen (z. B. über einen Bildschirm)? | |
| MPII-3.2 | Erstellt das Produkt physische Berichte oder Bilder, die personenbezogene Daten beinhalten? | Hierbei sind dauerhafte Abzüge der digitalen Information gemeint (hard copy). |
| MPII-3.3 | Kann das Produkt personenbezogene Daten von einem Wechseldatenträger auslesen oder darauf schreiben (z. B. externe Festplatte, USB-Speicherstick oder andere USB-Speichermedien, DVD-R/RW, CD-R/RW, CF/SD Karte, etc.)? | Bitte geben Sie hier an, ob es technisch möglich ist personenbezogene Daten von Wechseldatenträgern auszulesen oder darauf zu schreiben und ob dies für die Zweckbestimmung notwendig ist. |
| MPII-3.4 | Kann das Produkt personenbezogene Daten über eine feste Kabelverbindung (z. B. RS-232, RS-423, USB, FireWire, etc.) empfangen oder versenden? | Bitte geben Sie hier an, ob es technisch möglich ist personenbezogene Daten über eine feste Kabelverbindung zu empfangen oder zu versenden und ob dies deaktivierbar/physikalisch geschützt ist. |
| MPII-3.5 | Kann das Produkt personenbezogene Daten über eine (drahtgebundene) Netzwerkverbindung empfangen oder versenden (z. B. RJ45, Glasfaser, etc.)? | Hier wird empfohlen, dass wenn die Antwort „yes“ lautet, auf das Kapitel TXCF verwiesen wird. |
| MPII-3.6 | Kann das Produkt personenbezogene Daten über eine drahtlose Netzwerkverbindung empfangen oder versenden (z. B. WiFi, Bluetooth, NFC, Infrarot, Mobiltelefon, etc.)? | Hier wird empfohlen, dass wenn die Antwort „yes“ lautet, auf das Kapitel TXCF verwiesen wird. |
| MPII-3.7 | Kann das Produkt personenbezogene Daten über externe Netzwerke (z. B. Internet) empfangen oder versenden? | |

| FragenID | Frage | Empfehlung |
|---|---|---|
| MPII-3.8 | Kann das Produkt personenbezogene Daten über Mechanismen zum Scannen importieren? | |
| MPII-3.9 | Kann das Produkt personenbezogene Daten über ein proprietäres Protokoll übertragen oder versenden? | |
| MPII-3.10 | Nutzt das Produkt andere Mechanismen, um personenbezogene Daten zu übertragen, zu importieren oder zu exportieren? Listen Sie diese bitte in einem Freitextfeld auf. | Hier sollten als Funktionen auch funkbasiertes (RFID) und das Lesen eines Fingerabdrucks oder anderer biometrischer Informationen, aufgeführt werden. |

## 3.3 Automatisches Abmelden (ALOF)

Die Fähigkeit des Produkts Zugriffe oder Missbrauch durch nicht autorisierte Nutzer zu verhindern, wenn das Gerät über einen gewissen Zeitraum nicht genutzt wird.

| FragenID | Frage | Empfehlung |
|---|---|---|
| ALOF-1 | Kann das Produkt so konfiguriert werden, dass es, nach einer gewissen Zeit der Inaktivität, den (angemeldeten) Nutzer dazu auffordert sich erneut zu autorisieren (z. B. durch eine automatische Abmeldung, Sitzungssperrung oder einen passwortgeschützter Bildschirmschoner). | Bitte geben Sie hier an, ob diese Mechanismen (erneute Anmeldung und passwortgeschützter Bildschirmschoner nach einer bestimmten Zeit der Inaktivität des Nutzers) voreingestellt sind oder ob sie konfigurierbar sind. Dies kann helfen zu verstehen, wie ein solcher Mechanismus ausgeschaltet werden kann (z. B. pro Session oder global durch entsprechende Warnungen an den Nutzer). |
| ALOF-2 | Ist das Zeitintervall, bevor es zu einer automatischen Abmeldung / Bildschirmsperre, bedingt durch Inaktivität kommt, durch Nutzer oder Administratoren konfigurierbar? Bitte geben Sie im Freitextfeld die Zeit, feste Vorgabe oder ein einstellbares Zeitintervall an. | Geben Sie bitte an, ob der Nutzer oder der Administrator das Zeitintervall für eine automatische Abmeldung/Bildschirmsperre selbständig konfigurieren kann. Präzisieren Sie bitte, ob das Produkt auf eine durch den Nutzer bestimmte Zeit oder durch eine zugewiesene Rolle (z. B. Administrator, Nutzer) konfiguriert werden kann. |

## 3.4 Revisionskontrolle (AUDT)

Die Fähigkeit zuverlässig Aktivitäten auf dem Produkt zu protokollieren und zu überwachen (Audit Trail).

| FragenID | Frage | Empfehlung |
|---|---|---|
| AUDT-1 | Kann das Produkt zusätzlich zu Protokollen des Betriebssystems weitere Audit-Protokolle oder Berichte erzeugen? | Falls Sie hier mit „no“ antworten, geben Sie bitte bei den Antworten AUDT-1.1 bis AUDT-8 „n/a“ an. |

| FragenID | Frage | Empfehlung |
|---|---|---|
| AUDT-1.1 | Wird die Nutzer-ID in den Audit-Protokollen mit aufgezeichnet? | Wenn dem so ist, geben Sie bitte an, ob das Datensubjekt (z. B. der Patient) für jede personenbezogene Information im Audit-Protokoll identifiziert werden kann. Geben Sie bitte zudem an, ob im Audit-Pfad zwischen dem Erstellen, Anzeigen, Exportieren, etc. von personenbezogenen Daten und anderen Daten unterschieden werden kann. |
| AUDT-1.2 | Existieren andere personenbezogene Daten im Audit-Protokoll? Wenn ja, beschreiben Sie dies bitte in einem Freitextfeld. | Wenn dem so ist, geben Sie bitte an, ob das Datensubjekt (z. B. der Patient) für jede personenbezogene Information im Audit-Protokoll identifiziert werden kann. Geben Sie bitte zudem an, ob im Audit-Pfad zwischen dem Erstellen, Anzeigen, Exportieren, etc. von personenbezogenen Daten und anderen Daten unterschieden werden kann. |
| AUDT-2 | Werden bestimmte Ereignisse durch das Audit-Protokoll aufgezeichnet? | Wenn Sie hier mit „yes“ antworten, spezifizieren Sie bitte die Ereignisse in den Freitextfeldern der folgenden Fragen. |
| AUDT-2.1 | Erfolgreiche Anmelde- und Abmeldeversuche? | |
| AUDT-2.2 | Nicht erfolgreiche Anmelde- und Abmeldeversuche? | |
| AUDT-2.3 | Veränderung der Nutzerrechte? | |
| AUDT-2.4 | Erstellen, Ändern oder Löschen von Nutzerkonten? | Hier ist gemeint, dass beispielsweise eine E-Mail-Adresse eines Nutzers geändert werden kann, nicht jedoch die Nutzerrechte, wie in AUDT-2.3. |
| AUDT-2.5 | Anzeige (z. B. Bildschirm, Ausdruck) von klinischen oder personenbezogenen Daten? | |
| AUDT-2.6 | Erzeugung, Veränderung oder Löschung von Daten? | Wenn Sie hier mit „yes“ antworten, geben Sie bitte an, welche Form der Datenmanipulation (Erzeugung und/oder Veränderung und/oder Löschung) mit aufgezeichnet wird. |
| AUDIT-2.7 | Import/Export von Daten über Wechseldatenträger (z. B. USB-Speicherstick, externe Festplatte, DVD)? | Wenn Sie hier mit „yes“ antworten, geben Sie bitte an, in welcher Detailtiefe die Daten erfasst werden (z. B. nur die Patienten-ID, eine Liste der Dokumenten-IDs). |
| AUDT-2.8 | Empfangen/Versenden von Daten und Kommandos über ein Netzwerk oder über direkte Punk-zu-Punkt-Verbindungen? | Wenn Sie hier mit „yes“ antworten, geben Sie bitte an, in welcher Detailtiefe die Daten erfasst werden (z. B. nur die Patienten-ID, eine Liste der Dokumenten-IDs). |

| FragenID | Frage | Empfehlung |
|---|---|---|
| AUDT-2.8.1 | Fernwartung oder Vor-Ort-Wartung? | Wenn Sie hier mit „yes“ antworten, geben Sie bitte an, welche Arten der Service-Aktivitäten aufgezeichnet werden. |
| AUDT-2.8.2 | Programmierschnittstellen (API) und ähnliche Aktivitäten? | Wenn Sie hier mit „yes“ antworten, geben Sie bitte die proprietären und die standardmäßigen Netzwerk APIs, wie z. B. FHIR bei HL7, an, die das Produkt unterstützt und deren Erfassung für die Audit-Protokolle.<br><br>Weisen Sie bitte zusätzlich darauf hin, ob weitere Informationen in der Produktdokumentation enthalten sind. |
| AUDT-2.9 | Notfall-Zugriff? | Wenn Sie hier mit „yes“ antworten, spezifizieren Sie bitte, welche Daten bei einem Notfall-Zugriff abgefragt werden und wie der Notfall-Zugriff dokumentiert wird. |
| AUDT-2.10 | Andere Vorkommnisse, z. B. Software-Updates? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| AUDT-2.11 | Werden die Audit-Fähigkeiten detaillierter beschrieben? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| AUDT-3 | Kann der Betreiber/Bediener selbständig auswählen oder festlegen, welche Vorkommnisse im Audit-Protokoll protokolliert werden? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| AUDT-4 | Existiert eine Liste der Attribute der Daten, die im Audit-Protokoll für ein Ereignis erfasst werden? Wenn ja, beschreiben Sie dies bitte in einem Freitextfeld. | Bitte geben Sie hier die Datenattribute an, die im Audit-Protokoll erfasst werden oder verweisen Sie auf die Produktdokumentation. |
| AUDT-4.1 | Erfasst das Audit-Protokoll Datum und Zeit? | |
| AUDT-4.1.1 | Können das Datum und die Zeit über das Netzwerk Zeit Protokoll (NTP) oder eine gleichwertige Zeitquelle synchronisiert werden? | Geben Sie hier bitte an, wie die Zeit gesetzt werden kann, wenn nicht NTP genutzt wird. |
| AUDT-5 | Können Audit-Log Inhalte exportiert werden? | |
| AUDT-5.1 | Über physische Medien? | |
| AUDT-5.2 | Über IHE Audit Trail und Node Authentication (ATNA) Profile nach SIEM? | |

| FragenID | Frage | Empfehlung |
|---|---|---|
| AUDT-5.3 | Über andere Kommunikationsverfahren (z. B. externe Servicegeräte, mobile Anwendungen)? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| AUDT-5.4 | Werden die Audit-Protokolle während des Transports oder auf den Speichermedien verschlüsselt? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| AUDT-6 | Können Audit-Protokolle durch den Kunden überwacht/geprüft werden? Wenn nein, beschreiben Sie bitte den Audit-Prozess im Freitextfeld. | |
| AUDT-7 | Werden die Audit-Protokolle vor Veränderung/Löschung geschützt? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| AUDT-7.1 | Werden die Audit-Protokolle vor dem Zugriff geschützt? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| AUDT-8 | Können Audit-Protokolle durch das Produkt selbst analysiert werden? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |

## 3.5 Berechtigungen (AUTH)

Die Fähigkeit des Produkts die Autorisierung des Nutzers zu erkennen.

| FragenID | Frage | Empfehlung |
|---|---|---|
| AUTH-1 | Verhindert das Produkt einen unautorisierten Zugriff durch eine Nutzeranmeldung oder andere Mechanismen? | Falls dem so ist, geben Sie bitte an, welche physischen oder technischen Sicherheitsmaßnahmen (Passwort, biometrische Merkmale, Chipkarten, Schlüsselkarten, etc.) durch das Produkt genutzt werden, um unautorisierten Zugriff zu verhindern. |
| AUTH-1.1 | Kann das Produkt so konfiguriert werden, dass es zentrale Verwaltungssysteme für die Benutzeranmeldung (z. B. LDAP, OAuth) zur Autorisierung der Nutzer verwendet? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| AUTH-1.2 | Können Kunden Gruppenrichtlinien (Policies) auf das Produkt übertragen (z. B. Active Directory)? | |

| FragenID | Frage | Empfehlung |
|---|---|---|
| AUTH-1.3 | Werden spezielle Benutzergruppen, organisatorische Einheiten oder Gruppenrichtlinien (Policies) benötigt? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | |
| AUTH-2 | Können Nutzer abgestufte Rechte zugeteilt bekommen, die auf dem Rollenprinzip basieren (z. B. Gast, regulärer Nutzer, Administrator)? | |
| AUTH-3 | Kann der Kunde des Produkts unbeschränkte administrative Rechte erlangen (z. B. auf das Betriebssystem oder lokale Applikationen über lokale Root-Rechte, bzw. den Administrator-Account)? | Bei einer Antwort mit „yes“, geben Sie bitte an, ob das Produkt mehrere privilegierte Benutzerkonten (z. B. Administrator, Root-Rechte) unterstützt und ob es Einschränkungen für Nutzer gibt, den Administrator-Account zu benutzen. Es sollte zudem deutlich zwischen Betreiber, einschließlich Installation, Wartung und Außerbetriebnahme, und Bediener, hier ist der Benutzer im medizinischen Normalbetrieb gemeint, unterschieden werden. |
| AUTH-4 | Werden alle Zugriffe zu Netzwerk-Schnittstellen (API) über eine Zugriffsautorisierung gesteuert? Falls nicht, erläutern Sie dies bitte im Freitextfeld. | Bitte stellen Sie hier die detaillierte Zugriffsautorisierung dar. |
| AUTH-5 | Läuft das Produkt standardmäßig in einem eingeschränkten Zugriffsmodus oder im Kiosk Modus (Auto-Login)? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |

## 3.6 Sicherheits-Upgrades für das Produkt (CSUP)

Die Fähigkeit durch Personal des Herstellers vor Ort, Fernwartungspersonal des Herstellers oder autorisiertes Kundenpersonal Sicherheits-Updates auf dem Produkt zu installieren oder zu aktualisieren.

| FragenID | Frage | Empfehlung |
|---|---|---|
| CSUP-1 | Läuft auf dem Produkt irgendwelche Software oder Firmware (damit ist sowohl vom Hersteller selbst als auch durch Drittanbieter hergestellte Software gemeint), die Sicherheits-Updates während ihrer geplanten Verwendungszeit benötigt. Wenn nicht, dann überspringen Sie dieses Kapitel. | Geben Sie bitte an, welche Randbedingungen es beim Aufspielen von Sicherheits-Updates gibt und verweisen Sie auf die Produktdokumentation, die diese Randbedingungen näher bezeichnet. |

| FragenID | Frage | Empfehlung |
|---|---|---|
| CSUP-2 | Beinhaltet das Produkt ein Betriebssystem? Wenn ja, füllen Sie bitte die nachfolgenden Fragen, bis einschließlich 2.4 aus. | Geben Sie bitte an, welche Randbedingungen es beim Aufspielen von Sicherheits-Updates gibt und verweisen Sie auf die Produktdokumentation, die diese Randbedingungen näher bezeichnet. Wenn Sie „no“ angeben und ein Betriebssystem erforderlich ist (SaMD), beantworten Sie bitte auch die Fragen bis einschließlich 2.4. |
| CSUP-2.1 | Liefert die Produktdokumentation Anleitungen für den Bediener oder Betreiber, wie Software-Patches oder Updates des Betriebssystems durchgeführt werden? | |
| CSUP-2.2 | Benötigt das Produkt den Hersteller oder herstellereigenen Service, um Software-Patches oder Updates für das Betriebssystem durchzuführen? | |
| CSUP-2.3 | Ist es möglich Software-Patches und Updates für das Betriebssystem auf dem Produkt per Fernwartung zu installieren? | |
| CSUP-2.4 | Ist es erlaubt, dass Sicherheits-Updates für das Betriebssystem durch Dritt-Komponenten-Anbieter (z. B. Microsoft) ohne vorherige Freigabe des Herstellers installiert werden? | Geben Sie bitte auch dann „no“ an, wenn es eine generische, vom Hersteller vorgegebene Freigabeprozedur gibt und erklären Sie diese. |
| CSUP-3 | Beinhaltet das Produkt Treiber und Firmware? Wenn ja, füllen Sie bitte die nachfolgenden Fragen, bis einschließlich 3.4 aus. | Geben Sie bitte an, welche Randbedingungen es beim Aufspielen von Sicherheits-Updates gibt und verweisen Sie auf die Produktdokumentation, die diese Randbedingungen näher bezeichnet. |
| CSUP-3.1 | Liefert die Produktdokumentation Anleitungen für den Bediener oder Betreiber, wie Software-Patches oder Updates für das Produkt selbst durchgeführt werden? | |
| CSUP-3.2 | Benötigt das Produkt den Hersteller oder herstellereigenen Service, um Software-Patches oder Updates für das Produkt selbst durchzuführen? | |
| CSUP-3.3 | Ist es möglich Software-Patches und Updates für das Produkt selbst auf dem Produkt per Fernwartung zu installieren? | |

| FragenID | Frage | Empfehlung |
|---|---|---|
| CSUP-3.4 | Ist es erlaubt, dass Sicherheits-Updates für das Produkt selbst durch Dritt-Komponenten-Anbieter (z. B. Microsoft) ohne vorherige Freigabe des Herstellers installiert werden? | Diese Frage zielt auf den Fall, dass das Produkt Komponenten von Dritt-Anbietern enthält. |
| CSUP-4 | Benutzt das Produkt Anti-Schadsoftware? Wenn ja, füllen Sie bitte die nachfolgenden Fragen, bis einschließlich 4.4 aus. | Geben Sie bitte an, welche Randbedingungen es beim Aufspielen von Updates dieser Anti-Schadsoftware gibt und verweisen Sie auf die Produktdokumentation, die diese Randbedingungen näher bezeichnet. |
| CSUP-4.1 | Liefert die Produktdokumentation Anleitungen für den Bediener oder Betreiber, wie Software-Patches oder Updates der Anti-Schadsoftware durchgeführt werden? | |
| CSUP-4.2 | Benötigt das Produkt den Hersteller oder herstellereigenen Service, um Software-Patches oder Updates der Anti-Schadsoftware durchzuführen? | |
| CSUP-4.3 | Ist es möglich Software-Patches und Updates der Anti-Schadsoftware auf dem Produkt per Fernwartung zu installieren? | |
| CSUP-4.4 | Ist es erlaubt, dass Sicherheits-Updates der Anti-Schadsoftware durch Dritt-Komponenten-Anbieter (z. B. Microsoft) ohne vorherige Freigabe des Herstellers installiert werden? | |
| CSUP-5 | Beinhaltet das Produkt weitere handelsübliche (Software-)Komponenten (COTS), die nicht zum Betriebssystem gehören? Wenn ja, füllen Sie bitte die nachfolgenden Fragen, bis einschließlich 5.4 aus. | Geben Sie bitte an, welche Randbedingungen es beim Aufspielen von Sicherheits-Updates gibt und verweisen Sie auf die Produktdokumentation, die diese Randbedingungen näher bezeichnet. |
| CSUP-5.1 | Liefert die Produktdokumentation Anleitungen für den Bediener oder Betreiber, wie Software-Patches oder Updates dieser handelsüblichen Komponenten durchgeführt werden? | |
| CSUP-5.2 | Benötigt das Produkt den Hersteller oder herstellereigenen Service, um Software-Patches oder Updates dieser handelsüblichen Komponenten durchzuführen? | |
| CSUP-5.3 | Ist es möglich Software-Patches und Updates dieser handelsüblichen Komponenten auf dem Produkt per Fernwartung zu installieren? | |

| FragenID | Frage | Empfehlung |
|---|---|---|
| CSUP-5.4 | Ist es erlaubt, dass Sicherheits-Updates dieser handelsüblichen Komponenten durch Dritt-Komponenten-Anbieter (z. B. Microsoft) ohne vorherige Freigabe des Herstellers installiert werden? | |
| CSUP-6 | Gibt es auf dem Produkt weitere Software-Komponenten (z. B. Assetmanagement-Software oder Lizenzverwaltungsprogramme)? Wenn ja, füllen Sie bitte die nachfolgenden Fragen, bis einschließlich 6.4 aus. | Geben Sie bitte an, welche Randbedingungen es beim Aufspielen von Sicherheits-Updates gibt und verweisen Sie auf die Produktdokumentation, die diese Randbedingungen näher bezeichnet. |
| CSUP-6.1 | Liefert die Produktdokumentation Anleitungen für den Bediener oder Betreiber, wie Software-Patches oder Updates der weiteren Software-Komponenten durchgeführt werden? | |
| CSUP-6.2 | Benötigt das Produkt den Hersteller oder herstellereigenen Service, um Software-Patches oder Updates der weiteren Software-Komponenten durchzuführen? | |
| CSUP-6.3 | Ist es möglich Software-Patches und Updates der weiteren Software-Komponenten auf dem Produkt per Fernwartung zu installieren? | |
| CSUP-6.4 | Ist es erlaubt, dass Sicherheits-Updates der weiteren Software-Komponenten durch Dritt-Komponenten-Anbieter (z. B. Microsoft) ohne vorherige Freigabe des Herstellers installiert werden? | |
| CSUP-7 | Informiert der Hersteller den Kunden, wenn Updates zur Installation freigegeben worden sind? Wenn ja, beschreiben Sie dies bitte genauer im Freitextfeld. | Bitte geben Sie hier an, über welchen Kommunikationskanal Sie diese Informationen zur Verfügung stellen und ob es sich um das Betriebssystem, die Hauptapplikations-Software, Anti-Schadsoftware, kommerzielle Software oder um weitere Komponenten handelt. |
| CSUP-8 | Kann das Produkt automatisch Software-Updates installieren? | Bitte geben Sie hier an, ob es sich um das Betriebssystem, die Hauptapplikations-Software, Anti-Schadsoftware, kommerzielle Software oder um weitere Komponenten handelt. |
| CSUP-9 | Hat der Hersteller eine Liste von geprüfter Dritt-Anbieter-Software, die auf dem Produkt installiert werden kann? Wenn ja, referenzieren Sie dies bitte in einem Freitextfeld. | Geben Sie bitte die Liste der geprüften Dritt-Anbieter-Software an oder verweisen Sie auf diese. Zudem beschreiben Sie bitte den Genehmigungsprozess bei Anfragen von weiterer Dritt-Anbieter-Software. |

| FragenID | Frage | Empfehlung |
|---|---|---|
| CSUP-10 | Kann der Betreiber/Bediener vom Hersteller freigegebene Software von Dritt-Anbietern auf dem Produkt installieren? | Hier sollten Sie bitte zwischen den unterschiedlichen Rollen unterscheiden und ob es beispielsweise möglich ist, dass auch Anwender Installationsrechte erhalten. |
| CSUP-10.1 | Verfügt das Produkt über einen Mechanismus, um der Installation von nicht geprüfter Software vorzubeugen? | Bitte geben Sie hier auch Whitelisting-Software an. |
| CSUP-11 | Verfügt der Hersteller über einen Prozess, um Schwachstellen und Updates zu bewerten? | Hier ist es auch möglich den Prozess verallgemeinert darzustellen und eine entsprechende Fallunterscheidung (Betriebssystem, Hauptapplikations-Software, Anti-Schadsoftware, kommerzielle Software oder weitere Komponenten) vorzunehmen. |
| CSUP-11.1 | Verfügt der Hersteller über einen Prozess, der den Kunden regelmäßig über Updates, mit einem Bewertungs- und Genehmigungsstatus, informiert? | |
| CSUP-11.2 | Gibt es einen regelmäßigen Update-Zyklus? Wenn ja, beschreiben Sie diesen bitte im Freitextfeld. | |

## 3.7 De-Identifikation von Gesundheitsdaten (DIDT)

Die Fähigkeit des Produkts Informationen direkt entfernen zu können, die es ermöglichen eine Person zu identifizieren.

| FragenID | Frage | Empfehlung |
|---|---|---|
| DIDT-1 | Verfügt das Produkt über einen eingebauten Mechanismus, um personenbezogene Daten zu de-identifizieren? | Bitte geben Sie hier an, ob sich der Anonymisierungs- oder Pseudonymisierungs-Prozess nach einem Standard oder einer Hilfestellung richtet und ob der Mechanismus verschieden konfiguriert werden kann. |
| DIDT-1.1 | Unterstützt das Produkt eine Anonymisierung von Profilen nach dem DICOM-Standard? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | DICOM-Standards werden bei medizinischen, bildgebenden Verfahren verwendet. |

## 3.8 Datensicherungs- und Wiederherstellungsmechanismen (DTBK)

Wiederherstellungsmöglichkeiten nach Beschädigung oder Zerstörung von Daten, Hardware, Software oder Konfigurationsinformationen.

| FragenID | Frage | Empfehlung |
|---|---|---|
| DTBK-1 | Hat das System einen (primären) Langzeitspeicher von personenbezogenen Daten oder andere Patientendaten (z. B. PACS)? | |
| DTBK-2 | Ist es möglich, dass das Produkt auf Werkseinstellungen zurückgesetzt werden kann? | |
| DTBK-3 | Verfügt das Produkt über eine eingebaute Möglichkeit eine Datensicherung auf einem Wechseldatenträger zu erstellen? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | Bitte geben Sie an, ob es Einschränkungen bei der Wiederherstellung von Daten oder bei der Notfallwiederherstellung gibt. Beziehen Sie sich bitte dabei auf die eingebauten Funktionen oder Optionen, die es erlauben, dass Wiederherstellungsdateien auf Wechseldatenträgern (z. B. optischer Plattenspeicher, Magnetplatte, Magnetband, etc.) gespeichert werden. |
| DTBK-4 | Verfügt das Produkt über eine eingebaute Möglichkeit eine Datensicherung auf einem nicht lokalen Speicher durchzuführen? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | Bitte geben Sie an, ob es Einschränkungen bei der Wiederherstellung von Daten oder bei der Notfallwiederherstellung gibt. Beziehen Sie sich bitte dabei auf die eingebauten Funktionen oder Optionen, die es erlauben, dass Wiederherstellungsdateien auf nicht lokalen Speichern zu sichern. Bitte beschreiben Sie zudem, wie die Daten geschützt werden (z. B. durch Verschlüsselung oder Weglassen dieser Daten). |
| DTBK-5 | Verfügt das Produkt über die Möglichkeit eine Sicherung der Konfigurationsdaten sowie eine Patch-/Software-Wiederherstellung durchzuführen? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | Bitte geben Sie an, ob es Einschränkungen bei der Wiederherstellung von Daten oder bei der Notfallwiederherstellung gibt. Beziehen Sie sich bitte dabei auf die eingebauten Funktionen oder Optionen, die es erlauben, dass Wiederherstellungsdateien auf lokalen Speichern oder nicht lokalen Speichern über das Netzwerk zu sichern. Bitte beschreiben Sie zudem, wie die personenbezogenen Daten geschützt werden (z. B. durch Verschlüsselung oder Ausnahme vom Wiederherstellungsprozess). |
| DTBK-6 | Verfügt das Produkt über die Möglichkeit die Integrität und Authentizität von Wiederherstellungsdateien zu prüfen? | |

## 3.9 Notfallzugriff (EMRG)

Die Möglichkeit für den Nutzer des Produkts auf personenbezogene Daten zugreifen zu können die im Falle eines medizinischen Notfalls benötigt werden und auf dem Produkt gespeichert sind.

| FragenID | Frage | Empfehlung |
|---|---|---|
| EMRG-1 | Bietet das Produkt eine Funktion für den Notfallzugriff (z. B. "break-the-glass-Konzept")? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | Falls es eine solche Funktion gibt, beschreiben Sie bitte, in wieweit beim Notfallzugriff auf personenbezogene Daten zugegriffen werden kann. Der Notfallzugriff kann auch Teil der Zweckbestimmung sein. |

## 3.10 Integrität und Authentizität von Gesundheitsdaten (IGAU)

Wie das Produkt sicherstellt, dass gespeicherte Daten auf dem Produkt nicht ohne Autorisierung verändert oder gelöscht werden können und auch wirklich vom Erzeuger stammen und wie die Verfügbarkeit sichergestellt wird.

| FragenID | Frage | Empfehlung |
|---|---|---|
| IGAU-1 | Verfügt das Produkt über Mechanismen zur Prüfung der Integrität gespeicherter Gesundheitsdaten (z. B. durch Hash-Werte oder digitale Signaturen)? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| IGAU-2 | Bietet das Produkt Fehlersicherungsfunktionen und Wiederherstellungsmechanismen für gespeicherte Gesundheitsdaten (z. B. RAID-5)? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | |

## 3.11 Detektion von und Schutz vor Malware (MLDP)

Die Fähigkeit des Produkts Schadsoftware effektiv zu verhindern und zu erkennen.

| FragenID | Frage | Empfehlung |
|---|---|---|
| MLDP-1 | Ist das Produkt in der Lage ausführbare Software zu hosten? | Unter „ausführbarer Software hosten" ist zu verstehen, dass beliebige Software aus anderen Quellen installiert oder ausgeführt werden kann, auch wenn diese nicht vom Hersteller freigegeben ist. |
| MLDP-2 | Unterstützt das Produkt die Verwendung von Anti-Schadsoftware (oder anderen Mechanismen zur Abwehr von Schadprogrammen)? | Geben Sie bitte an, ob es Einschränkungen beim Anti-Schadsoftware-Support, bei der Beschaffung, bei der Installation oder bei der Konfiguration gibt oder geben Sie entsprechende Produktdokumente als Referenz an, in der diese Einschränkungen aufgeführt sind. |

| FragenID | Frage | Empfehlung |
|---|---|---|
| MLDP-2.1 | Besitzt das Produkt bei der Auslieferung bereits vorinstallierte Anti-Schadsoftware? | |
| MLDP-2.2 | Besitzt das Produkt die Option Anti-Schadsoftware nach der Auslieferung zu installieren oder zu aktivieren? | |
| MLDP-2.3 | Kann der Betreiber/Bediener des Produktes Anti-Schadsoftware installieren oder aktualisieren? | Geben Sie hier bitte an, ob es Berechtigungen des Betreibers gibt, die erlaubten Einstellungen an Anti-Schadsoftware vorzunehmen. |
| MLDP-2.4 | Kann der Betreiber/Bediener des Produktes unabhängig Einstellungen ändern oder Anti-Schadsoftware (re-)konfigurieren? | |
| MLDP-2.5 | Erscheinen Warnmeldungen über erkannte Schadsoftware auf der Benutzeroberfläche des Produktes? | Wenn Sie hier mit „no“ antworten, führen Sie bitte auf, wie der Nutzer gewarnt wird, wenn Schadsoftware detektiert wird. |
| MLDP-2.6 | Kann das Produkt nur durch vom Hersteller autorisiertes Personal repariert werden, wenn Schadsoftware darauf entdeckt worden ist? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| MLDP-2.7 | Werden Warnmeldungen in ein Audit-Log oder ein Wartungsprotokoll geschrieben? | |
| MLDP-2.8 | Gibt es Einschränkungen bei der Nutzung von Anti-Schadsoftware (Beschaffung, Installation, Konfiguration, Planung)? | |
| MLDP-3 | Wenn Sie bei MLDP-2 mit „no“ geantwortet haben und keine Anti-Schadsoftware auf dem Produkt installiert werden kann, sind andere Schutzmechanismen implementiert oder verfügbar? | Wenn Sie bei MLDP-2 mit „yes“ geantwortet haben, so können Sie hier ein „n/a“ eintragen. |
| MLDP-4 | Kann das Produkt derart konfiguriert werden, dass eine spezifische Gruppe von Programmen und Diensten auf dem Produkt zugelassen werden (Whitelisting)? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| MLDP-5 | Kann ein Host-basiertes System zur Erkennung oder Abwehr von Angriffen konfiguriert oder installiert werden? | Wenn Sie hier mit „yes“ antworten, füllen Sie bitte MLDP-5.1 und MLDP-5.2 entsprechend aus. |

| FragenID | Frage | Empfehlung |
|---|---|---|
| MLDP-5.1 | Kann ein Host-basiertes System zur Erkennung oder Abwehr von Angriffen durch den Kunden konfiguriert werden? | |
| MLDP-5.2 | Kann ein Host-basiertes System zur Erkennung oder Abwehr von Angriffen durch den Kunden installiert werden? | |

## 3.12 Authentisierung von Kommunikationspartnern (NAUT)

Beschreibt die Fähigkeit des Produkts die Kommunikationspartner/ Knoten zu authentifizieren.

| FragenID | Frage | Empfehlung |
|---|---|---|
| NAUT-1 | Besitzt oder unterstützt das Produkt irgendeine Form der Verbindungsauthentifizierung, die sicherstellt, dass sowohl der Sender als auch der Empfänger von Daten sich gegenseitig erkennen und autorisiert sind die gesendeten Daten zu empfangen (z. B. Web APIs, SMTP, SNMP)? Wenn ja, beschreiben Sie dies bitte kurz im Freitextfeld. | |
| NAUT-2 | Werden Steuerungsmechanismen für den Netzwerkzugriff unterstützt (z. B. eine interne Firewall oder verwendet das Produkt Whitelisting für Netzwerkverbindungen)? Wenn ja, beschreiben Sie dies bitte kurz im Freitextfeld. | |
| NAUT-2.1 | Sind die Einstellungen der Firewall dokumentiert und verfügbar zur Durchsicht? Wenn ja, beschreiben Sie bitte, wie diese eingesehen werden können im Freitextfeld. | |
| NAUT-3 | Verwendet das Produkt Zertifikate für die Autorisation von Netzwerkverbindungen? Wenn ja, beschreiben Sie bitte im Freitextfeld, wie die Zertifikate verwaltet werden. | Bitte geben Sie an, wie die Zertifikate verwaltet werden (Zertifikatsmanagement). Geben Sie gegebenenfalls auch nötige technische Eigenschaften der unterstützten Zertifikate und Protokolle an, wie beispielsweise die unterstützten Schlüssellängen für asymmetrische Verschlüsselungen. |

## 3.13 Verbindungs- und Vernetzungsmöglichkeiten (CONN)

Alle Verbindungen zu Netzwerken und Wechseldatenträgern müssen berücksichtigt werden, wenn angemessene Sicherheitsmaßnahmen getroffen werden sollen. Dieser Abschnitt beschreibt alle Optionen, die ein Produkt bietet, dieses mit anderen zu verbinden.

| FragenID | Frage | Empfehlung |
|---|---|---|
| CONN-1 | Kann das Produkt in ein Netzwerk eingebunden werden? Wenn Sie hier mit „yes“ antworten, beschreiben Sie bitte die Hardwarekomponenten. Wenn Sie mit „no“ antworten, schreiben Sie bitte „n/a“ für alle kommenden Fragen. | Bitte listen Sie alle installierten oder optional installierbaren Hardwarekomponenten und die Grundfunktionalitäten des Betriebssystems, die das Produkt benötigt, um in einem Netzwerk eingebunden werden zu können. Beschreiben Sie bitte, ob diese Funktionen käuflich zu erwerben sind oder ausgeschaltet werden können. |
| CONN-1.1 | Unterstützt das Produkt kabellose Netzwerkverbindungen? | |
| CONN-1.1.1 | Unterstützt das Produkt WLAN? Wenn ja, führen Sie bitte eine Liste der unterstützten Authentifizierungsprotokolle (z. B. WPA2 EAP-TLS) in einem Freitextfeld auf. | Hier sollen nur die Authentifizierungsprotokolle für WLAN angegeben werden. |
| CONN-1.1.2 | Unterstützt das Produkt Bluetooth? Wenn ja, führen Sie bitte die vom Produkt unterstützten Bluetooth-Sicherheitsmechanismen in einem Freitextfeld auf und ob diese erzwungen werden können. | |
| CONN-1.1.3 | Unterstützt das Produkt noch weitere kabellose Netzwerkverbindungen (z. B. Zigbee oder proprietäre Lösungen)? Wenn ja, beschreiben Sie diese bitte in einem Freitextfeld. | Hier sind alle drahtlosen Netzwerke, außer WLAN und Bluetooth, gemeint. |
| CONN-1.1.4 | Unterstützt das Produkt darüber hinaus noch weitere kabellose Verbindungen (z. B. kundenspezifische RF-Kontrollen, kabellose Detektoren)? Wenn ja, beschreiben Sie diese bitte in einem Freitextfeld. | |
| CONN-1.2 | Unterstützt das Produkt physische Netzwerkverbindungen? | |
| CONN-1.2.1 | Besitzt das Produkt nutzbare RJ45 Ethernet-Ports? Wenn ja, beschreiben Sie bitte im Freitextfeld, wie diese genutzt und gesichert werden. | |
| CONN-1.2.2 | Besitzt das Produkt nutzbare USB-Ports? Wenn ja, beschreiben Sie bitte im Freitextfeld, wie diese genutzt und gesichert werden. | Die Sicherung kann auch eine physische Sicherung sein. Bitte verweisen Sie dann auf PLOK. |
| CONN-1.2.3 | Werden Wechseldatenträger von dem Produkt verwendet, unterstützt oder sind diese sogar für die Nutzung notwendig? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | |

| FragenID | Frage | Empfehlung |
|---|---|---|
| CONN-1.2.4 | Unterstützt das Produkt weitere physische Verbindungen? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | |
| CONN-2 | Stellt der Hersteller eine Liste aller Netzwerkports und -protokolle zur Verfügung, die im Produkt genutzt werden oder genutzt werden können? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | Beschreiben Sie bitte, ob die Netzwerkprotokolle für ein vernetztes Produkt vonnöten sind. Bitte listen Sie die Transportprotokolle (z. B. IPv4, IPv6), die Anwendungsprotokolle (z. B. DICOM, IEEE 11073, HL7) oder andere Serviceprotokolle (z. B. DHCP, SMB, RDP) und andere kundenspezifische Protokolle sowie die entsprechende Versionsnummer, wenn dies angezeigt ist. |
| CONN-3 | Kommuniziert das Produkt im Normalbetrieb mit anderen Systemen innerhalb der Umgebung des Nutzers, als Teil seiner Zweckbestimmung? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | |
| CONN-4 | Kommuniziert das Produkt im Normalbetrieb mit weiteren Systemen, die nicht zur Umgebung des Nutzers gehören (z. B. Diensteanbieter)? Wenn ja, beschreiben Sie bitte im Freitextfeld den Zweck dieser Funktion. | |
| CONN-5 | Macht oder erhält das Produkt API-Aufrufe? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| CONN-6 | Benötigt das Produkt eine Internetverbindung für die Zweckbestimmung? Wenn ja, beschreiben Sie bitte, warum diese Verbindung notwendig ist im Freitextfeld. | |
| CONN-7 | Unterstützt das Produkt Transport Layer Security (TLS)? Wenn ja, beschreiben Sie bitte, welche Versionen unterstützt und welche verboten sind im Freitextfeld. | Falls das Produkt zu TLS äquivalente Mechanismen verwendet, geben Sie bitte „yes“ an und beschreiben Sie das verwendete Protokoll und seine Version. |
| CONN-7.1 | Ist TLS konfigurierbar? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | Geben Sie bitte hier beispielsweise den verwendeten Satz an Cipher Suites an. |
| CONN-8 | Kann der Betreiber die Funktionen des Produkts über ein separates Gerät kontrollieren (z. B. Telemedizin)? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | |

## 3.14 Authentifizierung und Autorisierung von Personen (PAUT)

Die Möglichkeit das Produkt so zu konfigurieren, dass Nutzer authentifiziert werden können.

| FragenID | Frage | Empfehlung |
|---|---|---|
| PAUT-1 | Ist das Produkt so konfigurierbar, dass eindeutige Nutzer-/Bedienernamen und Passwörter für alle Nutzer und Rollen, Service-Zugänge eingeschlossen, unterstützt werden? | |
| PAUT-1.1 | Ist das Produkt so konfigurierbar, dass eine Authentisierung eindeutiger Nutzer-/Bedienernamen und Passwörter für alle Nutzer und Rollen, Service-Zugänge eingeschlossen, unterstützt wird? | |
| PAUT-2 | Ist das Produkt so konfigurierbar, dass die Authentifizierung der Nutzer durch einen externen Authentifizierungsdienst (z. B. MS Active Directory, NDS, LDAP) erfolgen kann? | Bitte spezifizieren Sie, welche Mechanismen genutzt werden. |
| PAUT-3 | Ist das Produkt so konfigurierbar, dass es Nutzer nach einer bestimmten Anzahl von fehlgeschlagenen Anmeldeversuchen sperrt? | Bitte geben Sie hier möglichst viele Details für Funktionen zur Abmeldung der Nutzer an. |
| PAUT-4 | Werden alle voreingestellten Standard-Nutzer-Konten (z. B. technischer Service, Administrator) in der Dokumentation aufgeführt? Wenn nicht, geben Sie dies bitte im Freitextfeld an. | |
| PAUT-5 | Können alle Standard-Passwörter geändert werden? Wenn nicht, geben Sie dies bitte im Freitextfeld an. | |
| PAUT-6 | Kann das Produkt dahingehend konfiguriert werden bestimmte (Organisationsspezifische) Regelungen zur Komplexität von Passwörtern bei der Erstellung von Nutzerkonten zu erzwingen? Wenn es irgendwelche Grenzen gibt die Passwörter einzuschränken, listen sie diese bitte in einem Freitextfeld auf. | Bitte antworten Sie mit „yes“, wenn die Komplexität des Passworts konfigurierbar ist. Bitte antworten Sie mit „no“, wenn die Komplexität des Passworts nicht konfigurierbar ist. Bitte beschreiben Sie die Komplexitätsregeln und -grenzen. |
| PAUT-7 | Kann das Produkt dahingehend konfiguriert werden, dass Passwörter periodisch ihre Gültigkeit verlieren? | Bitte geben Sie die Gültigkeitsdauer an und ob administrierbare Kontrolle vorhanden sind. |
| PAUT-8 | Unterstützt das Produkt eine Multi-Faktor-Authentifizierung? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |

| FragenID | Frage | Empfehlung |
|---|---|---|
| PAUT-9 | Unterstützt das Produkt die Möglichkeit des Single-Sign-On (SSO)? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| PAUT-10 | Können Nutzerkonten auf dem Produkt gesperrt oder deaktiviert werden? | |
| PAUT-11 | Unterstützt das Produkt biometrische Anmeldeverfahren? | |
| PAUT-12 | Unterstützt das Produkt physikalische Token? | |
| PAUT-13 | Unterstützt das Produkt Gruppen-Authentisierung (z. B. von Krankenhaus-Teams)? | Hier sind rollenbasierte Zugriffskontrollen (role-based access control) oder ähnliche Kontrollschemata gemeint. Bitte verweisen Sie ggf. auf die DSGVO. |
| PAUT-14 | Speichert oder verwaltet das Produkt oder die Anwendung selbst die Anmeldedaten für Personen? Wenn ja, beschreiben Sie bitte wie das Produkt dies implementiert hat im Freitextfeld. | |
| PAUT-14.1 | Werden die Anmeldeinformationen von Personen sicher gespeichert? Wenn ja, beschreiben Sie bitte wie das Produkt dies implementiert hat im Freitextfeld. | |

## 3.15 Physische Zugriffssperren (PLOK)

Physische Sperren können verhindern, dass unautorisierte Nutzer, die physischen Zugriff zum Produkt haben, die Integrität und Vertraulichkeit der personenbezogenen Daten auf dem Produkt oder dazugehörigen Wechseldatenträgern kompromittieren können.

| FragenID | Frage | Empfehlung |
|---|---|---|
| PLOK-1 | Handelt es sich bei dem Produkt um ein reines Software-Produkt? | Wenn dem so ist, beantworten Sie bitte die nachfolgenden Antworten aus diesem Bereich mit „n/a“. |
| PLOK-2 | Sind alle Komponenten des Produkts, die private Daten beinhalten (abgesehen von Wechseldatenträgern) physisch abgesichert (d. h. können diese nicht ohne Werkzeug entfernt werden)? | Diese Frage bezieht sich auf die typische Installation und Konfiguration des Produkts. Bitte beachten Sie bei der Beantwortung der Frage auch die interne Speicherung von personenbezogene Daten sowie auf anderen Speichermedien. Beantworten Sie die Frage bitte mit „yes“, wenn physisch auf die Speichermedien zugegriffen werden kann oder sie mittels Werkzeug ausgebaut werden können. Hier wäre ein physischer Schlüssel als Werkzeug zu erachten. |

| FragenID | Frage | Empfehlung |
|---|---|---|
| PLOK-3 | Werden alle Komponenten des Produkts, die private Daten beinhalten (abgesehen von Wechseldatenträgern) physisch durch einen einzigartigen Schließmechanismus geschützt? | |
| PLOK-4 | Bietet das Produkt die Möglichkeit für den Kunden ein physisches Schloss anzubringen, um den Zugang zu Wechseldatenträgern zu verhindern? | |

## 3.16 Entwicklungsplan von Drittanbieter-Softwarekomponenten über den gesamten Lebenszyklus (RDMP)

Die Pläne des Herstellers für die Unterstützung der Sicherheit von Drittanbieter-Komponenten innerhalb des gesamten Lebenszyklus des Produkts, einschließlich End-of-Life.

| FragenID | Frage | Empfehlung |
|---|---|---|
| RDMP-1 | Wurde ein sicherer Software-Entwicklungsprozess, wie ISO/IEC 27034 oder IEC 62304, während der Produktentwicklung implementiert? | Bitte geben Sie die Standards zur sicheren Softwareentwicklung, die bei diesem Produkt verwendet wurden, an oder beschreiben Sie kurz den Softwareentwicklungsprozess. |
| RDMP-2 | Bewertet der Hersteller des Medizinprodukts, ob die Anwendungen und Softwarekomponenten von Drittanbietern in einem sicheren Produktentwicklungsprozess entwickelt werden? | Die sicheren Produktentwicklungsprozesse von Drittanbieter-Software, einschließlich open source-Software, sollen durch den Hersteller bewertet werden. |
| RDMP-3 | Stellt der Hersteller eine Webseite oder andere Quellen zur Verfügung, die Informationen zur Support-Dauer und Updates liefern? Wenn ja, bitte führen Sie die URL oder andere Möglichkeiten zum Zugang im Freitextfeld auf. | |
| RDMP-4 | Gibt es herstellerseitig einen Plan, wie das Ende der Lebenszeit von Drittkomponenten adressiert wird? | |

## 3.17 Liste aller Softwarekomponenten (SBOM)

Das Software Bill of Materials (SBoM) ist eine Liste von Software Komponenten, welche im beschriebenen Produkt integriert sind und beschrieben werden, damit der Betreiber Sicherheitsmaßnahmen ergreifen kann. Diese Liste dient dem Zweck der Planung, Vorbereitung und Durchführung von Sicherheitsmaßnahmen durch den Anbieter der Gesundheitsleistung. Dies beinhaltet auch Informationen für das Management der Assets sowie Notfallmanagement.

| FragenID | Frage | Empfehlung |
|---|---|---|
| SBOM-1 | Ist das SBoM für dieses Produkt verfügbar? | Geben Sie bitte an, wie sie das SBoM zur Verfügung stellen und ob es Einschränkungen gibt (z. B. Non-Disclosure Agreements). Das SBoM kann direkt tabellarisch oder per Hyperlink in das MDS2-Formular eingepflegt werden. |
| SBOM-2 | Ist im SBoM eine allgemeine oder standardisierte Methode vorgesehen, die Softwarekomponenten zu beschreiben? Wenn ja, nennen Sie diese bitte im Freitextfeld. | |
| SBOM-2.1 | Sind die Softwarekomponenten benannt? | Hier ist zu beachten, dass mindestens die oberste Paketebene benannt wird (z. B. Linux Distribution). |
| SBOM-2.2 | Sind die Entwickler/Hersteller der Softwarekomponenten benannt? | |
| SBOM-2.3 | Sind die Hauptversions-Nummern der Softwarekomponenten benannt? | |
| SBOM-2.4 | Sind zusätzliche beschreibende Elemente vorhanden? | Zusätzliche Informationen zu beschreibenden Elementen (z. B. Patch-Tags, Software ID-Tags) sind in den folgenden Standards und Dokumenten enthalten:<br>ISO/IEC 19770-2:2015, Software Data Exchange (SPDX) 2.1. |
| SBOM-3 | Existiert ein Befehl oder eine Methode um die installierten Softwarekomponenten auf dem Produkt aufzulisten? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | Hiermit ist gemeint, dass der Betreiber in der Lage sein muss die installierten Softwarekomponenten, soweit zutreffend mit Versionsnummer, nachzuvollziehen. |
| SBOM-4 | Existiert ein Update-Prozess für das SBoM? Wenn ja, beschreiben Sie diesen bitte im Freitextfeld oder referenzieren Sie dort das verwendete Quellmaterial. Wenn ja, beschreiben oder zeigen Sie diese Referenzen im Freitextfeld. | Hier ist zu empfehlen, dass beschrieben wird, wie das SBoM und auch das Software-Produkt herstellerseitig aktualisiert wird, so dass sich der Betreiber darauf einstellen kann, in welcher Häufigkeit Aktualisierungen geplant sind und auf welchen Wegen er hierüber informiert wird, bzw. sich informieren kann. |

## 3.18 System- und Anwendungshärtung (SAHD)

Die dem Produkt inhärente Widerstandsfähigkeit gegen Cyberangriffe und Schadsoftware.

| FragenID | Frage | Empfehlung |
|---|---|---|
| SAHD-1 | Wurde das Produkt in Übereinkunft mit Industriestandards gehärtet? Wenn ja, beschreiben Sie die Härtungsmaßnahmen im Freitextfeld. | Unter die möglichen System-Härtungsmaßnahmen fallen beispielsweise der BSI-Grundschutz oder DISA-STIGs. Es ist zu empfehlen, dass bei Produkten, die nur aus Software (SaMD) bestehen, beschrieben wird, welcher Standard für das Produkt angewendet werden kann. |
| SAHD-2 | Besitzt das Produkt Zertifizierungen oder Bescheinigungen zu Cyber-Sicherheitseigenschaften? Wenn ja, beschreiben Sie dies im Freitextfeld. | |
| SAHD-3 | Verfügt das Produkt über einen Mechanismus zur Prüfung der (Software-)Integrität? | Bitte geben Sie an, welche Mechanismen implementiert wurden, um die Anwendungsprogramme, die Systemkonfiguration und/oder die Gerätedaten vor Manipulationen zu schützen. |
| SAHD-3.1 | Verfügt das Produkt über einen Mechanismus, der prüft, ob die installierte Software vom Hersteller autorisiert ist (z. B. einen releasespezifischen Hash-Wert, Prüfsummen, digitale Signaturen, etc.)? | |
| SAHD-3.2 | Verfügt das Produkt über einen Mechanismus der sicherstellt, dass Software-Updates vom Hersteller autorisiert sind (z. B. einen Release-spezifischen Hash-Wert, Prüfsummen, digitale Signaturen, etc.)? | |
| SAHD-4 | Kann ein Nutzer die Software-Integrität verifizieren? (Damit gemeint ist, ob der Betreiber/Bediener feststellen kann, ob das System (unerlaubt) manipuliert worden ist). Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | Beschreiben Sie hier bitte den typischen Output bei der Verifikation der Software-Integrität. |
| SAHD-5 | Ist die Steuerung der (Zugriffs-)Kontrolle so konfigurierbar, dass sie einen Zugang auf Ebene der einzelnen Dateien, des Patienten oder mittels anderer Zugriffskontrollmechanismen ermöglicht? | Beschreiben Sie bitte, wie die Zugriffskontrolle auf der Ebene einzelner Dateien funktioniert (z. B. Nutzerkonto gegenüber Administratorkonto, Fernwartungszugriff gegenüber vor-Ort-Zugriff) und verweisen Sie gegebenenfalls auf das Kapitel AUTH. |
| SAHD-5.1 | Bietet das Produkt rollenbasierte Zugriffskontrollen? | Bitte verweisen Sie hier gegebenenfalls auf das Kapitel AUTH. |
| SAHD-6 | Gibt es System- oder Nutzerkonten, die werksseitig eingeschränkt nutzbar oder deaktiviert sind? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |

| FragenID | Frage | Empfehlung |
|---|---|---|
| SAHD-6.1 | Lassen sich, nach der Erstkonfiguration, System- oder Nutzerkonten durch den Endnutzer konfigurieren? | |
| SAHD-6.2 | Können einige System- oder Nutzerkonten, wie die von Servicetechnikern, so eingeschränkt werden, dass sie die geringsten Zugriffsrechte zugewiesen bekommen? | |
| SAHD-7 | Werden alle geteilten Ressourcen (z. B. gemeinsame Dateien), die nicht für die Zweckbestimmung notwendig sind, auf dem Produkt deaktiviert? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | Geben Sie bitte an, welche geteilten Ressourcen werksseitig ausgeschaltet sind oder welche, nach der Erstkonfiguration, durch den Endnutzer konfigurierbar sind. |
| SAHD-8 | Wurden alle Kommunikationskanäle (Ports) und -protokolle, die nicht für die Zweckbestimmung des Produkts notwendig sind, geschlossen oder deaktiviert? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | Geben Sie bitte an, welche Ports oder Protokolle werksseitig ausgeschaltet sind oder welche, nach der Erstkonfiguration, durch den Endnutzer konfigurierbar sind. |
| SAHD-9 | Wurden alle Dienste (z. B. Telnet, FTP, IIS etc.) die nicht für die Zweckbestimmung des Produkts notwendig sind, entfernt oder deaktiviert? | Geben Sie bitte an, ob die nicht genutzten Dienste vor oder während der Erstinstallation herstellerseitig entfernt oder deaktiviert wurden oder ob der Endnutzer dies nachträglich konfigurieren darf oder muss. |
| SAHD-10 | Wurden alle Anwendungen Standardanwendungen (COTS) sowie vom Betriebssystem mitgelieferte (z. B. Microsoft Explorer), die nicht für die Zweckbestimmung des Produkts benötigt werden, gelöscht oder deaktiviert? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | Geben Sie bitte an, ob die nicht genutzten Anwendungen vor oder während der Erstinstallation herstellerseitig entfernt oder deaktiviert wurden oder ob der Endnutzer dies nachträglich konfigurieren darf oder muss. |
| SAHD-11 | Kann das Produkt von einem unkontrollierten Medium oder einem Wechseldatenträger gestartet werden (damit ist jede andere Boot-Quelle gemeint, die nicht zum internen Laufwerk oder zur Speicherkomponente gehören)? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | Beschreiben Sie bitte welche externen Datenträger vom Produkt akzeptiert werden. |
| SAHD-12 | Kann Software oder Hardware, die nicht vom Hersteller autorisiert worden ist, ohne Zuhilfenahme physischer Werkzeuge auf dem Produkt installiert werden? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | Beschreiben Sie bitte alle Einschränkungen, in Bezug auf die Installation von Soft- und Hardware auf dem Produkt, die sich für den Betreiber ergeben. |

| FragenID | Frage | Empfehlung |
|---|---|---|
| SAHD-13 | Beinhaltet die Produktdokumentation Anleitungen für Netzwerk-Sicherheits-Scans während des Betriebes für den Betreiber? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | |
| SAHD-14 | Kann das Produkt über die standardmäßig vorgegebenen Einstellungen hinaus gehärtet werden? | |
| SAHD-14.1 | Sind Anleitungen herstellerseitig verfügbar, die eine erhöhte Härtung ermöglichen? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | |
| SAHD-15 | Kann das System einen Zugriff auf das BIOS oder andere Bootloader während des Startens verhindern? | Hier wird empfohlen „n/a“ anzugeben, wenn das Medizinprodukt kein BIOS oder andere Bootloader besitzt. |
| SAHD-16 | Wurden zusätzliche Methoden, die nicht unter SAHD aufgeführt sind, zur Härtung des Produkts implementiert? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | |

## 3.19 Sicherheitsleitfäden für Betreiber (SGUD)

Verfügbarkeit von Sicherheitsanweisungen oder -leitfäden für den Betreiber und Administrator des Produkts sowie den Verkauf und Kundendienst des Herstellers.

| FragenID | Frage | Empfehlung |
|---|---|---|
| SGUD-1 | Wurden sicherheitsrelevante Eigenschaften des Produkts für den Nutzer dokumentiert? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | Bitte beantworten Sie die Frage mit „yes“ wenn der Hersteller ausgewählte Sicherheitsdokumente oder eine Sicherheitsdokumentation im Nutzerhandbuch, in der Betriebsanleitung oder in anderen Dokumenten, wie security White Paper, die dem Betreiber zur Verfügung stehen, inkludiert hat. Bitte referenzieren Sie auf die entsprechende Dokumentation. |
| SGUD-2 | Bietet das Produkt die Möglichkeit Daten permanent vom Produkt selbst oder angeschlossenen Medien zu löschen und bietet es hierfür eine Anleitung? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | Bitte beantworten Sie die Frage mit „yes“ wenn der Hersteller solche Anleitungen dem Betreiber zur Verfügung stellt. Nennen Sie bitte die entsprechenden Spezifikationen (z. B. HMG InfoSec Standard 5, BSI, NIST 800-88). |
| SGUD-3 | Werden alle Konten, die Zugriff auf das System gewähren, dokumentiert? | |

| FragenID | Frage | Empfehlung |
|---|---|---|
| SGUD-3.1 | Kann der Betreiber/Bediener die Passworteinstellung für alle Konten verwalten? | Bitte geben Sie an, ob jeder Fernwartungszugang oder jede Einrichtung, die Zugriff hat, bekannt ist und ob die entsprechenden Zugriffskontrollen dokumentiert sind (z. B. Remote Desktop Protokoll (RDP) und Protokolle für den Fernwartungszugang, wie Intelligent Plattform Management Interface (IPMI)) Führen Sie bitte auf, ob der Betreiber die Passwörter selbständig für alle Konten aktivieren, deaktivieren und kontrollieren kann. |
| SGUD-4 | Enthält die Produktdokumentation Sicherheitsanweisungen und Empfehlungen zu alternativen Schutzmaßnahmen? | Geben Sie hier bitte die Empfehlungen zu alternativen Schutzmaßnahmen, z. B. Netzwerksegmentierung, Internet-Firewall, etc. an. |

## 3.20 Integrität und Vertraulichkeit von gespeicherten Patienteninformationen (STCF)

Beschreibt die Fähigkeit des Produkts, dass bei einem nicht autorisierten Zugriff die Integrität und Vertraulichkeit der personenbezogenen Daten, welche auf dem Produkt oder einem Transportmedium gespeichert sind, geschützt bleibt.

| FragenID | Frage | Empfehlung |
|---|---|---|
| STCF-1 | Kann das Produkt abgelegte Daten verschlüsseln (Data at rest)? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | Geben Sie bitte die verfügbaren Verschlüsselungsalgorithmen oder eine entsprechende Referenz an. Die Frage bezieht sich ausschließlich auf lokal gespeicherte Daten. Unter 3.21 TXCF-2 werden Informationen zur Datenverschlüsselung vor der Übermittlung über das Netzwerk oder vor dem Export abgefragt. |
| STCF-1.1 | Werden alle Daten verschlüsselt oder anderweitig geschützt? Wenn ja, beschreiben Sie bitte die Schutzmechanismen im Freitextfeld. | Hier ist zu empfehlen, dass falls der Schutz nur einen Teil der gesamten Daten umfasst, auch beantwortet wird, ob Daten z. B. zur Einstellung und Konfiguration oder nur gewisse Daten, wie patientenbezogene Daten oder Patientenakten, geschützt werden. |
| STCF-1.2 | Ist die Verschlüsselung der Daten standardmäßig vorkonfiguriert? | |
| STCF-1.3 | Sind Anleitungen verfügbar, wie der Kunde die Verschlüsselung konfigurieren kann? | |

| FragenID | Frage | Empfehlung |
|---|---|---|
| STCF-2 | Können die Schlüssel für die Verschlüsselung geändert oder konfiguriert werden? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |
| STCF-3 | Werden die Daten in einer Datenbank auf dem Produkt gespeichert? Wenn ja, beschrieben Sie dies bitte im Freitextfeld. | |
| STCF-6 | Werden die Daten in einer Datenbank außerhalb des Produkts gespeichert? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | |

## 3.21 Sichere Datenübermittlung (TXCF)

Beschreibt die Fähigkeit des Produkts während der Datenübertragung die Vertraulichkeit der Informationen sicherzustellen.

| FragenID | Frage | Empfehlung |
|---|---|---|
| TXCF-1 | Werden personenbezogene Daten nur über eine dedizierte Leitung von einem Punkt zum anderen übertragen? | Eine dedizierte Punkt-zu-Punkt-Verbindung ist der Öffentlichkeit nicht zugänglich (z. B. in kontrollierten Räumen, wie Untersuchungszimmern, Verteilerschränken und Haustechnikräumen). |
| TXCF-2 | Werden personenbezogene Daten verschlüsselt, bevor sie durch ein Netzwerk übertragen oder auf einen Wechseldatenträger kopiert werden? Wenn ja, geben Sie bitte im Freitextfeld an, welcher Verschlüsselungsmechanismus angewendet wird. | Bitte referenzieren Sie bei den Verschlüsselungsmechanismen auf die entsprechenden Standards. |
| TXCF-2.1 | Wenn standardmäßig keine Verschlüsselung erfolgt, kann der Kunde die Verschlüsselungsoptionen konfigurieren? | |
| TXCF-3 | Sind die personenbezogenen Datenübertragungen beschränkt auf eine vorgegebene Liste von Zieladressen im Netzwerk? | Eine vorgegebene Liste ist ein Mechanismus, der die Anzahl an Verbindungen und die Art der Verbindungen pro Produkt einschränkt. |
| TXCF-4 | Werden sämtliche Verbindungen auf authentifizierte Systeme beschränkt? Wenn ja, beschreiben Sie dies bitte im Freitextfeld. | Bitte geben Sie an, wie die Einschränkungen bewerkstelligt werden, ob weitere Zugriffskontrollen unterstützt werden und welche Methoden unterstützt werden. |

| FragenID | Frage | Empfehlung |
|---|---|---|
| TXCF-5 | Unterstützt das Produkt sichere Übertragungsmethoden (DICOM, HL7, IEEE 11073) oder sind diese implementiert? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | |

## 3.22 Datenintegrität bei Übermittlung (TXIG)

Hier wird die Fähigkeit des Produkts beschrieben die Integrität der übertragenen Daten zu wahren.

| FragenID | Frage | Empfehlung |
|---|---|---|
| TXIG-1 | Unterstützt das Produkt Maßnahmen (z. B. digitale Signaturen), die dafür geeignet sind, sicherzustellen, dass die Daten während der Übertragung nicht verändert werden? Wenn ja, beschreiben Sie bitte im Freitextfeld, wie dies erreicht wird. | |
| TXIG-2 | Besteht das Produkt aus Teilkomponenten, die über außenliegende Kabel miteinander verbunden sind? Wenn ja, stellen Sie bitte im Freitextfeld ein entsprechendes Diagramm zur Verfügung. | Bitte verweisen Sie hier auf das Deployment-Diagramm, vgl. DOC-10. |

## 3.23 Fernwartung (RMOT)

Die Fernwartung bezeichnet jede Art von Wartungsarbeiten am Produkt, die von einem Techniker über ein Netzwerk oder andere Remoteverbindung, durchgeführt wird.

| FragenID | Frage | Empfehlung |
|---|---|---|
| RMOT-1 | Gibt es eine Serviceschnittstelle zur Fernwartung, um das Produkt analysieren oder reparieren zu können? Wenn ja, beschreiben Sie bitte im Freitextfeld, wie dies erreicht wird. | |
| RMOT-1.1 | Erlaubt das Produkt, dass der Betreiber/Bediener eine Fernwartungssitzung initiiert, um das Produkt zu analysieren oder zu reparieren? | Hier sollte zwischen Betreiber und Bediener unterschieden werden. |
| RMOT-1.2 | Existiert eine Anzeige oder Meldung für einen freigeschalteten und aktiven Fernwartungszugriff? | |
| RMOT-1.3 | Können personenbezogene Daten während der Fernwartungssitzung gesehen werden oder kann auf sie zugegriffen werden? | |

| FragenID | Frage | Empfehlung |
|---|---|---|
| RMOT-2 | Erlaubt oder nutzt das Produkt Fernwartungsverbindungen, um Daten für die vorausschauende Wartung zu generieren? Wenn ja, beschreiben Sie bitte im Freitextfeld, wie dies erreicht wird. | |
| RMOT-3 | Gibt es weitere Möglichkeiten für eine Fernzugriff-Funktionalität (z. B. Software-Updates, Remote Training)? Wenn ja, beschreiben Sie diese bitte im Freitextfeld. | |

## 3.24 Weitere zu berücksichtigende Cyber-Sicherheitseigenschaften (OTHR)

Hier sollte der Hersteller weitere bestehende Sicherheitseigenschaften des Produkts angeben, die sich nicht den bestehenden Kategorien des Dokuments zuweisen lassen. Darüber hinaus sollten die Sicherheitsmaßnahmen, die der Betreiber/Bediener außerhalb des Produkts realisieren soll, aufgeführt werden, wenn sie nicht den anderen Kategorien des Dokuments zuweisen lassen.

# 4 Links

Zusammenfassende Übersicht über die im Text referenzierten Quellen:

1. Allianz für Cyber-Sicherheit

   https://www.allianz-fuer-cybersicherheit.de

2. Link zum MDS2-Formular der NEMA

   https://www.nema.org/Standards/Pages/Manufacturer-Disclosure-Statement-for-Medical-Device-Security.aspx

Dieses Dokument wurde durch den „Expertenkreis CyberMed der ACS“ erstellt, dem neben Vertretern des Bundesamtes für Sicherheit in der Informationstechnik auch Mitarbeiter anderer Organisationen angehören. Weitere Informationen finden Sie unter: https://www.allianz-fuer-cybersicherheit.de/

Kommentare und Hinweise zu diesem Dokument können von Lesern an info@cyber-allianz.de gesendet werden.