Leitfaden IT-Sicherheit

A) Metainformationen

1. Ziele des Leitfadens

Dieser Leitfaden hat das Ziel, Medizinprodukte-Herstellern und Benannten Stellen eine Handlungsanleitung und eine konkrete Checkliste an die Hand zu geben, um

- zu verstehen, was die Erwartungen der Benannten Stellen sind,
- die schrittweise Umsetzung der IT-Sicherheit der Produkte zu befördern,
- das Fehlen einer harmonisierten Norm (zwischenzeitlich) bestmöglich zu kompensieren.

Im Gegensatz zu vielen anderen Leitfäden zur IT-Sicherheit bezieht sich dieser nur auf Medizinprodukte und hat die Patientensicherheit ("Safety") im Fokus.

Der Leitfaden hat **nicht** die Zielsetzung, als Lehrbuch oder Leitfaden für das Erreichen der IT-Sicherheit zu dienen. Vielmehr möchte er ein Leitfaden für deren Überprüfung sein.

Der Anhang nennt die Erwägungsgründe, die zur Entwicklung dieses Leitfadens führten.

2. Anwendungsbereich

Dieser Leitfaden wendet sich an Hersteller von Medizinprodukten, insbesondere von vernetzbaren Medizinprodukten, und deren Dienstleister sowie an Personen und Organisation, die die IT-Sicherheit dieser Produkte bewerten müssen.

Er hat die IT-Sicherheit der Produkte im Fokus, nicht die IT-Sicherheit der Organisation.

Der Leitfaden ist auch geeignet, um die technischen Maßnahmen zu bewerten, die der vom Datenschutz gefordert werden. Dennoch liegt der Schwerpunkt auf der Patientensicherheit, nicht der Vertraulichkeit von Daten.

3. Hinweise zur Verwendung

a) Aufbau und Struktur des Leitfadens

Dieser Leitfaden folgt dem Gedanken, dass die IT-Sicherheit auf drei wesentlichen Säulen ruht:

1. Anforderungen an Prozesse
2. Anforderungen an Produkte
3. Dokumentierte Nachweise, dass diese Anforderungen an die Prozesse und Produkte erfüllt sind

Die Struktur dieses Leitfadens folgt diesem Gedanken: Er enthält in Kapitel B) zuerst allgemeine Anforderungen, formuliert im Kapitel C) die Anforderungen an den Prozess (inklusive Dokumentation) und in Kapitel D) die Anforderungen an das Produkt (inklusive Dokumentation). Innerhalb dieser "Hauptkapitel" gliedern sich die Anforderungen entlang der Software-Lebenszyklus-Prozesse:

1. **Anforderungen an die Prozesse**
    1. ***Anforderungen an den Entwicklungsprozess***
        1. Zweckbestimmung und Stakeholder-Anforderungen
        2. System- und Software-Anforderungen
        3. System- und Software-Architektur
        4. Implementierung und Erstellung der Software
        5. Bewertung von Software-Einheiten

6. System- und Software-Tests
7. Produktfreigabe

2. ***Anforderungen an die der Entwicklung nachgelagerten Phase***
    1. Produktion, Distribution, Installation
    2. Marktüberwachung
    3. Incident Response Plan

2. **Anforderungen an das Produkt**
    1. Vorbemerkungen und allgemeine Anforderungen
    2. System-Anforderungen
    3. System- und Software-Architektur
    4. Begleitmaterialien

Die Anforderungen mit Bezug zum Risikomanagement sind in die Anforderungen entlang des Produktlebenszyklus eingewoben.

b) Anwendbare Kapitel und Anforderungen

Die Hersteller sollten den Leitfaden zuerst nutzen, um die Vollständigkeit der Vorgabedokumente (Verfahrens- und Arbeitsanweisungen, Checklisten usw.) zu prüfen. Dazu sollten sie die Kapitel B) bis D) berücksichtigen.

Anschließend sollten sie sowie die Personen, die produktspezifisch die IT-Sicherheit bewerten (u.a. interne und externe Auditoren und Prüfer der technischen Dokumentation), den Leitfaden nutzen, um für das jeweilige Produkt die IT-Sicherheit zu bewerten. In diesem Fall können sie die Kapitel C) und D) dieses Leitfadens als Checkliste nutzen.

Dieser Leitfaden enthält Anforderungen, die nicht bei allen Produkten anwendbar sind. Hersteller begründen die Ausschlüsse, die nicht offensichtlich sind.

c) Priorisierung

Sollten die Hersteller nicht alle Anforderungen dieses Leitfadens von Beginn an erfüllen können, sollten so möglich und sinnvoll die Anforderungen in der Reihenfolge deren Priorität (zuerst Stufe 0, zum Schluss Stufe 3) erfüllen. Diese Stufen beschreibt der Anhang.

Die Akzeptanz des erreichten Sicherheitsniveaus ist zu bewerten.

d) Kommentare

Der Leitfaden enthält zu den meisten Anforderungen "Kommentare". Diese Kommentare umfassen Begründungen, Referenzen, Anmerkungen und v.a. Tipps für Auditoren und Reviewer.

Da der deutsche Begriff "Sicherheit" nicht genau zwischen den bedeutsamen Schutzzielen Gefährdungsfreiheit und Informationssicherheit unterscheidet, wird zur Hervorhebung auch der Begriff Security für Informationssicherheit verwendet. Entsprechend steht der Begriff "Risiko" für die technische Möglichkeit der Reduktion von Gefährdungsfreiheit, währen der Begriff "Bedrohung" für mögliche Angriffe im Bereich Informationssicherheit steht.

Als Ausblick für die weitere Entwicklung des Leitfadens lässt sich ein Trend zur Umsetzung der Normenreihe ISO 2700x feststellen. Dies ist den erkennbaren Versuchen professioneller Angreifer geschuldet, die Malware zukünftig über die IT-Infrastrukur der Hersteller-Organisation, über Kommunikationsmittel, Konfigurationswerkzeuge, Software-Werkzeuge und Bibliotheken in die Medizinprodukte einschleusen werden. Weiter Absicherungsmaßnahmen werden also bereits "früher" im Entwicklungsprozess greifen müssen, womit dann eben Themen der Informationssicherheit im Betrieb in den Vordergrund rücken.

e) Verbindlichkeit

Dieser Leitfaden ist weder eine gesetzliche Anforderung noch eine harmonisierte Norm. Entsprechend unterscheidet er auch nicht zwischen normativen und informativen Elementen.

Vielmehr trägt der Leitfaden Best-Practices zusammen, um den gesetzlich geforderten "State-of-the-Art" bestmöglich zu beschreiben.

4. Autoren und Nutzungsrechte

Diesen Leitfaden haben die folgenden Autoren verfasst:

- Dr. Andreas Purde (TÜV SÜD)
- Olaf Teichert (TÜV SÜD)
- Prof. Dr. Christian Johner (Johner Institut)

Dr. Georg Heidenreich (Siemens Healthcare GmbH) hat als Reviewer wesentlich beigetragen.

5. Dokumentenlenkung, Dokumentenidentifikation

Dieses Dokument wird über das Versionsverwaltungssystem git bzw. die Plattform GitHub verwaltet. Einzig die in diesem Repository genannten Dokumente sind gültig.

Die Versionshistorie einschließlich der jeweiligen Autoren kann der Dokumentenhistorie entnommen werden.

Die freigegebenen Versionen sind über ein Tag im Repository als solche gekennzeichnet. Versionen ohne Tag sind Dokumente im Entwurfsstadium.

B) Allgemeine Anforderungen

1. Prozesse

Die Hersteller sollten alle unten genannten Aspekte entweder in den Verfahrensanweisungen oder in den entsprechenden Plänen abdecken, um zu gewährleisten, dass die IT-Sicherheit systematisch gewährleistet wird. Üblicherweise sind die folgenden Verfahrensanweisungen bzw. Pläne betroffen:

- Entwicklung
- Risikomanagement
- Verifizierung und Validierung (falls nicht Teil der Entwicklung)
- Marktbeobachtung (Post-Market Surveillance) und Vigilanz
- Service, Installation, Außerbetriebnahme
- Kundenkommunikation
- Managementbewertung (ISO 13485 fordert "anwendbare neue oder überarbeitete regulatorische Anforderungen" zu berücksichtigen.)

Nutzt der Hersteller ausgelagerte Prozesse, so gelten die Anforderungen entsprechend. Beispielsweise müsste ein (Software-)Entwicklungsdienstleister verpflichtet werden, die für ihn relevanten Kapitel dieser Leitlinie zu beachten.

2. Kompetenzen

Die Hersteller müssen sicherstellen und nachweisen, dass sie über ausreichend Kompetenzen verfügen, um eine dem Stand der Technik entsprechende Informationssicherheit (auch: IT-Sicherheit) zu gewährleisten. Diese Nachweise gelingen oft am leichtesten durch interne oder externe Schulungen.

Hersteller können dabei auch auf die Kompetenz externer Ressourcen zugreifen.

ID	Anforderung	Stufe	Kommentare
B.2.1	Der Hersteller hat eine Liste aller Rollen erstellt, die mit dem Thema IT-Sicherheit direkt oder indirekt befasst sind B2-01	1	
B.2.2	Der Hersteller hat für jede Rollen die Kompetenzen mit Bezug zur IT-Sicherheit bestimmt B2-02	1	
B.2.3	Der Hersteller hat Aufzeichnungen (z.B. Schulungsunterlagen), die den Schluss erlauben, dass die Personen tatsächlich über diese Kompetenzen verfügen	1	
B.2.4	Die (Software-)Entwicklungspläne legen produktspezifisch die (darüber hinausgehenden oder abweichenden) Kompetenzen fest	2	Forderung seit ISO 13485:2016

[**B2-01**] Beispiele sind: Entwickler, Tester, Regulatory Affairs und Qualitätsmanager, Mitarbeiter in Service und Support, Produktmanager, Medizinprodukteberater

[**B2-02**] Es sollten Kompetenzen (verstehen, können) und nicht primär Themen genannt sein

3. Dokumentation

Die Hersteller sollten den Nachweis führen können, die relevanten Anforderungen dieser Leitlinie beachtet zu haben. Es gibt keine spezifischen Anforderungen an die Dokumentation und "Objective Evidence".

Es besteht in Europa (im Gegensatz zu den USA) auch keine Pflicht, ein spezifisches Dokument zur IT-Sicherheit zu erstellen. Vielmehr können Hersteller diese Aspekte in bereits bestehenden Dokumenten wie den Vorgabedokumenten des QM-Systems und der technischen Dokumentation (z.B. Software-Akte, Risikomanagementakte) integrieren.

C) Anforderungen an die Prozesse

1. Anforderungen an die Produktentwicklung

a) Zweckbestimmung und Stakeholder-Anforderungen

ID	Anforderung	Stufe	Kommentare
C.1.a.1	Der Hersteller hat alle Nachbarsysteme (Medizinprodukte, IT-Systeme) bestimmt, die mit dem Produkt verbunden werden dürfen.	0	
C.1.a.2	Der Hersteller hat eine Liste an Rollen erstellt (Personen, Nachbarssysteme), die mit dem Produkt interagieren dürfen	0	Liste der Rollen zeigen lassen
C.1.a.3	Der Hersteller hat alle Märkte und alle dort relevanten regulatorischen Anforderungen festgelegt.	0	sich die Liste der regulatorischen

ID	Anforderung	Stufe	Kommentare
			Anforderungen mit Bezug zur IT-Sicherheit zeigen lassen
C.1.a.4	Der Hersteller hat die vorgesehenen primären und sekundären Benutzer mit ihren IT-Kompetenzen festgelegt.[C1-01]	1	
C.1.a.5	Der Hersteller hat die vorgesehene Nutzungsumgebung festgelegt.[C1-02]	1	
C.1.a.6	Der Hersteller hat die Risiken (Gefährdung) analysiert, die folgen, wenn die nicht die spezifizierten Benutzer in der spezifizierten Benutzungsumgebung mit dem System arbeiten [C1-03]	1	
C.1.a.7	Der Hersteller hat im Risikomanagement beschrieben, welche Bedrohungen für die IT-Sicherheit bestehen und was die Folgen für Patienten, Anwender und Dritte wären	1	
C.1.a.8	Der Hersteller hat die Risikoakzeptanzkriterien nachvollziehbar aus dem Nutzen des Produkts und dem State-of-the-Art abgeleitet	1	
C.1.a.9	Der Hersteller hat ein System entwickelt, mit dem er IT-sicherheitsbezogene Risiken bewerten kann[C1-04]	2	

[**C1-01**] Primäre Benutzer sind diejenigen, die das Produkt im Sinne der medizinischen Zweckbestimmung anwenden. Sekundäre Benutzer sind alle anderen Personen, die das Produkt im bestimmungsgemäßen Gebrauch nutzen z.B. bei der Installation, Konfiguration, Update/Upgrade

[**C1-02**] Beispiele finden sich in der Sektion zum Labeling

[**C1-03**] Beispiele: Der Betreiber hat keinen Virenschutz installiert. Benutzer teilen sich ein Passwort.

[**C1-04**] Beispiele für solche Klassifikationssystem sind DREAD und CVSS. Allerdings haben diese keinen Bezug zur Gefährdungsfreiheit ("Safety").

b) System- und Software-Anforderungen

i) Authentifizierung und Autorisierung

ID	Anforderung	Stufe	Kommentare
C.1.b.i.1	Der Hersteller hat alle Datenschnittstellen identifiziert	0	Liste der Datenschnittstellen zeigen lassen (drahtgebunden, WLAN, USB usw.)
C.1.b.i.2	Der Hersteller hat für jede Datenschnittstelle die verwendeten Protokolle und Standards spezifiziert[C2a-01]	1	

ID	Anforderung	Stufe	Kommentare
C.1.b.i.3	Der Hersteller hat für jede Datenschnittstellen die Funktionen spezifiziert, die über die jeweilige Schnittstelle angeboten werden	0	Liste der Funktionen zeigen lassen
C.1.b.i.4	Der Hersteller hat die Sicherheitsrelevanz (im Sinne von Gefährdung) aller Funktionen analysiert.	0	
C.1.b.i.5	Der Hersteller hat die Auswirkungen sicherheitsrelevanter (im Sinne von Gefährdung) Funktionen im Risikomanagement dokumentiert	0	
C.1.b.i.6	Der Hersteller hat jedes Benutzungsszenario[C2a-02] untersucht, welche Risiken sich aus einer nicht spezifizierten Anzeige von Informationen (z.B. keine, falsche, zu späte Anzeige) ergeben.	1	In Risikomanagement- oder Usability-Akte zeigen lassen
C.1.b.i.7	Der Hersteller hat für jede Rolle und jedes Nachbarsystem die Funktionen des Produkts bestimmt, auf die sie über die jeweilige Schnittstelle zugreifen darf	1	"Mapping" von Rollen auf Funktionen zeigen lassen z.B. in Form einer Tabelle
C.1.b.i.8	Der Hersteller hat die Wahl des Authentifizierungsverfahren (Benutzername / Passwort, Biometrisches Verfahren, Token z.B. Karte) für alle Rollen und alle Nachbarsysteme begründet	1	Die Begründung sollte risikobasiert sein
C.1.b.i.9	Der Hersteller hat ggf. weitere Mechanismen gefordert, um die Wahrscheinlichkeit unautorisierter Zugriffe zu minimieren [C2a-04]	2	
C.1.b.i.10	Der Hersteller hat im Risikomanagement die Auswirkungen für die Patientensicherheit analysiert, wenn eine Person nicht auf Patienten- oder Gerätedaten zugreifen kann (z.B. keine Berechtigung, Passwort vergessen), und entsprechende Maßnahmen definiert [C2a-05]	1	Hier geht es um die Abwägung der Schutzziele "Vertraulichkeit" versus "Safety"

[**C2a-01**] Die Standards lassen sich aufteilen u.a. auf die strukturelle Interoperabilitätsebene (z.B. TCP/IP, HTTPs, SFTP, CAN, RS232, USB), auf die syntaktische (z.B. csv, JSON, XML, HL7), auf die semantische (z.B. Nomenklaturen und Kodierungssysteme wie LOINC (u.a. Laborwerte), ATC (Medikamente), ICD (Diagnosen), UCUM (Einheiten) und auf die organisatorische Ebene (IHE))

[**C2a-02**] Alternativ zu den Benutzungsszenarien kann auch jede zusammengehörende Gruppe an UI-Elementen (z.B. Bildschirmseiten, Panels) untersucht werden, die im Rahmen dieses Benutzungsszenarios angeboten werden. Diese Aktivität ist Teil der allgemeinen Analyse der Risiken, die durch die Umsetzung von Produktmaßnahmen der Informationssicherheit entstehen können.

[**C2a-04**] z.B. Einschränkung erlaubter IP- oder MAC-Adressen, physischer Zugriffsschutz

[**C2a-05**] Im Gegensatz zu den oben genannten Punkten, geht es hier um Risiken, die sich ergeben, obwohl sich das System spezifikationsgemäß verhält. Diese Aktivität ist Teil der allgemeinen Analyse der Risiken, die durch die Umsetzung von Produktmaßnahmen der Informationssicherheit entstehen können. Es geht also nicht um

Risiken durch mangelnde IT-Sicherheit, sondern um Risiken (im Sinne von Gefährdungsfreiheit, Verfügbarkeit und Performanz), die aus Maßnahmen zur Erhöhung der IT-Sicherheit folgen.

ii) Daten, Kommunikation

ID	Anforderung	Stufe	Kommentare
C.1.b.ii.1	Der Hersteller hat eine Liste aller vom System verwalteten Daten [C2b-01] erstellt	1	
C.1.b.ii.2	Der Hersteller hat die Schutzwürdigkeit dieser Daten mit Bezug zur Vertraulichkeit und deren Auswirkung auf die Patientensicherheit bewertet.	1	
C.1.b.ii.3	Der Hersteller hat im Risikomanagement die Auswirkungen bewertet, wenn der Schutz besonders schützenswerter Daten nicht mehr gegeben ist	1	
C.1.b.ii.4	Der Hersteller hat im Risikomanagement die Folgen einer Überlastung des Systems durch zu viele Anfragen (z.B. DoS) oder Anfragen mit zu großen Daten-Volumina untersucht und falls notwendig Maßnahmen definiert	2	
C.1.b.ii.5	Der Hersteller hat im Risikomanagement die Folgen analysiert, wenn das Netzwerk nicht mehr oder nicht mehr in der erwarteten Güte zur Verfügung steht.	2	
C.1.b.ii.6	Der Hersteller hat im Risikomanagement die Folgen eines Datenverlusts analysiert und ggf. Maßnahmen wie Backup festgelegt	2	
C.1.b.ii.7	Der Hersteller hat allgemein oder produktspezifisch festgelegt, nach welchen Überprüfungskriterien[C2b-02] externe Daten vor der weiteren Verarbeitung überprüft werden müssen[C2b-03]	2	

[**C2b-01**] Beispiele für solche Daten sind Patientendaten (z.B. demographische Daten, Anamnesen, Diagnosen), Untersuchungsdaten (z.B. Laborwerte, radiologische und pathologische Bilder) und Behandlungsdaten (Verschreibungen, Einstellungen von Medizingeräten), Konfigurationsdaten der Produkte, Daten der Anwender (insbesondere Zugangsdaten), Keys, Software Zertifikate, Programm-Code (inklusive SOUP/OTS).

[**C2b-02**] Beispiele für Überprüfungen: Überprüfung auf falsche Länge, auf Vollständigkeit, auf falschen Zeichensatz, auf nicht erwartete Zeichen, auf mehrfach geschickte Daten, auf veraltete / verspätete Daten, nicht erwartete oder falsche Formate (z.B. kein Escaping von Zeichen mit besonderer Bedeutung wie Trennzeichen, kein wohlgeformtes XML, ungültige JSON-Dateien, falsche Datentypen, XML, das nicht dem spezifizierten Schema entspricht), andere Zeichensätze, im Input enthaltene Schlüsselworte und (ungültige) Befehle, BigEndian statt Little Endian, Werte, die nicht im vorgesehenen Wertebereich enthalten sind (z.B. im Klassifikations- oder Kodierungssystem), falsche Zeitzone, falsches Zahlenformat, unmögliche Daten (z.B. Geburtstag in der Zukunft), widersprüchliche Daten usw.

[**C2b-03**] Falls möglich und sinnvoll empfehlen sich Listen erlaubter Werte (White-Listing)

iii) Patches

ID	Anforderung	Stufe	Kommentare
C.1.b.iii.1	Der Hersteller verfügt über eine dokumentierte Planung, wie Patches aufgespielt und wieder entfernt werden. Dieser Plan beinhaltet die Entwicklung, die Verteilung, die Installation und Überprüfung der Patches.	1	Dieser Plan kann Teil des Incident Response Plans sein (s.u.)
C.1.b.iii.2	Der Hersteller verfügt eine Liste aller SOUP-/OTS-Komponenten	1	Diese Forderung zählt eher zum Kapitel "System- und Software-Architektur"
C.1.b.iii.3	Der Hersteller hat abgeschätzt, wie häufig Patches notwendig sind und wie diese installiert werden müssen	2	

iv) Sonstiges

ID	Anforderung	Stufe	Komme
C.1.b.iv.1	Der Hersteller hat festgelegt, wie das Medizinprodukt die Anwender im Fall einer Kompromittierung der Cybersecurity informiert	2	
C.1.b.iv.2	Der Hersteller hat abgeschätzt, welche Funtionalität das Medizinprodukt auch im Falle einer Komprimittierung der Cybersecurity gewähren muss.		

c) System- und Software-Architektur

ID	Anforderung	Stufe	Kommentare
C.1.c.1	Der Hersteller hat alle SOUP-/ OTS-Komponenten dokumentiert (inkl. Version, Hersteller, Referenz auf Informationen zu Updates, Release-Notes)	1	Liste / Tabelle zeigen lassen. Die FDA fordert die "Cybersecurity Bill of Materials (CBOM)"
C.1.c.2	Der Hersteller hat die spezifischen Risiken, die sich durch die Wahl der Technologien (insbesondere Programmiersprache, SOUP- / OTS-Komponenten) ergeben analysiert.	2	
C.1.c.3	Der Hersteller hat Maßnahmen ergriffen, um sicherzustellen, dass die verwendeten Werkzeuge (z.B. Entwicklungsumgebung, Compiler), sowie die Plattformen und SOUP/OTS-Komponenten frei von Schadcode sind C3-01	2	
C.1.c.4	Der Hersteller haben einer Liste aller Dienste C3-02 erstellt, die das Produkt (z.B. durch sein Betriebssystem) nach "außen" anbietet bzw. nutzt	1	sich diese Liste zeigen lassen

ID	Anforderung	Stufe	Kommentare
C.1.c.4	Der Hersteller hat für jeden Dienst begründet, weshalb dieser (zeitlich unbeschränkt) nach außen sichtbar sein muss	2	sich vom Hersteller erklären lassen, wie/wo gefordert und geprüft ist, dass nicht (zeitlich unbeschränkt) benötigte Dienste auch nicht (zeitlich unbeschränkt) angeboten werden. Ziel ist die "Attack Surface Reduction"
C.1.c.5	Wenn das Produkt eine Schnittstelle anbietet, hat der Hersteller im Risikomanagement beschrieben, wie Angriffe über diese Schnittstelle beherrscht werden	1	eine völlige Beherrschung dieser Risiken ist bei USB-Schnittstellen i.d.R. kaum möglich, aber auch nicht in allen Fällen erforderlich
C.1.c.6	Der Hersteller hat für jeden nach außen sichtbaren Dienst den Prozess identifiziert, der diesen Dienst anbietet / realisiert	2	
C.1.c.7	Der Hersteller hat für jeden Prozess den Nutzer (auf Betriebssystemebene) identifiziert und begründet, wenn dieser nicht mit minimalen Rechten ("worst case" als Root) läuft	2	
C.1.c.8	Der Hersteller hat Risiken durch mangelnde IT-Sicherheit systematisch durch ein Threat-Modeling abgeleitet.	2	Sich das Modell zeigen lassen, dass zumindest die externen Akteure und/oder Bedrohungen und die bedrohten Objekte erkennen lassen muss
C.1.c.9	Der Hersteller hat die Risiken analysiert, die sich durch das (Auto-)Update von Anti-Malware ergeben	1	
C.1.c.10	Der Hersteller hat festgelegt, wie das Produkt eine Kompromittierung der IT-Sicherheit feststellen, diese dokumentieren (log) und darauf wie schnell reagieren muss.		
C.1.c.11	Bezüglich des Auditlogs hat der Hersteller festgelegt, wo dessen Daten liegen, wie diese geschützt, aktualisiert und in welcher Form dieses automatisiert ausgewertet werden kann.		
C.1.c.12	Der Hersteller hat für alle Software-Komponenten C3-03, Dienste bzw. Prozesse, Daten und Software-Komponenten analysiert, welche Risiken entstehen, wenn diese sich aufgrund eines Problems mit der IT-	1	Entspricht einem FMEA-Ansatz

ID	Anforderung	Stufe	Kommentare
	Sicherheit nicht spezifikationsgemäß verhalten		
C.1.c.14	Der Hersteller hat die Software-Anforderungen in der Software-Architektur berücksichtigt	1	Beispielhaft für o.g. Software-Anforderungen sich die Komponente(n) bzw. Technologien in der Architektur zeigen lassen, die die Anforderungen realisieren

[C3-01] Zu den Maßnahmen zählen die Anforderung, dass Entwicklungswerkzeuge, Entwicklungsumgebungen und Bibliotheken (SOUP, OTS-Komponenten) nur von als sicher eingestuften und freigegebenen Quellen geladen werden dürfen, dass die IT-Infrastruktur durch geeignete Maßnahmen wie Virenschutz und Firewalls geschützt sind und dass Bibliotheken vor der Verwendung auf Schadcode untersucht werden (z.B. mit Virenscanner). Diese Forderungen betreffen ggf. auch den Einkaufsprozess.

[C3-02] Beispiel für von Betriebssystemen üblicherweise angebotene Dienste: Webserver, RPC, Cloud-Services, Laufwerke (z.B. USB), Datenbank, DICOM, Dienste über Socket-Verbindungen

[C3-03] zumindest die Top-Level-Komponenten. Diese Komponenten entsprechen auch den Objekten

d) Implementierung und Erstellung der Software

ID	Anforderung	Stufe	Kommentare
C.1.d.1	Der Hersteller hat Coding-Guidelines erstellt, die Anforderungen spezifisch für die IT-Sicherheit stellt. C4-01	1	sich vom Hersteller die Coding-Guidelines und entsprechende Forderungen zeigen lassen
C.1.d.2	Der Hersteller spielt nur Code auf, bei dem Reverse-Engineering und Auslesen des RAMs nicht zu inakzeptablen Risiken führen kann. C4-02	3	
C.1.d.3	Der Hersteller überprüft entweder die Software (Source-Code und Binaries) vor der Auslieferung auf Schadcode und/oder er hat auf allen an der Entwicklung und "Produktion" der Software beteiligten Rechner gegen Malware geschützt.	0	
C.1.d.4	Der Hersteller hat Maßnahmen bestimmt, mit denen Buffer-Overflows gefunden und beseitigt werden können.	2	

[C4-01] Beispiele sind Code-Metriken (z.B. McCabe Maß), Vorgaben zur Dokumentation / Kommentierung des Codes und zu dessen Formatierung, ebenso das Verbot unsicherer Funktionen (in C "gets", "strcopy" und weiterer Funktion), zudem die Pflicht mit Annotationen (z.B. SAL) zu verwenden, um Buffer-Overflows zu vermeiden, die Pflicht, die Übergabeparameter auch für interne Schnittstellen grundsätzlich zu überprüfen usw.

[C4-02] Beispiele wären ein physischer Zugriffsschutz, Obfuscation von Code, Betriebssystem mit Address Space Layout Randomization. Diesen Schutz realisieren üblicherweise die Betriebssysteme

e) Bewertung von Software-Einheiten

ID	Anforderung	Stufe	Kommentare
C.1.e.1	Der Hersteller hat mindestens eine Methode festgelegt, mit der die Einhaltung der Coding-Guidelines überprüft wird.	1	das wird dem Hersteller gelingen, wenn er Werkzeuge zur statischen Code-Analyse einsetzt und/oder Vorgaben für die Code-Reviews macht.
C.1.e.2	Der Hersteller verlangt Code-Reviews für alle Komponenten, die (IT-)sicherheitsrelevanten Funktionen abbilden.	2	
C.1.e.3	Der Hersteller hat konkrete Prüfkriterien[C5-01] in seinen Vorgabedokumenten für die Code-Reviews.	1	
C.1.e.4	Die Code-Reviews werden nach dem Vier-Augen-Prinzip und nur von Personen durchgeführt, die über die notwendige Kompetenz verfügen. Der Hersteller hat diese Kompetenz dokumentiert[C5-02].	2	
C.1.e.5	Der Hersteller hat festgelegt, welche Tests (z.B. Unit-Tests) mit welchen Testfällen[C5-03] und welchem zu erreichenden Abdeckungsgraden notwendig sind.	1	
C.1.e.6	Der Hersteller hat für alle SOUP- bzw. OTS-Komponenten beschrieben, wie diese zu verifizieren sind.	1	

[**C5-01**] Beispiele: Keine Verwendung unsicherer Funktionen, "Input-Sanitization" zumindest bei allen externen Schnittstellen

[**C5-02**] Dokumentiert ist im doppelten Sinne zu verstehen: 1. Der Hersteller hat die notwendigen Kompetenzen festgelegt (siehe ISO 13485:2016 Kapitel 7.3.2 f). 2. Der Hersteller hat dokumentiert, dass die konkreten Personen über die Kompetenzen verfügen.

[**C5-03**] Beim Ableiten der Testfälle kann man sich an der o.g. Liste von Überprüfungskriterien orientieren.

f) System- und Software-Tests

ID	Anforderung	Stufe	Kommentare
C.1.f.1	Der Hersteller sieht im Testplan [C6-01] Portscans an allen relevanten Netzwerkschnittstellen vor und führt diese auch durch.	1	
C.1.f.2	Der Hersteller sieht im Testplan Penetrationstests an allen relevanten Datenschnittstellen und/oder für alle bekannten Schwachstellen der	2	für eine bekannte OTS-Komponente in der NIST Common / National Vulnerability Database eine Schwachstelle recherchieren und vom Hersteller

ID	Anforderung	Stufe	Kommentare
	eingesetzten OTS-Komponenten C6-02 vor und führt diese auch durch.		erklären lassen, wie er sicherstellt, dass diese nicht ausgenutzt werden kann, bzw. weshalb diese nicht relevant ist
C.1.f.3	Der Hersteller sieht im Testplan den Einsatz eines "Vulerability Scanners" vor.		
C.1.f.4	Der Hersteller sieht im Testplan Fuzz-Tests an allen relevanten Datenschnittstellen mit mindestens einem Werkzeug vor und führt diese auch durch C6-03	2	
C.1.f.5	Der Hersteller sieht im Testplan eine Überprüfung der Sicherheit gegen die üblichen Angriffsvektoren vor.C6-04	2	
C.1.f.6	Der Hersteller sieht im Testplan die Überprüfung vor, die Robustheit und Leistungsfähigkeit zu prüfen.		
C.1.f.7	Der Hersteller sieht im Testplan die Überprüfung aller System-/Software-Anforderungen (s.o.) vor.	1	
C.1.f.8	Der Hersteller lässt seine Software zusätzlich zu den o.g. Maßnahmen durch IT-Sicherheitsexperten überprüfen.	3	Zu dieser Überprüfung müssen Fuzz- und Penetrationstests ebenso zählen wie die Analyse der System-/ Software-Architektur und des Quell-Codes, um auf Stufe 3 zu gelangen
C.1.f.9	Der Hersteller bezieht beim Systemtest die Testberichte Dritter (z.B. SOUP-Hersteller) mit ein (soweit verfügbar)		

[**C6-01**] Dieser Plan kann Teil des Entwicklungsplans, eines V&V-Plans oder eines anderen Plans sein.

[**C6-02**] Die Schwachstellen sind z.B. in der NIST National Vulnerability Database (NVD) hinterlegt. Üblicherweise setzt man Scanner wie Nessus oder OpenVAS ein. Die Anforderung lautet nicht, dass beim Penetrationstest notwendigerweise alle bekannten Schwachstellen getestet werden. Die FDA fordert diese Cross Reference zwischen den "CBOMs" und der NVD expliit ein.

[**C6-03**] Im Fokus beim Fuzz-Testing sollte der eigene Code stehen und weniger die OTS-Software. Der Einsatz mehrerer Scanner führt meist zu einem größeren Bereich von Input-Werten.

[**C6-04**] z.B. DoS, SQL-Injection, Cross-Site-Scripting, Directory Transversal, Buffer-Overflow, syntaktisch oder semantisch fehlerhafte Anfragen,

g) Produktfreigabe

ID	Anforderung	Stufe	Kommentare
C.1.g.1	Der Hersteller hat die häufigsten Fehler [C8-01] und daraus resultierenden Gefährdungen in der Risikoanalyse adressiert oder kann zumindest darlegen, weshalb diese Risiken beherrscht sind.	1	ein Beispiel aus einer der verlinkten Listen häufigster Fehler auswählen und den Hersteller um eine Begründung bitten
C.1.g.2	Der Hersteller diskutiert in der Risikoanalyse Risiken durch alle relevanten Angriffs-Vektoren (s.o.) und zeigt, wie diese beherrscht werden.	1	
C.1.g.3	Der Hersteller hat alle Maßnahmen zur Risikobeherrschung auf Wirksamkeit überprüft.	1	z.B. Referenzen auf entsprechende Tests zeigen lassen
C.1.g.4	Der Hersteller hat eine Traceability Matrix erstellt, mit der er dokumentiert, dass alle Risiken mit Bezug zur IT-Sicherheit durch Maßnahmen beherrscht werden.	2	
C.1.g.5	Der Hersteller hat den Risikomanagementbericht und den IT Security Report erstellt.	2	Der IT Security Report kann in Europa durchaus Teil des Risikomanagementberichts sein, in den USA nicht.
C.1.g.6	Der Hersteller hat die notwendigen Pläne für die der Entwicklung nachgelagerten Phase (z.B. Post-Market und Incident Response Plan) erstellt	1	Details weiter unten
C.1.g.7	Der Hersteller hat die Vollständigkeit der Tests durch eine Traceability Matrix geprüft, die die Tests mit den Anforderungen verknüpft.	2	

[**C8-01**] z.B. gemäß OWSAP top 10 oder CWE/SANS top 25

2. Anforderungen an die der Entwicklung nachgelagerten Phasen

a) Produktion, Distribution, Installation

ID	Anforderung	Stufe	Kommentare
C.2.a.1	Der Hersteller hat beschrieben, wie sichergestellt ist, dass nur genau die vorgesehenen Artefakte (Dateien) in genau der vorgesehenen Version im Produkt oder als Produkt ausgeliefert werden	1	hier geht es ums Konfigurationsmanagement. Auch bei Downloads oder AppStores relevant

ID	Anforderung	Stufe	Kommentare
C.2.a.2	Der Hersteller hat beschrieben, wie die für die Installation verantwortlichen Personen wissen, welches die aktuellste Version ist und wie Verwechslungen bei der Installation ausgeschlossen werden können	2	Dies ist nur bei stand-alone Software relevant. Hier wäre eine Verfahrens- oder Arbeitsanweisung zu erwarten
C.2.a.3	Der Hersteller hat beschrieben, wie bei der Installation sichergestellt wird, dass die Anforderungen, die in den Begleitmaterialien spezifiziert sind (s.o.) tatsächlich erfüllt sind	1	Hier wäre eine Verfahrens- oder Arbeitsanweisung zu erwarten
C.2.a.4	Der Hersteller hat Verfahren etabliert, die gewährleisten, dass er mit den Betreibern und Anwendern seiner Produkte zeitnah kommunizieren kann	1	Bei unkritischen Produkten ist die Stufe 2 vertretbar

b) Marktüberwachung

ID	Anforderung	Stufe	Kommentare
C.2.b.1	Der Hersteller hat einen Post-Market Surveillance Plan erstellt.	0	
C.2.b.2	Der Hersteller hat beschrieben, welche Informationen aus der nachgelagerten Phase gesammelt werden D2-01	1	
C.2.b.3	Der Hersteller hat beschrieben, wie und über welche Kanäle Informationen aus der nachgelagerten Phase gesammelt werden	1	
C.2.b.4	Der Hersteller hat beschrieben, wie Informationen aus der nachgelagerten Phase ausgewertet bzw. bewertet werden D2-02	2	erklären lassen, wie der Hersteller eine Trendumkehr erkennt und definiert und welche Schwellwerte er dazu festgelegt hat D2-03
C.2.b.5	Der Hersteller hat beschrieben, welche Maßnahmen daraus resultieren D2-04	2	sich die Verbindung zu den Korrektur- und Vorbeugemaßnahmen in den Prozessbeschreibungen zeigen lassen
C.2.b.6	Der Hersteller hat für jede OTS-Komponente mindestens eine Quelle und die Frequenz deren Überwachung festgelegt, über die er über IT-Sicherheitsbezogene Probleme informiert wird D2-05 und beschrieben, welche Rolle mit welchen Werkzeugen diese Auswertung vornimmt	2	Zu diesen Quellen sollten die Webseiten des OTS-Herstellers sowie die NIST Datenbank mit den Vulnerabilities zählen.

ID	Anforderung	Stufe	Kommentare
C.2.b.7	Der Hersteller hat beschrieben, wie er überwacht, dass verwendete Technologien und Verfahren (z.B. Kryptologie) noch sicher sind	2	

[**D2-01**] Beispiele: Audit-Logs, Vulnerability Datenbanken, Kundenbeschwerden, Anrufe bei Hotline, Beobachtungen (z.B. Verhalten der Anwender), Behörden-Datenbanken (FDA MAUDE, BfArM, SwissMedic etc.), Social Media, Google-Suche, Gesetze, Normen usw.. Alles auch zu ähnlichen Produkten oder Technologien

[**D2-03**] Die MDR fordert dies im Anhang zur Post-Market Surveillance. Die Hersteller müssen festlegen, wann (z.B. Incident/Near Incident) die Maßnahme (s.u.) zu ergreifen ist.

[**D2-04**] Maßnahmen können beinhalten: Rückrufe, Behördenmeldungen, CAPA, Produktverbesserung, Prozessverbesserung, Training (Anwender, intern), Information der Kunden, Änderung der Begleitmaterialien, Einschränkung der Zweckbestimmung. Die Festlegung muss somit die Festlegung einschließen, wer (z.B. Anwender, Benannte Stelle, Behörde), wie (z.B. Field Safety Note) zu informieren ist.

[**D2-05**] Die Frequenz müsste mindestens jährlich, bei kritischen Komponenten häufiger als monatlich erfolgen. Die UL 2900-2-1 spricht von Update-Zyklen von zwei Wochen.

c) Incident Response Plan

(inkl. Rückrufe, Patches, Kundenkommunikation)

ID	Anforderung	Stufe	Kommentare
C.2.c.1	Der Hersteller hat einen Incident Reponse Plan erstellt [D3-01]	2	
C.2.c.2	Der Incident Response Plan regelt, nach welchen Kriterien der Hersteller Informationen aus dem Markt bewertet und wann er den Notfallplan in Kraft setzt ...	2	
C.2.c.3	wer wie innerhalb welcher Fristen die Patches entwickelt und freigibt,	2	
C.2.c.4	wie der Kunde die Patches bezieht,	2	
C.2.c.5	wie der Hersteller sicherstellt, dass die Patches auch installiert werden,	2	
C.2.c.6	wer die Kunden in welcher Form und Frist informiert,	2	
C.2.c.7	in welchen Fällen eine Stilllegung oder ein sonstiger Rückruf des Produkts wie angeordnet wird.	2	

[**D3-01**] Der Incident Response Plan kann Teil anderer Pläne oder Dokumente sein z.B. des Post-Market Surveillance Plans oder der Vorgaben zur Vigilanz.

D) Anforderungen an das Produkt

1. Vorbemerkungen und allgemeine Anforderungen

Dieser Abschnitt beschreibt technische Funktionen des Produkts, die die Informationssicherheit unterstützen. Sie sind über die Anforderungsspezifikation (System-/Software-Anforderungen) einzubringen und als Anforderungen umzusetzen.

Die nachfolgenden technischen Produktmaßnahmen für Informationssicherheit (‚Security-Controls') müssen grundsätzlich für die Sicherstellung der Zweckbestimmung unter Berücksichtigung der intendierten Betriebsumgebung angemessen sein: Zur Erhaltung der grundlegenden Anforderungen an Gefährdungsfreiheit und Funktion darf der Hersteller im begründeten, dokumentierten Einzelfall auf die Implementierung einzelner Produktmaßnahmen verzichten. Der Hersteller kann also zu jeder einzelnen der nachfolgenden Anforderungen anstelle einer Implementierung auch in der Dokumentation (z.B. Lastenheft) einen Hinweis einbringen, warum die jeweilige Anforderung im Hinblick auf die Zweckbestimmung und unter Berücksichtigung der Einsatzumgebung nicht implementiert wurde und welches Restrisiko besteht.

Die Hersteller müssen jede der im Folgenden genannten Maßnahme daraufhin überprüfen, ob sie neue Risiken einführt, die selbst wieder beherrscht werden müssen.

2. System-/Software-Anforderungen

a) Authentifizierung

ID	Anforderung	Stufe	Kommentare
D.2.a.1	Das Produkt erlaubt den Benutzern nur dann seine Nutzung, wenn sie sich am Produkt authentifiziert haben	0	Zugehörige Testfälle zeigen lassen
D.2.a.2	Das Produkt erlaubt an jeder Datenschnittstelle den daran angeschlossenen Nachbarsystemen (z.B. andere Medizinprodukte, IT-Systeme), nur dann mit ihm Daten auszutauschen, wenn diese vom Produkt authentifiziert wurden	0	dto. Die Forderung, dass die Daten nur verschlüsselt übertragen werden dürfen, findet sich weiter unten.
D.2.a.3	Das Produkt erlaubt eine Authentifizierung mit Passwort nur, wenn dieses Passwort eine definierte eine Mindestlänge hat von denen mindestens eines ein nicht alphanumerisches Zeichen ist und das mindestens einen Groß- und einen Kleinbuchstaben enthält C2a-02	1	Die Wahl des Mechanismus zur Authentifizierung hat der Hersteller begründet siehe oben.
D.2.a.4	Das Produkt hat kein Default-Passwort oder verlangt, dass ein solches bei der ersten Nutzung geändert wird	0	
D.2.a.5	Das Produkt sperrt Benutzer und Nachbarsysteme nach n Versuchen für m Minuten aus, wobei der Hersteller n und m Werte oder Untergrenzen festlegt. Der Hersteller hat die "Safety-bezogenen" Risiken als Folge des Aussperrens analysiert und ggf. risikominimierende Maßnahmen implementiert C2a-03.	1	
D.2.a.6	Das Produkt zeigt im Falle eines nicht erfolgreichen Logins nur Informationen an, die es dem Anwender nicht erlauben die genaue Ursache der Sperrung zu erkennen, wie z.B. falscher Benutzername oder falsches Passwort.	2	

ID	Anforderung	Stufe	Kommentare
D.2.a.7	Das Produkt beendet Bediensitzungen für Benutzer und Nachbarsysteme nach n Minuten Inaktivität, wobei der Hersteller für n den Wert oder dessen Obergrenze festlegt.	2	
D.2.a.8	Das Produkt weist jedem Benutzer und jedem Nachbarsystem bei der Authentifizierung eine Rolle zu	1	Erklären lassen, in welcher/welchen Software-Komponente(n) Komponenten diese Funktionalität implementiert und wie dies geprüft ist. Die FDA fordert sogar ein hierarchisches Rollenkonzept.
D.2.a.9	Das Produkt erlaubt jeder Rolle den Zugriff auf nur die Funktionen, für die die sie berechtigt ist. Dies gilt insbesondere auch für das Update/Upgrade des Produkts	1	dto.
D.2.a.10	Das Produkt erlaubt berechtigten Benutzern, andere Benutzer und Nachbarsysteme zu sperren C2a-04	1	
D.2.a.11	Das Produkt erlaubt berechtigten Benutzern, die Authentifizierung notwendigen Elemente (Passwörter, kryptografische Schlüssel, Zertifikate) anderer Benutzer und Nachbarsysteme zurückzusetzen	1	
D.2.a.12	Das Produkt erlaubt berechtigten Benutzern, andere Benutzer und Nachbarsysteme zu löschen	1	
D.2.a.13	Das Produkt erlaubt es Benutzern nicht, die eigene Berechtigung zu ändern	2	
D.2.a.14	Das Produkt erlaubt es, Berechtigungen auszuhebeln ("Breaking the glass"), und identifiziert / dokumentiert die Person und die GründeC2a-05	2	
D.2.a.15	In einer Client-Server Architektur werden alle Cyber-Sicherungsmaßnahmen serverseitig berechnet und geprüft	2	
D.2.a.16	In einer Client-Server Architektur werden alle Eingaben des Clients serverseitig geprüft	2	

[**C2a-02**] Idealerweise müssten auch Passwörter ausgeschlossen werden, die über Wörterbuch-Angriffe erraten werden können. Die Mindestlänge hängt davon ab, ob Brute-Force-Angriffe möglich sind, was bei einer

Datenschnittstelle einfacher ist als abei einer Benutzerschnittstelle. Es gibt Systeme, bei denen "nicht-alphanumerische" Zeichen nicht möglich sind. Das sollte bei der Wahl der Mindestlänge betrachtet werden.

[**C2a-03**] Beispielsweise implementiert der Hersteller ein "Breaking the glass", d.h. eine Möglichkeit, das Berechtigungskonzept zu umgehen, um zeitnah auf wichtige Daten zugreifen zu können. Dieses Umgehen muss protokolliert und später gerechtfertigt werden.

[**C2a-04**] Auch dieses Sperren darf nicht zu Safety-Risiken führen. Daher sollte das Sperren nicht während der Untersuchung oder Behandlung möglich sein, sondern beispielsweise nur im Wartungsmodus.

[**C2a-05**] Es gibt Situationen, in denen Safety wichtiger ist als Security insbesondere als Vertraulichkeit. In diesen Notfallsituationen muss ein Anwender auf Daten (insbesondere Patienten- oder Verschreibungsdaten) zugreifen, auch wenn ihm oder ihr die notwendigen Berechtigungen fehlen. Ein Beispiel wäre, dass ein Notfallpatient behandelt werden muss und man vor der Behandlung (z.B. Medikamente, Bluttransfusion) auf die Daten wie Medikamenten-Unverträglichkeiten oder Laborwerte (z.B. Blutgruppe) zugreifen muss. Dieser Zugriff muss einem Behandelnden immer und unabhängig von den Berechtigungen möglich sein. Das "Breaking-the-glass" lässt sich z.B. als Button implementieren.

b) Kommunikation und Speicherung

ID	Anforderung	Stufe	Kommentare
D.2.b.1	Das Produkt erlaubt es Benutzern, alle patientenspezifischen Daten endgültig zu löschen. Das Produkt erlaubt es, die Berechtigungen dafür zu beschränken (z.B. auf Rollen).	2	
D.2.b.2	Das Produkt schützt Daten vor ungewolltem Löschen. C2b-01	2	Hersteller müssen prüfen, ob kein höherwertiges Schutzziel dem entgegensteht, wie die zuvor genannte Anforderung.
D.2.b.3	Das Produkt übermittelt Daten, zumindest sicherheitsbezogene Daten, über seine Datenschnittstellen nur in verschlüsselter Form. Das gilt auch für das Abspeichern auf externen Datenträgern.	1	Nachfragen, welche Verschlüsselung zum Einsatz kommt und wie der initiale Schlüsselaustausch realisiert ist
D.2.b.4	Das Produkt sichert die Integrität der Daten vor ungewollter Veränderung z.B. durch kryptographische Verfahren	2	Das gilt insbesondere für sicherheitsrelevante Daten wie die unter C2b-01 genannten.
D.2.b.5	Das Produkt lehnt per Default alle eingehenden Verbindungen (z.B. USB, TCP, Bluetooth) ab.	2	Forderung der FDA
D.2.b.6	Das Produkt überprüft alle Benutzereingaben und alle eingehenden Daten vor der weiteren Verarbeitung anhand von Hersteller festgelegten Überprüfungskriterien (s.o.) C2b-02	1	Jeweils ein Beispiel für einen Dateninput an der Benutzer- und an der Datenschnittstelle auswählen und sich die Überprüfung im Code zeigen lassen
D.2.b.7	Das Produkt nutzt für die Übertragung von zeitkritischen Daten, die relevant für die	2	

ID	Anforderung	Stufe	Kommentare
	Patientensicherheit sind, keine kabellose Übertragung.		
D.2.b.8	Das Produkt speichert Passwörter nur als "salted hash"	2	z.B. nach Hash-Verfahren fragen und ggf. zeigen lassen
D.2.b.9	Das Produkt speichert personenidentifizierende Merkmale nur verschlüsselt	2	Erklären lassen, was der Hersteller als personenidentifizierende Merkmale definiert und welchen Verschlüsselungs-mechanismus er nutzt
D.2.b.10	Das Produkt schützt kritische Daten vor ungewollter Veränderung und vor Verlust	2	
D.2.b.11	Das Programm überprüft bei jedem Neustart, ob die Mechanismen in Takt sind, mit denen die Daten vor Verlust und Veränderung geschützt werden.		
D.2.b.12	Das Produkt erlaubt es Nutzern, Datenschnittstellen zu deaktivieren (z.B. USB, Fernzugriff)	2	
D.2.b.13	Das Produkt prüft den Programm-Code bei jedem Neustart auf Integrität	2	
D.2.b.14	Das Produkt stellt im Fall einer Kompromittierung einen Notfall-Modus für Funktionen bereit, die relevant für die Sicherheit der Patienten sind.	2	

[**C2b-01**] Der Schutz kann auch in einer Undo-Funktion bestehen. Ggf. ist der Zeitraum für ein Undo zu beschränken. Es ist zu beachten, dass die Anforderungen des Datenschutzes nach einem (endgültigen) Löschen der Daten erfüllt werden.

[**C2b-02**] Diese Überprüfung sollte auf allen Interoperabilitätsebenen stattfinden. Beispielsweise wären auch die Protokolle, Formate zu überprüfen wie die Wohlgeformtheit von XML-Dateien.

c) Patches

ID	Anforderung	Stufe	Kommentare
D.2.c.1	Das Produkt erlaubt es, Patches (eigener Code, SOUP-/OTS-Komponenten) aufzuspielen.	1	Hersteller sollte Ausnahmen begründen können, ebenso, ob das Patchen remote erfolgen darf oder muss.
D.2.c.2	Das Produkt erlaubt es, fehlerhafte Patches wieder zu entfernen ("roll-back)".	2	

ID	Anforderung	Stufe	Kommentare
D.2.c.3	Das Produkt beschränkt die Möglichkeit, Patches aufzuspielen oder zu entfernen auf die berechtigten (authentifizieren und autorisierten) Benutzer.[C3c-01]	2	
D.2.c.4	Das Produkt prüft geänderten Programm-Code (Patches) vor der ersten Verwendung sowie beim Neustart auf Integrität. [C2c-02]	2	Diese Prüfungen erfolgen üblicherweise über Signaturen, die selbst vor Fälschung gesichert sein müssen

[**C2c-01**] Diese Prüfung erfolgt üblicherweise auf einem rollenbasierten Berechtigungskonzept sowie einer Authentifizierung der Nutzer.

[**C2c-02**] Dies ist ein Sonderfall der Forderung, dass jeder Programm-Code beim Neustart auf Integrität zu prüfen ist. Der Programm-Code beinhaltet die Software und die Firmware. Die Prüfung muss kryptographische Verfahren nutzen.

d) Sonstiges

ID	Anforderung	Stufe	Kommentare
D.2.d.1	Das Produkt protokolliert alle wesentlichen Aktionen [C3d-01] am/im System in einem Audit-Log, inklusive Tag und Uhrzeit und Akteur (Nutzer, System)	2	
D.2.d.2	Das Produkt stellt sicher, das es die korrekte Systemzeit hat	3	sich den Mechanismus erklären lassen. Auch wie sichergestellt ist, dass Nutzer die Uhrzeit nicht ungewollt und unbemerkt ändern können
D.2.d.3	Das Produkt schützt das Audit-Log vor Veränderung	2	sich vom Hersteller erklären lassen, wie der Schutz gewährleistet wird und wie eine Änderung des Audit-Logs vom System identifiziert wird. Ggf. sogar verantwortliche Software-Komponente zeigen lassen
D.2.d.4	Das Produkt implementiert Mechanismen, mit denen ein Einbruch oder Angriff [C3d-02] erkannt und darauf reagiert[C3d-03] werden kann	3	
D.2.d.5	Das Produkt erlaubt den Austausch von Zertifikaten	2	

[**C3d-01**] z.B. erfolgreiche und nicht erfolgreiche Anmeldeversuche, Aufruf wesentlicher Funktionen (inklusive Ändern von Konfigurationseinstellungen), Identifikation von Sicherheitsproblemen (z.B. durch Geräte eigenständig durchgeführte Selbsttests, Detektion von Malware, etc.), Aufspielen und Entfernen von Patches, Anlegen, Ändern und Löschen von Benutzern, Passwörtern und Berechtigungen, Hinzufügen oder Entfernen von Speichermedien, Anschluss oder Entfernen von Nachbarsystemen

[**C3d-02**] Nicht so allgemein formulieren, sondern konkrete Systemanforderung spezifizieren z.B. System erkennt eine CPU-Auslastung größer x%, eine Datenverkehr größer y MB/s, ein Speichermedium, dass voller ist als z%, mehr als n Einlog-Versuche innerhalb m Minuten usw.

[**C3d-03**] Ebenfalls sehr spezifisch formulieren, idealerweise über ein an den Schnittstellen beobachtbares Verhalten wie "schaltet sich aus", "deaktiviert die Datenverbindung", "zeigt folgende Warnmeldung an" usw.

3. System-/Software-Architektur

ID	Anforderung	Stufe	Kommentare
D.3.1	Die Software verwendet für alle kryptographischen Funktionen (z.B. Verschlüsselung, Signierung) ausschließlich bewährte Bibliotheken / Komponenten (keine eigene Implementierung). C3-01	1	die Bibliothek muss in der Liste der SOUP-/OTS-Komponenten enthalten sein. Vom Hersteller sich die Auswahl(kriterien) erklären lassen
D.3.2	Die Software verwendet für unterschiedliche Funktionen (z.B. Verschlüsselung der Kommunikation, Verschlüsselung der Daten) unterschiedliche Technologien oder Schlüssel.	3	
D.3.3	Die Software ist soweit technisch möglich vor Malware (Viren, Würmern usw.) geschützt.	1	Sich erklären lassen, wie das System vor Malware geschützt ist und wie dieser Schutz aufrechterhalten wird
D.3.4	Die Software basiert auf den Versionen der SOUP-/OTS-Komponenten, die keine sicherheitsrelevanten Schwachstellen enthalten. Ausnahmen sind begründet	1	sich in SOUP-Liste ein Beispiel herauspicken und auf der Herstellerseite die Version recherchieren und prüfen, welche Schwachstellen in Nachfolge-Versionen gepatched wurden

[**C3-01**] Die FDA besteht auf dem https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Standards und der NIST FIPS 140-2 Suite B .

4. Begleitmaterialien

Die Begleitmaterialien beziehen sich v.a. auf die Gebrauchs- und Installationsanweisungen. Ggf. müssen die Hersteller auch Trainingsmaterialien bereithalten.

ID	Anforderung	Stufe	Kommentare
D.4.1	Die Gebrauchsanweisung legt die vorgesehene IT-Umgebung für den Betrieb fest.[13]	1	
D.4.2	Die Gebrauchsanweisung legt fest, welche Aktivitäten[14] die Betreiber wie und wie häufig durchführen müssen.	1	
D.4.3	Die Installations- und Service-Anleitungen legen fest, welche weiteren Rollen (Betreiber, Service-Techniker) welche Aktivitäten[15] wie häufig durchführen müssen.	1	

ID	Anforderung	Stufe	Kommentare
D.4.4	Die Begleitmaterialien beschreiben, wie mit verlorengegangenen oder gestohlenen Authentifizierungs-Elementen (z.B. Karten, Zertifikaten, kryptographischen Schlüsseln) sowie mit vergessenen Passwörtern umgegangen werden soll.	1	
D.4.5	Die Begleitmaterialien beschreiben, wie die Anwender erkennen können, dass das Produkt ein Problem mit der IT-Sicherheit hat, und wie sie sich in diesem Fall verhalten sollen.	2	Dies bedingt, dass das Produkt diese Detektion implementiert
D.4.6	Die Begleitmaterialien beschreiben, welche Anti-Malware-Software für das Produkt zugelassen und von wo (z.B. Link) diese zu beziehen ist und wer für deren Aktualisierung verantwortlich ist.	2	nur soweit anwendbar
D.4.7	Die Begleitmaterialien enthalten die Kontaktdaten des Herstellers, über die dieser z.B. bei Problemen mit der IT-Sicherheit zu erreichen ist. D4-04	1	
D.4.8	Die Begleitmaterialien beschreiben das Produkt auch technisch D4-05	2	Das ist insbesondre eine FDA Anforderung

[**13**] Beispiele: Netzwerk / Schnittstellen (Bandbreite, Verfügbarkeit, Ports, IP-Ranges, Latenzen, Verschlüsselung, Firewalls usw.), Virenschutz, Betriebssysteme, physische Zugriffsberechtigungen, andere Software, die zeitgleich auf dem System laufen darf oder eben nicht (Spiele?, Firewall, Datenbank, Webserver). Die FDA verlangt bei den Schnittstellen auch eine Angabe über die Richtung der Kommunikation.

[**14**] Beispiele: Ausbildung der Anwender (z.B. zum Umgang mit Passwörtern), Aktualisierung des Virenschutzes, Information des Herstellers über Zwischenfälle, Aufspielen von Updates und Patches, Monitoring, Backup (und Restore)

[**15**] Beispiele: Installation, Anschluss an Netzwerk, Auswerten der Audit-Logs, Löschen nicht benötigter Benutzer, Austausch von Schlüsseln oder Zertifikaten, Löschen von temporären Dateien

[**D4-04**] Ggf. muss der Hersteller auch angeben, für welchen Zeitraum er beabsichtigt, den Support anzubieten.

[**D4-05**] Netzwerk-, Architektur, Fluss- und Zustanddiagramme. Schnittstellen, Komponenten, Kommunikationspfade, Authentifizierungsmechanismen für jede kommunizierende "Komponente" wie Webseiten, Server, Cloud-Speicher und Interoperable Systeme. "Design Features", die validierte Software-Updates und Patches gestatten. Liste aller Komponenten wie 3rd Party Software (s. CBOM der FDA)

E) Anhänge

1. Priorisierung

Bei der Priorisierung von Anforderungen berücksichtigt der Leitfaden folgende Dimensionen:

- Risiko für den einzelnen Patienten (Kombination von Schweregrade und Wahrscheinlichkeit von Schäden)
- Tragweite (nur ein Patient, ganzes Krankenhaus etc.)
- Umsetzbarkeit (finanzieller und zeitlicher Aufwand, Voraussetzungen bezüglich Werkzeuge)

Die Priorisierung mündet in den folgenden Reifegradstufen

- **Stufe 0 ("Laien-Niveau")**: Selbst die meisten Laien würden diese Anforderung erfüllen. Wer nicht einmal die Anforderungen dieser Stufe erfüllt, sollte keine Medizinprodukte entwickeln. Diese Anforderungen darf und muss ein Auditor bereits im allerersten Audit als erfüllt erwarten.
- **Stufe 1 (Niveau "fortgeschrittener Anfänger")**: Der Hersteller hat sich des Themas IT-Sicherheit bereits angenommen. Bei unkritischeren Produkten und den ersten Audits kann dieses Niveau akzeptiert werden. In jedem Folgejahr wird jedoch eine Verbesserung erwartet, bis die Stufe 2 erreicht wird.
- **Stufe 2 ("State-of-the-art")**: Das ist das Niveau, das Hersteller auf Dauer in der Regel erreichen müssen. Es entspricht aber noch nicht dem Stand der Wissenschaft.
- **Stufe 3 ("Experten-Niveau")**: Dieses Niveau erreichen hauptberufliche IT-Security-Experten. Es geht über das hinaus, was ein Auditor in der Regel bei Medizinprodukten erwarten darf. Energieversorger, Geheimdienste und das Militär müssten auf diesem Niveau agieren.

Abhängig vom Risiko eines Produkts kann ein Auditor bzw. Prüfe bereits von Beginn an eine bestimmte Stufe voraussetzen[E2-01].

[**E2-01**] Die Sicherheit der Patienten hat Vorrang, auch wenn dieser Ansatz dem Grundgedanken dieses Leitfadens widerspricht, besser Schritt für Schritt die IT-Sicherheit zu erhöhen, als gar nicht ins Handeln zu kommen.

2. Weiterführende Literatur

a) Gesetze

- MDR
- IVDR
- DSGVO
- 21 CFR Part 11

b) Normen und Best-Practice Guides

- AAMI/TIR57
- EN IEC 60601-1
- IEC 62443-2-1
- IEC 62443-4-1
- IEC 62443-4-2
- IEC 82304-1
- IEC 80001-1
- IEC/TR 80001-2-2
- IEC/TR 80001-2-8
- UL 2900-1
- UL 2900-2-1
- BSI-CS 132
- ISO/IEC 29147: Information technology — Security techniques — Vulnerability disclosure
- FDA Guidance Documents
    - “Content of Premarket Submissions for Management of Cybersecurity in Medical Devices”
    - "Postmarket Management of Cybersecurity in Medical Devices"

- "Design Considerations and Premarket Submissions - Recommendations for Interoperable Medical Devices"
- “Wireless Medical Telemetry Risks and Recommendations”

- BSI Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte

c) Fachliteratur, Lehrbücher

- Eckert: IT-Sicherheit: Konzepte - Verfahren - Protokolle (De Gruyter Studium
- Johner Institut: Videotrainings zur IT-Sicherheit bei Medizinprodukten
- Aktuelle Trends im Blog von Bruce Schneier

3. Erwägungsgründe

1. Hersteller entwickeln immer mehr vernetzte Medizinprodukte. Dadurch erhöhen sich die Risiken durch mangelnde IT-Sicherheit (z.B. gegen Cyberangriffe). Kunden sind über den Stand der Technik bei Beschaffungen nicht informiert und tragen die Aufwände für Absicherung - vor oder nach IT-Zwischenfällen. Die Anzahl der IT-Zwischenfälle steigt, wobei die Professionalität der Angreifer schnell zunimmt. Dem tragen viele Hersteller nur unzureichend Rechnung.
2. Die EU-Verordnungen (MDR, IVDR) fordern explizit die IT-Sicherheit. Die EU-Richtlinien fordern dies indirekt. Diese Vorgaben finden sich in den jeweiligen Anhängen I mit den grundlegenden (Sicherheits- und Leistungs-)Anforderungen. Dabei geht die Risiko-Analyse für Informationssicherheit über die Analyse von Szenarien der zweckbestimmten Bedienung hinaus. Informationssicherheit soll nämlich gerade die Szenarien außerhalb der zweckbestimmten Verwendung abdecken, sodass der Begriff des vorhersehbaren Missbrauchs genauer analysiert werden muss, weil der Hersteller nunmehr alle technischen Invasionsmöglichkeiten in das vernetzte Medizingerät betrachten muss.
3. Im Gegensatz zu den meisten anderen grundlegenden Anforderungen sind keine Normen zum Thema IT-Sicherheit harmonisiert. Daher gibt es keinen kanonischen Katalog an Anforderungen, der anerkannt den geforderten Stand der Technik reflektiert.
4. Die FDA hat sowohl mehrere *Guidance Documents* veröffentlicht als auch Normen wie die UL 2900-2-1 anerkannt. Diese Vorgaben sind uneinheitlich bezüglich der Granularität, Vollständigkeit und konzeptionellen Integrität. Sie erfüllen nur bedingt die Ansprüche, die an die Qualität einer Norm üblicherweise gestellt werden.
5. Viele Normen sind kostenpflichtig (trotz teilweise fragwürdiger Qualität). Hersteller müssen nach Auffassung der Autoren kostenfrei Zugang zu regulatorischen Anforderungen haben.
6. Weil die meisten Medizinprodukthersteller die IT-Sicherheit nicht oder nur unzureichend adressieren, erfüllen sie die grundlegenden Anforderungen nur teilweise. Es herrscht auf kein Konsens in Europe, welche technischen und prozessualen Pflichten den Hersteller betreffen.
7. Für die meisten Hersteller wäre es weder zeitlich noch finanziell umsetzbar, mit einem Schlag ein IT-Sicherheits-Niveau zu erreichen, wie es z.B. der UL 2900 fordert. Daher sollten die Hersteller schrittweise ein State-of-the-Art Niveau bezüglich der IT-Sicherheit anstreben und erreichen. Damit verfolgt dieser Leitfaden das Ziel, lieber schnell erste Verbesserungen umzusetzen, als wegen Überforderung nichts zu tun.
8. IT-Sicherheit muss in allen Phasen des Produkt-Lebenszyklusprozessen berücksichtigt werden. Eine Beschränkung auf das Testen ist unzureichend. Zusammen mit technischen Produktmaßnahmen ("Controls") und Dokumentation möchte dieser Leitfaden auf drei Säulen für Informationssicherheit hinweisen: Anforderungen, Prozess, Dokumentation. Die Struktur des Leitfadens reflektiert diese Säulen und wird auch nach den absehbaren technologischen Anpassungen noch bestehen bleiben.
9. Es ist zu erwarten, dass Normen zur IT-Sicherheit von Medizinprodukten entwickelt und harmonisiert werden, was aber noch Jahre in Anspruch nehmen kann. Daher bedarf es eines Leitfadens (nur) in dieser Zwischenphase.

10. Dieser Leitfaden sollte sehr zeitnah (bis November 2018) zur Verfügung, um rasch den Herstellern als Orientierung zu dienen und es ihnen zu ermöglichen, sofort zu handeln. Die hohe Geschwindigkeit seiner Entwicklung macht Kompromisse bezüglich der Abstimmung mit möglichst vielen Parteien unumgänglich.
11. Da der Leitfaden von einer stufenweisen Annäherung auf den Stand der Technik ausgeht und zudem in sehr kurzer Zeit entstanden ist, kann er keinen Anspruch auf Vollständigkeit erheben.
12. Der Leitfaden soll dennoch ein weitgehend allgemein akzeptiertes Niveau an Anforderungen repräsentieren. Die Auswahl und Priorität dessen Anforderungen müssen daher möglichst transparent nachvollziehbar sein.
13. Ein solcher Leitfaden muss die Spezifika von Medizinprodukten berücksichtigen, wozu die Prinzipen der Patientensicherheit (Safety) und eines risikobasierten Ansatzes zählen. Im konkreten Fall können ausgewählte Maßnahmen der Informationssicherheit ("Controls") nämlich den grundlegenden Anforderungen entgegenstehen. Aus diesem Grund kann es für Medizingeräte keine feste Liste von "Controls" geben. Maßgeblich ist jeweils die vom Hersteller festgelegte Zweckbestimmung des Produkts.
14. Die einfache Verständlichkeit und Umsetzbarkeit ist entscheidend für den erhofften positiven Einfluss eines Leitfadens auf die IT-Sicherheit. Daher stellt er möglichst keine abstrakten oder "high level" Anforderungen, sondern nennt "binär entscheidbare" Prüfkriterien.
15. Um die Umsetzbarkeit zu erhöhen, vermeiden die Autoren auch, möglichst viele Anforderungen zusammenzutragen. Vielmehr beschränken sie sich auf diejenigen, die sie für besonders relevant und umsetzbar halten.
16. Auch um die Verteilung und den Bekanntheitsgrad zu fördern, soll der Leitfaden kostenfrei verfügbar sein und bleiben.
17. Der Leitfaden fordert bewusst keine konkreten Technologien oder Verfahren. Zum einen sind diese einer zu hohen Änderung unterworfen, zum anderen möchten sich die Autoren des Leitfadens nicht anmaßen, für die Hersteller zu entscheiden, welche Technologien und Verfahren im konkreten Anwendungsfall die besten sind.
18. Der Leitfaden sollte auf Deutsch und Englisch verfügbar sein.
19. Der Fokus liegt auf der IT-Sicherheit der Medizinprodukte, nicht auf der IT-Sicherheit von Organisationen wie Krankenhäusern oder Medizinprodukteherstellern. Die Autoren des Leitfadens sind sich bewusst, dass die Angriffe zunehmend auch die Lieferkette der Medizinproduktehersteller betreffen. Dem müssen künftige Versionen dieses Leitfadens durch Anforderungen an die Organisation Rechnung tragen.