

	DIN EN IEC 81001-5-1 (VDE 0750-103-5-1)	DIN
	Diese Norm ist zugleich eine VDE-Bestimmung im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation“ bekannt gegeben worden.	VDE

ICS 35.240.80

Einsprüche bis 2022-02-17

Entwurf

Sicherheit, Effektivität und Sicherheit von Gesundheitssoftware und Gesundheits-IT-Systemen –

Teil 5-1: Sicherheit –

Aktivitäten im Produktlebenszyklus

(IEC 62A/1419/CDV:2020);

Deutsche und Englische Fassung prEN IEC 81001-5-1:2020

Health Software and health IT systems safety, effectiveness and security –

Part 5-1: Security –

Activities in the product lifecycle

(IEC 62A/1419/CDV:2020);

German and English version prEN IEC 81001-5-1:2020

Logiciels de santé et sécurité, efficacité et sûreté des systèmes TI de santé –

Partie 5-1: Sûreté –

Activités du cycle de vie du produit

(IEC 62A/1419/CDV:2020);

Version allemande et anglaise prEN IEC 81001-5-1:2020

Anwendungswarnvermerk

Dieser Norm-Entwurf mit Erscheinungsdatum 2021-12-17 wird der Öffentlichkeit zur Prüfung und Stellungnahme vorgelegt.

Weil die beabsichtigte Norm von der vorliegenden Fassung abweichen kann, ist die Anwendung dieses Entwurfs besonders zu vereinbaren.

Stellungnahmen werden erbeten

- vorzugsweise online im Norm-Entwurfs-Portal von DIN unter www.din.de/go/entwuerfe bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter www.entwuerfe.normenbibliothek.de, sofern dort wiedergegeben;
- oder als Datei per E-Mail an dke@vde.com möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter www.din.de/go/stellungnahmen-norm-entwuerfe oder für Stellungnahmen zu Norm-Entwürfen der DKE unter www.dke.de/stellungnahme abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE, Stresemannallee 15, 60596 Frankfurt am Main.

Die Empfänger dieses Norm-Entwurfs werden gebeten, mit ihren Kommentaren jegliche relevanten Patentrechte, die sie kennen, mitzuteilen und unterstützende Dokumentationen zur Verfügung zu stellen. Gesamtumfang 111 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn dieser Norm ist

Nationales Vorwort

Die Deutsche Fassung des europäischen Dokuments prEN IEC 81001-5-1:2020-11 „Sicherheit, Effektivität und Sicherheit von Gesundheitssoftware und Gesundheits-IT-Systemen – Teil 5-1: Sicherheit – Aktivitäten im Produktlebenszyklus“ (Entwurf in der Umfrage) ist unverändert in diesen Norm-Entwurf übernommen worden.

Die Internationale Elektrotechnische Kommission (IEC) und das Europäische Komitee für Elektrotechnische Normung (CENELEC) haben vereinbart, dass ein auf IEC-Ebene erarbeiteter Entwurf für eine Internationale Norm zeitgleich (parallel) bei IEC und CENELEC zur Umfrage (CDV-Stadium) und Abstimmung als FDIS (en: Final Draft International Standard) bzw. Schluss-Entwurf für eine Europäische Norm gestellt wird, um eine Beschleunigung und Straffung der Normungsarbeit zu erreichen. Dem entsprechend ist das internationale Dokument IEC 62A/1419/CDV:2020-11 „Health Software and health IT systems safety, effectiveness and security – Part 5-1: Security – Activities in the product lifecycle“ unverändert in den Entwurf prEN IEC 81001-5-1:2020-11 übernommen worden.

Da die Deutsche Fassung noch nicht endgültig mit der Englischen und Französischen Fassung abgeglichen ist, ist die englische Originalfassung des IEC-CDV entsprechend der diesbezüglich durch die IEC erteilten Erlaubnis beigelegt. Die Nutzungsbedingungen für den deutschen Text des Norm-Entwurfes gelten gleichermaßen auch für den englischen IEC-Text.

Das internationale Dokument wurde vom IEC/SC 62A „Common aspects of electrical equipment used in medical practice“ der Internationalen Elektrotechnischen Kommission (IEC) erarbeitet und unterliegt dem Copyright der IEC . Das Dokument wurde den nationalen Komitees zur Stellungnahme vorgelegt.

Bei der Abstimmung zu dem Europäischen Schluss-Entwurf bei CENELEC und dem Internationalen Schluss-Entwurf bei IEC [Final Draft International Standard (FDIS)] sind jeweils nur „JA/NEIN“-Entscheidungen möglich, wobei „NEIN“-Entscheidungen fundiert begründet werden müssen. Dokumente, die bei CENELEC als Europäische Norm angenommen und ratifiziert werden, sind unverändert als Deutsche Normen zu übernehmen.

Für dieses Dokument ist das nationale Arbeitsgremium DKE/UK 811.3 „Sicherheit von medizinisch genutzten Geräten/Systemen/Einrichtungen in der vernetzten Anwendung“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Aktuelle Informationen zu diesem Dokument können über die Internetseiten von DKE (www.dke.de) und DIN (www.din.de) durch eine Suche nach der Dokumentennummer aufgerufen werden.

Für den Fall einer undatierten Verweisung im normativen Text (Verweisung auf ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

Für den Fall einer datierten Verweisung im normativen Text bezieht sich die Verweisung immer auf die in Bezug genommene Ausgabe des Dokuments.

Der Zusammenhang der zitierten Dokumente mit den entsprechenden deutschen Dokumenten ergibt sich, soweit ein Zusammenhang besteht, grundsätzlich über die Nummer der entsprechenden IEC-Publikation. Beispiel: IEC 60068 ist als EN 60068 als Europäische Norm durch CENELEC übernommen und als DIN EN 60068 ins Deutsche Normenwerk aufgenommen.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. IEC ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Das Original-Dokument enthält Bilder in Farbe, die in der Papierversion in einer Graustufen-Darstellung wiedergegeben werden. Elektronische Versionen dieses Dokuments enthalten die Bilder in der originalen Farbdarstellung.

Sicherheit, Effektivität und Sicherheit von Gesundheitssoftware und Gesundheits-IT-Systemen – Teil 5-1: Sicherheit – Aktivitäten im Produktlebenszyklus

Inhalt

	Seite
Einleitung.....	8
1 Anwendungsbereich.....	10
1.1 * Zweck.....	10
1.2 * Anwendungsgebiet.....	10
1.3 Übereinstimmung.....	11
2 Normative Verweisungen.....	12
3 Begriffe.....	12
4 Allgemeine Anforderungen.....	19
4.1 Qualitätsmanagement.....	19
4.1.1 Qualitätsmanagementsystem.....	19
4.1.2 Identifikation von Verantwortlichkeiten.....	20
4.1.3 Identifikation der Anwendbarkeit.....	20
4.2 Risikomanagement der IT-Sicherheit.....	20
5 Software-Entwicklungsprozess.....	21
5.1 Planung der Softwareentwicklung.....	21
5.1.1 Aktivitäten im Lebenszyklusprozess.....	21
5.1.2 IT-Sicherheit der Entwicklungsumgebung.....	21
5.1.3 Sichere Programmierstandards.....	21
5.2 Anforderungsanalyse der Gesundheitssoftware.....	21
5.2.1 IT-Sicherheitsanforderungen an Gesundheitssoftware.....	21
5.2.2 Überprüfung der IT-Sicherheitsanforderungen.....	22
5.2.3 IT-Sicherheitsrisiken für erforderliche Software.....	22
5.3 Entwurf der Software-Architektur.....	22
5.3.1 Defense-in-Depth-Architektur/-Entwurf	22
5.3.2 Dokumentation bewährter Verfahren für sicheren Entwurf.....	23
5.3.3 Überprüfung des Entwurfs der IT-Sicherheitsarchitektur.....	23
5.4 Softwareentwurf.....	23
5.4.1 Bewährte Verfahren für den Softwareentwurf.....	23
5.4.2 Sicherer Entwurf.....	24
5.4.3 Sichere Schnittstellen für Gesundheitssoftware.....	24
5.4.4 Verifizierung der IT-Sicherheit des detaillierten Entwurfs.....	24
5.5 Implementierung und Verifizierung von Software-Einheiten.....	25
5.5.1 Sichere Programmierstandards.....	25
5.5.2 Überprüfung der IT-Sicherheitsimplementierung.....	25
5.6 Softwareintegrationsprüfung.....	25
5.7 Prüfung des Softwaresystems.....	26

5.7.1	Prüfung der Anforderungen an die IT-Sicherheit.....	26
5.7.2	Prüfung der Bedrohungsabschwächung.....	26
5.7.3	Prüfung auf Schwachstellen.....	26
5.7.4	Eindringprüfung.....	27
5.8	Softwarefreigabe.....	27
5.8.1	Beheben von Befunden vor der Freigabe.....	27
5.8.2	Freigabedokumentation.....	27
5.8.3	Dateiintegrität.....	28
5.8.4	Maßnahmen für private Schlüssel.....	28
5.8.5	Bewertung und Behandlung von auf die IT-Sicherheit bezogenen Problemen.....	28
5.8.6	Abschluss der Aktivitäten.....	28
5.8.7	Richtlinien für die sichere Außerbetriebnahme für Gesundheitssoftware.....	28
6	Softwarewartungsprozess	29
6.1	Festlegung eines Plans für die Softwarewartung.....	29
6.1.1	Zeitnahe Auslieferung von IT-Sicherheits-Updates.....	29
6.2	Analyse von Problemen und Änderungen.....	29
6.2.1	Überwachung öffentlicher Vorfallsberichte.....	29
6.2.2	Verifizierung von IT-Sicherheits-Updates.....	29
6.3	Implementierung von Änderungen.....	30
6.3.1	Dokumentation von IT-Sicherheits-Updates für unterstützte Software.....	30
6.3.2	Auslieferung von IT-Sicherheits-Updates für gewartete Software.....	30
6.3.3	Integrität von IT-Sicherheits-Updates für gewartete Software.....	30
7	IT-Sicherheits-Risikomanagement.....	31
7.1	Risikomanagement-Kontext.....	31
7.1.1	Sicherheitsumfeld des Produkts.....	31
7.2	Identifizierung von Schwachstellen, Bedrohungen und damit verbundenen negativen Auswirkungen.....	31
7.3	Einschätzung und Bewertung des IT-Sicherheitsrisikos.....	32
7.4	IT-Sicherheitsrisikobeherrschung.....	33
7.5	Überwachung der Wirksamkeit von Maßnahmen zur Risikobeherrschung.....	33
8	Software-Konfigurationsmanagementprozess	33
9	Problemlösungsprozess für Software.....	33
9.1	Überblick.....	33
9.2	Empfang von Benachrichtigungen über Schwachstellen.....	34
9.3	Überprüfen von Schwachstellen.....	34
9.4	Analyse von Schwachstellen.....	34
9.5	Behandlung von auf die IT-Sicherheit bezogenen Problemen.....	35
10	Qualitätsmanagementsystem.....	36
10.1	IT-Sicherheitsexpertise.....	36
10.2	Softwarekomponenten von Drittanbietern.....	36

10.3	Kontinuierliche Verbesserung.....	37
10.4	Offenlegung von auf die IT-Sicherheit bezogenen Problemen.....	37
10.5	Periodische Überprüfung des Managements von IT-Sicherheitsmängeln.....	37
10.6	Überprüfung der Begleitdokumentation.....	38
Anhang A (informativ) Erläuterungen.....		39
A.1	Zusammenhang mit IEC 62443.....	39
A.2	Zusammenhang mit IEC 62304.....	39
A.3	Risikotransfer.....	39
A.3.1	Einleitung.....	39
A.3.2	Gewartete Software.....	40
A.3.3	Unterstützte Software.....	40
A.3.4	Erforderliche Software.....	40
A.4	Bewährte Verfahren der sicheren Programmierung.....	40
Anhang B (informativ) Leitfaden zur Implementierung von IT-Sicherheits-Lebenszyklusaktivitäten.....		42
B.1	Überblick.....	42
B.2	Verwandte Arbeiten.....	42
B.3	Bedrohungs- / Risikoanalyse (en: threat / risk analysis, TRA).....	42
B.4	Bedrohungs- und Risikomanagement.....	43
B.5	Planung der Softwareentwicklung.....	44
B.5.1	Entwicklung.....	44
B.5.2	Anforderungsanalyse der Gesundheitssoftware.....	44
B.5.3	Entwurf der Software-Architektur.....	44
B.5.4	Implementierung und Verifizierung von Software-Einheiten.....	45
B.5.5	Sichere Implementierung.....	45
B.5.6	Nicht verwendet.....	45
B.5.7	IT-Sicherheitsprüfung.....	45
Anhang C (informativ) Bedrohungsmodellierung.....		47
C.1	Allgemeines.....	47
C.2	Attack-Defense-Trees.....	47
C.3	CAPEC / OWASP / SANS.....	47
C.4	CWSS.....	47
C.5	DREAD.....	47
C.6	Liste bekannter potenzieller Schwachstellen.....	48
C.7	OCTAVE.....	48
C.8	STRIDE.....	48
C.9	Trike.....	48
C.10	VAST.....	48
Anhang D (informativ) Verhältnis zu Verfahren in IEC 62443-4-1.....		49
D.1	ISO/IEC 81001-5-1 zu IEC 62443-4-1:2018.....	49
D.2	IEC 62443-4-1:2018 zu IEC/ISO 81001-5-1.....	50

Anhang E (informativ) In IEC 62443-4-1 festgelegte Dokumente.....	53
E.1 Einleitung.....	53
E.2 Freigabedokumentation.....	53
E.2.1 Produktdokumentation.....	53
E.2.2 Dokumentation des Defense-in-Depth-Konzepts der Gesundheitssoftware.....	54
E.2.3 Defense-in-Depth-Maßnahmen, die in der Umgebung erwartet werden.....	54
E.2.4 Richtlinien zur IT-Sicherheitshärtung.....	54
E.2.5 Informationen zu IT-Sicherheits-Updates.....	55
E.3 Dokumente zur Außerbetriebnahme von Gesundheitssoftware.....	56
Anhang F (normativ) Gesundheitssoftware in der Umstellung.....	57
F.1 Einleitung.....	57
F.2 Aktivitäten vor Inverkehrbringen.....	57
F.3 Begründung für die Benutzung von Gesundheitssoftware in der Umstellung.....	58
F.4 Aktivitäten nach Inverkehrbringen.....	58
Literaturhinweise Verweisungen auf andere Normen.....	59
Bilder	
Bild 1: – Software-Lebenszyklusprozesse (abgeleitet von IEC 62304, Ausgabe 1.1).....	10
Bild 2: – Anwendungsgebiet für GESUNDHEITSSOFTWARE (Quelle: IEC 62304, Ausgabe 2).....	11

Einleitung

Diese Internationale Norm legt ergänzende AKTIVITÄTEN fest, die vom HERSTELLER von GESUNDHEITSSOFTWARE - einschließlich der in Medizinprodukte integrierten Software - als Teil eines sicheren EntwicklungsLEBENSZYKLUS durchgeführt werden. Dieses Dokument kann daher die Übereinstimmung mit IEC 62443-4-1 unterstützen.

Dieses Dokument soll grundlegende bewährte Verfahren für einen sicheren SoftwareLEBENSZYKLUS bieten. Lokale Gesetze und Vorschriften müssen berücksichtigt werden.

Die PROZESSANFORDERUNGEN wurden aus IEC 62443-4-1, PRODUKTLEBENSZYKLUS-Management, abgeleitet. Die Umsetzung dieser Spezifikationen wird bestehende PROZESSE beim HERSTELLER erweitern - insbesondere bestehende PROZESSE, die mit IEC 62304 übereinstimmen.

Dieses Dokument legt AKTIVITÄTEN für GESUNDHEITSSOFTWARE fest, deren LEBENSZYKLUS Teil eines integrierenden PRODUKTprojekts sein kann. Einige in diesem Dokument festgelegte AKTIVITÄTEN hängen von der Eingabe und Unterstützung durch den PRODUKTLEBENSZYKLUS ab (z. B. die Definition bestimmter Kriterien). Beispiele umfassen:

- RISIKOMANAGEMENT
- Anforderungen
- Prüfung
- Nach Inverkehrbringen

In Fällen, in denen AKTIVITÄTEN für GESUNDHEITSSOFTWARE Unterstützung durch PROZESSE auf PRODUKTEBENE benötigen, legt dieses Dokument entsprechende Anforderungen über den GESUNDHEITSSOFTWARE-LEBENSZYKLUS hinaus fest.

Wie IEC 62304 schreibt dieses Dokument kein spezifisches System von PROZESSEN vor, aber es fordert, dass bestimmte AKTIVITÄTEN während des GESUNDHEITSSOFTWARE-LEBENSZYKLUS durchgeführt werden.

Dieses Dokument legt AKTIVITÄTEN fest, die vom HERSTELLER auszuführen sind. Für die Zwecke dieses Dokuments schließt dies alle Stellen ein, die für die KonstruktionsAKTIVITÄTEN im LEBENSZYKLUS der GESUNDHEITSSOFTWARE verantwortlich sind.

Abschnitt Vier legt fest, dass HERSTELLERGESUNDHEITSSOFTWARE innerhalb eines Qualitätsmanagementsystems (siehe 4.1) und eines RISIKOMANAGEMENTSYSTEMS (4.2) entwickeln und pflegen.

Die Abschnitte Fünf bis Acht legen die AKTIVITÄTEN und das resultierende Ergebnis als Teil des vom HERSTELLER implementierten Software-LEBENSZYKLUSPROZESSES fest. Diese Spezifikationen sind in der Reihenfolge von IEC 62304 angeordnet.

Die Abschnitte Neun und Zehn legen die AKTIVITÄTEN und das resultierende Ergebnis als Teil des ProblemlösungsPROZESSES bzw. des Qualitätsmanagementsystems fest, die vom HERSTELLER implementiert werden.

Der Anwendungsbereich dieses Dokuments beschränkt sich auf GESUNDHEITSSOFTWARE und ihre Verbindungsfähigkeit mit der VORGESEHENEN NUTZUNGsumgebung, beruhend auf IEC 62304, jedoch mit Schwerpunkt auf IT-SICHERHEIT.

Für den Ausdruck von Bestimmungen in diesem Dokument

- ist „kann“ die Beschreibung einer Möglichkeit oder einer Fähigkeit und
- „muss“ (en: must) eine von außen auferlegte Einschränkung.

ANMERKUNG **GESUNDHEITSSOFTWARE** kann als Software auf den Markt gebracht, in Medizinprodukte integriert, als Software, die selbst als Medizinprodukt gilt, oder in eine Allzweck-Computerplattform integriert werden.

1 Anwendungsbereich

1.1 * Zweck

Dieses Dokument definiert die Anforderungen an den LEBENSZYKLUS für die Entwicklung und Wartung von GESUNDHEITSSOFTWARE, die zur Unterstützung der Übereinstimmung mit IEC 62443-4-1 erforderlich sind - unter Berücksichtigung der spezifischen Erfordernisse für GESUNDHEITSSOFTWARE. Die Zusammenstellung von PROZESSEN, AKTIVITÄTEN und AUFGABEN, die in diesem Dokument beschrieben werden, legt einen allgemeinen Rahmen für sichere GESUNDHEITSSOFTWARE-LEBENSZYKLUSPROZESSE fest.

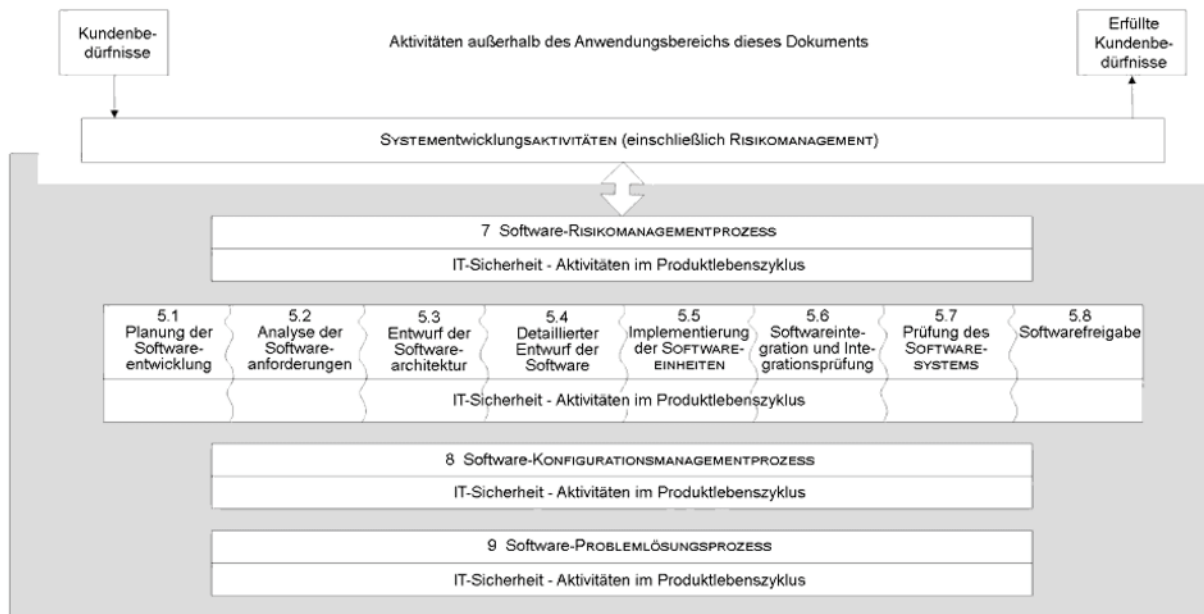


Bild 1: – Software-Lebenszyklusprozesse (abgeleitet von IEC 62304, Ausgabe 1.1)

Ziel ist es, die IT-SICHERHEIT von GESUNDHEITSSOFTWARE zu erhöhen, indem bestimmte AKTIVITÄTEN und AUFGABEN in den GESUNDHEITSSOFTWARE-LEBENSZYKLUSPROZESSEN vorgesehen werden und auch die SICHERHEIT der SOFTWARE-LEBENSZYKLUSPROZESSE selbst erhöht wird.

Es ist wichtig, ein angemessenes Gleichgewicht zwischen den Schlüsseleigenschaften SICHERHEIT, Effektivität und SCHUTZ zu erhalten, wie in IEC 81001-1 diskutiert.

Dieses Dokument enthält keine Festlegungen zum Inhalt der BEGLEITDOKUMENTATION.

1.2 * Anwendungsgebiet

Dieses Dokument gilt für die Entwicklung und Wartung von GESUNDHEITSSOFTWARE durch einen HERSTELLER, erkennt jedoch die entscheidende Bedeutung der wechselseitigen Kommunikation mit Organisationen (z. B. den HDO) an, die Verantwortung für die IT-SICHERHEIT der GESUNDHEITSSOFTWARE und der Systeme tragen, in die sie integriert ist, sobald die Software entwickelt und freigegeben worden ist. Die Normenreihe IEC/ISO 81001-5 (deren Teil 1 dies ist) wird daher so entwickelt, dass sie zukünftige Teile enthält, die sich mit der IT-SICHERHEIT für die Phasen der Implementierung, des Betriebs und der Nutzung des LEBENSZYKLUS für Organisationen wie HDO befassen.

Medizinprodukte-Software ist eine Teilmenge der GESUNDHEITSSOFTWARE. Aus diesem Grund gilt dieses Dokument für:

- Software als Teil eines Medizinprodukts;
- Software als Teil einer spezifischen Gesundheitshardware;
- Software als Medizinprodukt (en: software as a medical device, SaMD); und
- Nur-Software-Produkt für sonstige Anwendung im Gesundheitsbereich.

ANMERKUNG In diesem Dokument ist der Umfang der Software, die als Teil der LEBENSZYKLUSAKTIVITÄTEN für sichere GESUNDHEITSSOFTWARE betrachtet wird, größer und umfasst mehr Software (Treiber, Plattformen, Betriebssysteme) als bei der SICHERHEIT, da bei der IT-SICHERHEIT der Schwerpunkt auf jeglicher Nutzung einschließlich vorhersehbarer unbefugter Zugriffe und nicht nur auf der ZWECKBESTIMMUNG liegt.

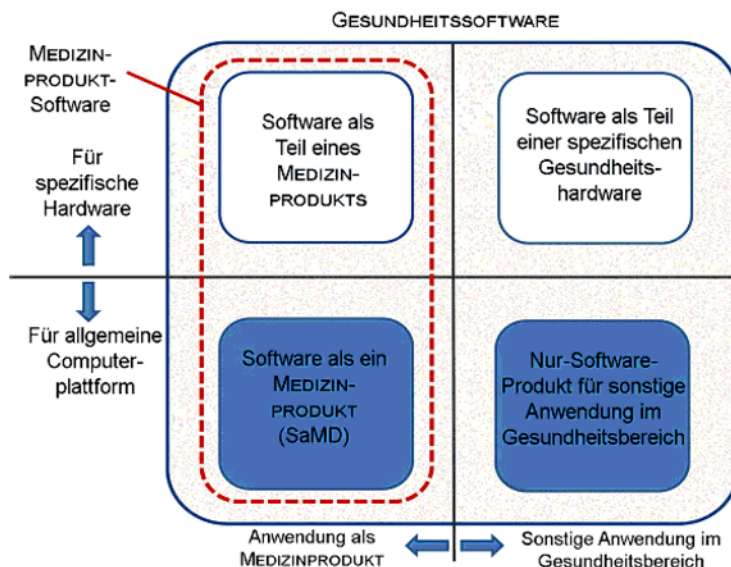


Bild 2: – Anwendungsgebiet für GESUNDHEITSSOFTWARE (Quelle: IEC 62304, Ausgabe 2)

1.3 Übereinstimmung

Die Übereinstimmung von GESUNDHEITSSOFTWARE mit diesem Dokument ist definiert als die Implementierung aller PROZESSE, AKTIVITÄTEN und AUFGABEN, die in den normativen Teilen dieses Dokuments benannt werden, mit Ausnahme von [Anhang F](#).

Die Übereinstimmung von GESUNDHEITSSOFTWARE IN DER UMSTELLUNG mit [Anhang F](#) dieses Dokuments ist definiert als die Implementierung aller PROZESSE, AKTIVITÄTEN und AUFGABEN, die in [Anhang F](#) dieses Dokuments benannt werden.

Übereinstimmung wird durch Untersuchung und durch Feststellung der Rückverfolgbarkeit der erforderlichen PROZESSE, AKTIVITÄTEN und AUFGABEN bestimmt.

Das Qualitätsmanagementsystem darf nach ISO 13485 oder anderen gleichwertigen Normen für Qualitätsmanagementsysteme implementiert werden.

IEC 62304 legt AKTIVITÄTEN fest, die auf der Klassifizierung der Software-SICHERHEIT beruhen. Die geforderten AKTIVITÄTEN werden im normativen Text von **IEC 62304** als „[Klasse A, B, C]“, „[Klasse B, C]“ oder „[Klasse C]“ gekennzeichnet, was darauf hinweist, dass sie selektiv abhängig von der Klassifizierung der Software, zu der sie gehören, gefordert werden. Die Anforderungen in diesem Dokument konzentrieren sich besonders auf die IT-SICHERHEIT und folgen daher nicht dem Konzept der SICHERHEITSKLASSEN. Für die Übereinstimmung mit diesem Dokument ist die Auswahl der AKTIVITÄTEN unabhängig von den SICHERHEITSKLASSEN.

Die Implementierung der in diesem Dokument festgelegten PROZESSE, AKTIVITÄTEN und AUFGABEN genügt, um die PROZESSanforderungen von IEC 62443-4-1 umzusetzen. HERSTELLER dürfen die Spezifikationen des Anhangs E implementieren, um eine vollständige Übereinstimmung mit IEC 62443-4-1 zu erreichen.

Dieses Dokument erfordert die Einführung eines oder mehrerer PROZESSE, die aus benannten AKTIVITÄTEN bestehen. Die LEBENSZYKLUSPROZESSE müssen diese AKTIVITÄTEN implementieren. Keine der Anforderungen in diesem Dokument erfordert es, diese AKTIVITÄTEN als einen einzelnen PROZESS oder als getrennte PROZESSE zu implementieren. Die in diesem Dokument festgelegten AKTIVITÄTEN sind üblicherweise Teil eines existierenden LEBENSZYKLUSPROZESSES.

2 Normative Verweisungen

Es gibt keine normativen Verweisungen in diesem Dokument.

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

ISO und IEC stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- IEC Electropedia: verfügbar unter <http://www.electropedia.org/>
- ISO Online Browsing Platform: verfügbar unter <http://www.iso.org/obp>

3.1

BEGLEITPAPIERE

Dokumentation, die einer GESUNDHEITSSOFTWARE und einem GESUNDHEITS-IT-SYSTEM oder einem Zubehör beigelegt ist und die Informationen für die verantwortliche Organisation oder den Bediener enthält, insbesondere bezüglich der SICHERHEIT

[QUELLE: ISO 81001-1:2020, 3.1]

3.2

AKTIVITÄT

Satz von einer oder mehreren aufeinander bezogenen oder sich gegenseitig beeinflussenden AUFGABEN

[QUELLE: IEC 62304:2021, 3.1]

3.3

ARCHITEKTUR

grundlegende Konzepte oder Eigenschaften eines Systems in seiner Umgebung, enthalten in seinen Elementen, Beziehungen und den Grundsätzen seiner Gestaltung und Entwicklung

[QUELLE: ISO/IEC/IEEE 24765:2017, 3.216, Definition 1]

3.4

RESSOURCE

physisches oder digitales Objekt, das für eine Person, eine Organisation oder eine Regierung einen Wert hat

Anmerkung 1 zum Begriff: Nach der Definition für eine RESSOURCE kann dies das Folgende umfassen:

- a) Daten und Informationen;
- b) GESUNDHEITSSOFTWARE und für seinen Betrieb benötigte Software;
- c) Hardwarekomponenten wie Computer, Mobilgeräte, Server, Datenbanken und Netzwerke;

- d) Dienste, einschließlich IT-SICHERHEIT, Softwareentwicklung, IT-Betrieb und extern bereitgestellte Dienste wie Rechenzentren, Internet und Software-as-a-Service sowie Cloud-Lösungen;
- e) Menschen und deren Qualifikationen, Fähigkeiten und Erfahrung;
- f) technische Verfahren und Dokumentation zur Verwaltung und Unterstützung der GESUNDHEITS-IT-INFRASTRUKTUR;
- g) GESUNDHEITS-IT-SYSTEME, die so konfiguriert und implementiert sind, dass sie die organisatorischen Ziele durch die Nutzung der RESSOURCEN erreichen; und
- h) immaterielle Werte wie Reputation und Ansehen.

[QUELLE: ISO 81001-1:2020, 3.3]

3.5

ANGRIFF

Versuch, einen WERT zu zerstören, aufzudecken, zu verändern, außer Funktion zu setzen, zu stehlen, zu diesem unbefugten Zugang zu erhalten oder diesen unbefugt zu verwenden

[QUELLE: ISO/IEC 27000:2018, 2.3]

3.6

ANGRIFFSFLÄCHE

physikalische und funktionale Schnittstellen eines Systems, die zugänglich sind und dadurch von einem Angreifer möglicherweise ausgenutzt werden können

[QUELLE: ISO/IEC 62443-4-1, 3.1.7]

3.7

VERFÜGBARKEIT

Eigenschaft, zugänglich und nutzbar zu sein, wenn eine befugte Entität Bedarf hat

[QUELLE: ISO/IEC 27000:2018, 2.9]

3.8

VERTRAULICHKEIT

die Eigenschaft, dass Informationen nicht unbefugten Personen, Entitäten oder PROZESSEN zugänglich gemacht oder offengelegt werden

[QUELLE: ISO/IEC 24767-1:2008, 2.1.2]

3.9

KONFIGURATIONSELEMENT

Einheit, die an einem gegebenen Referenzpunkt eindeutig identifiziert werden kann

[QUELLE: IEC 62304:2021]

3.10

KONFIGURATIONSMANAGEMENT

PROZESS, der die Einheitlichkeit von KONFIGURATIONSELEMENTEN sicherstellt, indem er Mechanismen zur Identifizierung, Kontrolle und Verfolgung von Versionen von KONFIGURATIONSELEMENTEN verwendet

[QUELLE: IEC 81001-1:2020, modifiziert]

3.11

DEFENSE-IN-DEPTH-KONZEPT

Ansatz zur Verteidigung des Systems gegen einen beliebigen bestimmten ANGRIFF mit Anwendung mehrerer unabhängiger Methoden

Anmerkung 1 zum Begriff: Ein DEFENSE-IN-DEPTH-KONZEPT bedingt selbst bei Einzelsystemen IT-SICHERHEITS- und Erkennungsschichten und hat folgende Merkmale:

- beruht auf dem Grundgedanken, dass jede Schutzmaßnahme überwunden werden kann und wahrscheinlich auch überwunden wird;
- Angreifer müssen jede Schicht überwinden oder umgehen, ohne dabei erkannt zu werden;
- eine Schwachstelle in einer Schicht kann durch die Fähigkeiten der anderen Schichten abgeschwächt werden;
- die IT-SICHERHEIT des Systems wird zu einem Satz von Schichten innerhalb der gesamten IT-NetzSICHERHEIT; und
- jede Schicht sollte eigenständig sein und nicht auf der gleichen Funktionalität wie die anderen Schichten beruhen, und sollte nicht die gleichen Ausfallarten wie diese aufweisen.

[QUELLE: IEC 62443-4-1, 3.1.15]

3.12

EXPLOIT (Substantiv)

definierter Weg, die IT-SICHERHEIT von IT-Systemen durch eine SCHWACHSTELLE zu verletzen

[QUELLE: ISO/IEC 27039:2015]

3.13

GESUNDHEITS-IT-INFRASTRUKTUR

kombinierter Satz von IT-RESSOURCEN, die dem Einzelnen oder der Organisation zur Entwicklung, Konfiguration, Integration, Wartung und Nutzung von IT-Diensten sowie zur Unterstützung von Gesundheit, Patientenversorgung und anderen organisatorischen Zielen zur Verfügung stehen

[QUELLE: ISO 81001-1:202x, 3.21]

3.14

GESUNDHEITS-IT-SYSTEM

eine Kombination von interagierenden Gesundheitsinformationselementen (einschließlich GESUNDHEITSSOFTWARE, Medizinprodukten, IT-Hardware, Schnittstellen, Daten, Verfahren und Dokumentation), die so konfiguriert und implementiert ist, dass sie die spezifischen Gesundheitsziele einer Person oder Organisation unterstützt und ermöglicht

[QUELLE: ISO 81001-1:2020, 3.22]

3.15

GESUNDHEITSSOFTWARE

Software, die speziell für das Management, die Aufrechterhaltung oder Verbesserung der Gesundheit von einzelnen Personen oder für die Pflege bestimmt ist, oder die entwickelt wurde, um in ein Medizinprodukt integriert zu werden

Anmerkung 1 zum Begriff: GESUNDHEITSSOFTWARE schließt Software als Medizinprodukt vollständig ein.

[QUELLE: ISO 81001-1:2020, 3.23]

3.16

GESUNDHEITSVERSORGUNGSORGANISATION

HDO, en: healthcare delivery organization

Einrichtung oder Unternehmen wie eine Klinik oder ein Hospital, die/das Dienstleistungen für die Gesundheitsversorgung bereitstellt

[QUELLE: ISO 81001-1:2020, 3.24]

3.17

INTEGRITÄT

Eigenschaft der Richtigkeit und Vollständigkeit

[QUELLE: ISO/IEC 27000:2018, 2.40]

3.18

VORGESEHENE NUTZUNGsumgebung

Bedingungen und Umfeld, in denen Benutzer mit der GESUNDHEITSSOFTWARE interagieren - wie vom HERSTELLER festgelegt

3.19

ZWECKBESTIMMUNG

ZWECKBESTIMMUNG

Verwendung, für die ein PRODUKT, ein PROZESS oder eine Dienstleistung nach den vom HERSTELLER erstellten Spezifikationen, Anweisungen und Informationen vorgesehen ist

Anmerkung 1 zum Begriff: Die vorgesehene medizinische Indikation, die Patientenpopulation, der Körperteil oder die Art des Gewebes, mit dem interagiert wird, das Benutzerprofil, die VORGESEHENE NUTZUNGsumgebung und das Funktionsprinzip sind typische Elemente der ZWECKBESTIMMUNG.

[QUELLE: ISO 81001-1:2020, 3.28, Anmerkung 1 modifiziert – „NUTZUNGsumgebung“ (en: use environment) durch „VORGESEHENE NUTZUNGsumgebung“ (en: intended environment of use) ersetzt.]

3.20

LEBENSZYKLUS

Abfolge aller Phasen im Leben eines PRODUKTS oder Systems, von der ersten Konzeption bis zur endgültigen Außerbetriebnahme und Entsorgung

[QUELLE: ISO 81001-1:2020, 3.32]

3.21

GEWARTETE SOFTWARE

SOFTWAREKOMPONENTE, für die der HERSTELLER das Risiko in Bezug auf die IT-SICHERHEIT übernimmt

Anmerkung 1 zum Begriff: Siehe auch [Anhang A.3](#).

3.22

HERSTELLER

natürliche oder juristische Person, die für die KonstruktionsAKTIVITÄTEN im LEBENSZYKLUS der GESUNDHEITSSOFTWARE verantwortlich ist

Anmerkung 1 zum Begriff: Die Konstruktion umfasst AKTIVITÄTEN zur Konzeption, zum Entwurf, zur Implementierung, zur Paketerstellung, zum Vertrieb und zur Wartung von GESUNDHEITSSOFTWARE.

Anmerkung 2 zum Begriff: Die Verantwortung erstreckt sich auf unterstützende AKTIVITÄTEN während des Betriebs.

Anmerkung 3 zum Begriff: Die Verantwortung kann bei mehreren Stellen entlang der Lieferkette, bei Dienstleistern oder bei Stellen in verschiedenen Phasen des LEBENSZYKLUS liegen.

Anmerkung 4 zum Begriff: Unabhängig davon wird jede spezifische rechtliche Verantwortlichkeit durch Verträge und Gesetze festgelegt.

3.23

PROZESS

Satz zusammenhängender oder sich gegenseitig beeinflussender AKTIVITÄTEN, der Eingaben zum Erzielen eines vorgesehenen Resultats (Ergebnisses) verwendet

[QUELLE: ISO 81001-1:202x, 3.38, modifiziert – "(Ergebnisses)" nach "Resultats" hinzugefügt.]

3.24

PRODUKT

Arbeitsergebnis einer Organisation, das ohne jegliche Transaktion zwischen Organisation und Kunden erzeugt werden kann

Anmerkung 1 zum Begriff: Die Erzeugung eines PRODUKTS wird erreicht, ohne dass notwendigerweise zwischen Anbieter und Kunden eine Transaktion stattfindet, sie kann jedoch dieses Dienstleistungselement bei der Lieferung an den Kunden einschließen.

Anmerkung 2 zum Begriff: Das vorherrschende Element eines PRODUKTS ist, dass es im allgemeinen materiell ist.

[QUELLE: ISO 81001-1:2020, 3.39]

3.25

ERFORDERLICHE SOFTWARE

SOFTWAREKOMPONENTE, für die der HERSTELLER Risiken in Bezug auf die IT-SICHERHEIT berücksichtigt, die vor der Freigabe der GESUNDHEITSSOFTWARE bekannt sind

Anmerkung 1 zum Begriff: Dies schließt UNTERSTÜTZTE SOFTWARE ein. Siehe [Anhang A.3](#).

3.26

RESTRISIKO

Risiko, das nach der Durchführung von Maßnahmen zur RISIKOBEHERRSCHUNG verbleibt

[QUELLE: ISO 81001-1:2020, 3.42]

3.27

RISIKOBEHERRSCHUNG

PROZESS, in dem Entscheidungen getroffen und Maßnahmen implementiert werden, durch die Risiken auf festgelegte Niveaus verringert oder innerhalb dieser gehalten werden

[QUELLE: ISO 81001-1:2020, 3.47]

3.28

RISIKOMANAGEMENT

systematische Anwendung von Managementstrategien, Verfahren und Praktiken auf die AUFGABEN der Analyse, Bewertung, Beherrschung und Überwachung von Risiken

[QUELLE: ISO 81001-1:2020, 3.50]

3.29

SICHERHEIT

Freiheit von unvertretbarem Risiko

Anmerkung 1 zum Begriff: Im Kontext der SICHERHEIT ist Risiko die Kombination der Wahrscheinlichkeit des Auftretens von Schäden und der Schwere der Schäden (siehe ISO/IEC Guide 51:2014).

Anmerkung 2 zum Begriff: Vorfälle im Bereich der IT-SICHERHEIT können zu Schäden führen und somit Auswirkungen auf die SICHERHEIT haben.

[QUELLE: ISO 81001-1:2020, 3.55, modifiziert – Anmerkungen zum Begriff hinzugefügt.]

3.30

SCHUTZ

IT-SICHERHEIT

Ein Zustand, in dem Informationen und Systeme vor unbefugten AKTIVITÄTEN wie Zugriff, Nutzung, Offenlegung,

Störung, Änderung oder Zerstörung in solch einem Maße geschützt sind, dass die damit verbundenen Risiken für VERTRAULICHKEIT, INTEGRITÄT und VERFÜGBARKEIT während des gesamten LEBENSZYKLUS auf einem akzeptablen Niveau gehalten werden

[QUELLE: ISO 81001-1:2020, 3.56]

3.31

SICHERHEITSFUNKTION

breite Kategorie von technischen, administrativen oder organisatorischen Maßnahmen zur Handhabung von Risiken für die VERTRAULICHKEIT, INTEGRITÄT, VERFÜGBARKEIT und Nachvollziehbarkeit von Daten und Systemen

[QUELLE: ISO 81001-1:2020, 3.57]

3.32

SICHERHEITSUMFELD

Mindestanforderungen und Annahmen über die Umgebung der GESUNDHEITSSOFTWARE - abgeleitet von der VORGESEHENEN NUTZUNGsumgebung auf PRODUKTEbene, unter zusätzlicher Berücksichtigung der Konfiguration und Integration der GESUNDHEITSSOFTWARE und unter Berücksichtigung des vorhersehbaren unbefugten oder unbeabsichtigten Zugriffs

3.33

ANALYSE DER SOFTWAREZUSAMMENSETZUNG

(elektronische) Analyse von Binärdateien

Anmerkung 1 zum Begriff: ANALYSE DER SOFTWAREZUSAMMENSETZUNG kann durch Werkzeuge oder Online-Dienste unterstützt werden.

3.34

SOFTWAREKOMPONENTE

jedes identifizierbare Teil eines Computerprogramms, d. h. Quellcode, Objektcode, Kontrollcode Kontrolldaten oder eine Zusammenstellung dieser Teile

[QUELLE: IEC 62304:2021, 3.32,]

3.35

SOFTWAREWARTUNG

Änderung von GESUNDHEITSSOFTWARE nach der Freigabe für ihre ZWECKBESTIMMUNG aus einem oder mehreren der folgenden Gründe:

- a) korrektiv, wie Fehlerbehebung;
- b) adaptiv, wie Anpassung an eine neue Hardware- oder Software-Plattform;
- c) verbessernd, wie Implementierung neuer Anforderungen;
- d) vorbeugend, wie die Erhöhung der Wartbarkeit.

Anmerkung 1 zum Begriff: Siehe auch ISO/IEC 14764:2006, 3.10.

[QUELLE: IEC 82304-1:2016, 3.21, modifiziert – In der Definition wurden die Worte „GESUNDHEITSSOFTWARE-PRODUKT“ durch „GESUNDHEITSSOFTWARE“ ersetzt, und Verweisung 3.10 wurde zur Anmerkung zum Begriff hinzugefügt, und „Hard-“ wurde durch „Hardware-“ ersetzt.]

3.36

UNTERSTÜTZTE SOFTWARE

SOFTWAREKOMPONENTE, für die der HERSTELLER den Kunden über bekannte Risiken in Bezug auf die IT-SICHERHEIT unterrichtet

Anmerkung 1 zum Begriff: Dies schließt GEWARTETE SOFTWARE ein. Siehe Anhang A.3.

3.37

AUFGABE

Teilarbeit, die erledigt werden muss, um ein bestimmtes Ziel zu erreichen

[QUELLE: IEC 62304:2021, 3.38, modifiziert – um ein bestimmtes Ziel zu erreichen]

3.38

BEDROHUNG

Potential für die Verletzung der SICHERHEIT, das besteht, wenn es einen Umstand, eine Fähigkeit, eine Aktion oder ein Ereignis gibt, die die IT-SICHERHEIT verletzen und die VERTRAULICHKEIT, INTEGRITÄT, VERFÜGBARKEIT von InformationsRESSOURCEN schädigen könnten

[QUELLE: ISO 81001-1:2020, 3.62]

3.39

BEDROHUNGSMODELL

dokumentiertes Ergebnis der AKTIVITÄT der BEDROHUNGSMODELLIERUNG

3.40

BEDROHUNGSMODELLIERUNG

systematische Erforschungstechnik zur Aufdeckung von Umständen oder Ereignissen, die das Potential haben, einem System Schaden in Form von Zerstörung, Offenlegung, Veränderung von Daten oder Denial-of-Service zuzufügen

[QUELLE: ISO 24765:2017, modifiziert – Ersatz von „Schaden“ (en: harm) durch „Schaden“ (en: damage).]

3.41

RÜCKVERFOLGBARKEIT

Verbindung zwischen dem Ursprung der Anforderungen über den gesamten ProjektLEBENSZYKLUS zu den Entwurfs-elementen und den Testfällen

[QUELLE: EN ISO 24765:2017, modifiziert]

3.42

GESUNDHEITSSOFTWARE IN DER UMSTELLUNG

GESUNDHEITSSOFTWARE, die vor der Veröffentlichung dieses Dokuments freigegeben wurde und die nicht alle im normativen Teil dieses Dokuments festgelegten Anforderungen erfüllt

Anmerkung 1 zum Begriff: Für GESUNDHEITSSOFTWARE IN DER UMSTELLUNG kann ihr HERSTELLER die Übereinstimmung mit [Anhang F](#), GESUNDHEITSSOFTWARE IN DER UMSTELLUNG, dieses Dokuments erklären.

3.43

VERTRAUENSGRENZE

Element eines BEDROHUNGSMODELLS, das eine Grenze darstellt, an der eine Authentifizierung erforderlich ist oder eine Änderung der Vertrauensstufe erfolgt (höher zu niedriger oder umgekehrt)

Anmerkung 1 zum Begriff: Mechanismen zur Durchsetzung von VERTRAUENSGRENZEN für PRODUKTbenutzer umfassen normalerweise Authentifizierung (beispielsweise Challenge/Response, Passwörter, Biometrie oder digitale Signaturen) und zugehörige Autorisierung (beispielsweise Regeln zur Zugriffskontrolle).

Anmerkung 2 zum Begriff: Mechanismen zur Durchsetzung von VERTRAUENSGRENZEN für Daten umfassen normalerweise Authentifizierung (beispielsweise Nachrichtenauthentifizierungs-codes und digitale Signaturen) und/oder InhaltsVALIDIERUNG.

3.44

NUTZUNGSUMGEBUNG

tatsächliche Bedingungen und Umfeld, in denen Benutzer mit der GESUNDHEITSSOFTWARE interagieren

Anmerkung 1 zum Begriff: Für die Zwecke dieses Dokuments schließt dies Datenschnittstellen ein.

[QUELLE: IEC 62366-1:2015; 3.20, modifiziert]

3.45

VALIDIERUNG

Bestätigung durch Bereitstellung eines objektiven Nachweises, dass die Anforderungen für einen spezifischen beabsichtigten Gebrauch oder eine spezifische beabsichtigte Anwendung erfüllt worden sind

Anmerkung 1 zum Begriff: Der für eine VALIDIERUNG erforderliche objektive Nachweis ist das Ergebnis eines Tests oder einer anderen Form der Bestimmung, z. B. Durchführen alternativer Berechnungen oder Überprüfen von Dokumenten.

Anmerkung 2 zum Begriff: Die Benennung „validiert“ wird zur Bezeichnung des entsprechenden Status verwendet.

Anmerkung 3 zum Begriff: Die Anwendungsbedingungen für VALIDIERUNG können echt oder simuliert sein.

[QUELLE: ISO 9000:2015, 3.8.13]

3.46

VERIFIZIERUNG

Bestätigung durch Bereitstellung eines objektiven Nachweises, dass festgelegte Anforderungen erfüllt worden sind

Anmerkung 1 zum Begriff: Der für eine VERIFIZIERUNG erforderliche objektive Nachweis kann das Ergebnis einer Prüfung oder anderer Formen der Bestimmung sein, z. B. Durchführen alternativer Berechnungen oder Überprüfen von Dokumenten.

Anmerkung 2 zum Begriff: Die für die VERIFIZIERUNG ausgeführten AKTIVITÄTEN werden manchmal als QualifizierungsPROZESS bezeichnet.

Anmerkung 3 zum Begriff: Das Wort „verifiziert“ bezeichnet den entsprechenden Status.

[QUELLE: ISO 81001-1:2020, 3.66, modifiziert – Anmerkung 1 zum Begriff wurde neu formuliert.]

3.47

SCHWACHSTELLE

Fehler oder SCHWÄCHE im Entwurf, der Implementierung oder dem Betrieb und Management eines Systems, der/die ausgenutzt werden könnte, um die IT-SICHERHEITSstrategie des Systems zu verletzen

[QUELLE: ISO 81001-1:2020, 3.67]

3.48

SCHWÄCHE

Art einer Unzulänglichkeit

Anmerkung 1 zum Begriff: Eine SCHWÄCHE kann zu einem IT-SICHERHEITSrisiko führen.

[QUELLE: ISO 81001-1:2020, 3.68, modifiziert]

4 Allgemeine Anforderungen

4.1 Qualitätsmanagement

4.1.1 Qualitätsmanagementsystem

Der HERSTELLER muss die AKTIVITÄTEN zur IT-SICHERHEIT im PRODUKTLEBENSZYKLUS auf der Grundlage eines etablierten und dokumentierten Qualitätsmanagementsystems

Im gesamten Dokument bedeutet „(eine) AKTIVITÄT(EN) einführen“, dass der HERSTELLER diese AKTIVITÄT(EN) dokumentieren und sicherstellen muss, dass diese AKTIVITÄT(EN) effektiv und vollständig durchgeführt wird (werden).

ANMERKUNG Erwägungen zur IT-SICHERHEIT in Qualitätsmanagementsystemen sind in [Abschnitt 10](#) beschrieben.

4.1.2 Identifikation von Verantwortlichkeiten

Der HERSTELLER muss die organisatorischen Rollen und das Personal, das für jede der in diesem Dokument geforderten AKTIVITÄTEN und PROZESSE verantwortlich ist, benennen und dokumentieren.

ANMERKUNG Personal kann durch funktionale Rollen anstelle von Namen identifiziert werden.

4.1.3 Identifikation der Anwendbarkeit

Der HERSTELLER MUSS die PRODUKTE oder Teile von PRODUKTEN identifizieren, für die der sichere LEBENSZYKLUS gilt.

ANMERKUNG 1 Bei GESUNDHEITSSOFTWARE werden eine gewisse IT-Vertrautheit sowie Netzwerk- oder Datenschnittstellenfähigkeiten vorausgesetzt, daher wird empfohlen, einen sicheren Software-LEBENSZYKLUS einzuhalten.

ANMERKUNG 2 Bei dieser Anforderung geht es nicht um PRODUKTinstanzen (und deren Identifikation), sondern um Typen von PRODUKTEN oder deren Teilen - zum Beispiel SOFTWAREKOMponenten. Das Vorhandensein dieser AKTIVITÄT(EN) bedeutet, dass der HERSTELLER über Kriterien verfügt, um zu bestimmen, welche Teile seiner PRODUKTE mit Hilfe der in diesem Dokument geforderten AKTIVITÄTEN entwickelt, gewartet und unterstützt werden sollen.

4.2 RISIKOMANAGEMENT der IT-SICHERHEIT

Der HERSTELLER muss einen PROZESS für das Management der mit der IT-SICHERHEIT verbundenen RISIKEN einführen. Dieser PROZESS muss die BEDROHUNGSMODELLIERUNG zur Identifizierung von SCHWACHSTELLEN, zur Abschätzung und Bewertung der damit verbundenen BEDROHUNGEN, zur Beherrschung dieser BEDROHUNGEN und zur Überwachung der Wirksamkeit der Maßnahmen zur RISIKOBEHERRSCHUNG (IT-SICHERHEIT) unter Berücksichtigung der ZWECKBESTIMMUNG und der NUTZUNGsumgebung der GESUNDHEITSSOFTWARE verwenden.

Der HERSTELLER muss die Kriterien für die Annehmbarkeit des Risikos aufstellen, die bei der Bestimmung der geeigneten Art und Weise des Umgangs mit jeder SCHWACHSTELLE angewendet werden müssen.

Das RISIKOMANAGEMENT FÜR DIE IT-SICHERHEIT sollte die Ergebnisse der AKTIVITÄT(EN) zur BEDROHUNGSMODELLIERUNG einbeziehen und den Richtlinien und bewährten Verfahren der Branche folgen.

Detaillierte PROZESSschritte sind in [Abschnitt 7](#) beschrieben.

ANMERKUNG Dieser PROZESS kann Teil eines bestehenden allgemeinen RISIKOMANAGEMENTPROZESSES sein. Das RISIKOMANAGEMENT FÜR DIE IT-SICHERHEIT kann im Rahmenwerk von ISO 14971 mit einer geeigneten Zuordnung von SCHWACHSTELLEN, BEDROHUNGEN und anderen auf die IT-SICHERHEIT bezogenen Begriffen und der Ergänzung von für die IT-SICHERHEIT relevanten AKTIVITÄTEN durchgeführt werden. (Siehe ISO/TR 24971:2020 für eine mögliche Zuordnung.)

Der HERSTELLER muss jedes RESTRISIKO im Zusammenhang mit einer SCHWACHSTELLE, das im System verbleibt, dokumentieren und muss auch die jeweils angewandten kompensierenden Maßnahmen dokumentieren.

Siehe [Anhang C](#) zur BEDROHUNGSMODELLIERUNG.

5 Software-EntwicklungsPROZESS

5.1 Planung der Softwareentwicklung

5.1.1 AKTIVITÄTEN im LEBENSZYKLUSPROZESS

Der HERSTELLER muss allgemeine LEBENSZYKLUSAKTIVITÄTEN - von der Konzeption bis zur Außerbetriebnahme - festlegen, die im Einklang mit einem allgemein anerkannten PRODUKTentwicklungsPROZESS stehen und in diesen integriert sind, einschließlich von unter anderem:

- a) KONFIGURATIONS MANAGEMENT mit Änderungsmaßnahmen und Änderungshistorie;
- b) PRODUKTbeschreibung und Anforderungsdefinition und RÜCKVERFOLGBARKEIT der Anforderungen;
- c) Praktiken für Entwurf und Implementierung von Software oder Hardware wie modularer Entwurf;
- d) PROZESS für wiederholbare Prüfungsverifizierung und -VALIDIERUNG;
- e) Überprüfung und Abnahme aller Aufzeichnungen zum EntwicklungsPROZESS;
- f) PRODUKTunterstützung; und
- g) IT-SICHERHEITS-Updates und -Patches für GESUNDHEITSSOFTWARE.

ANMERKUNG PRODUKTunterstützung bedeutet die Bereitstellung von Informationen, Hilfestellung und Schulung, um GESUNDHEITSSOFTWARE zu installieren und in der vorgesehenen Umgebung zu betreiben und verbesserte Fähigkeiten an die Benutzer zu verteilen. Siehe ISO 24765:2017.

Der HERSTELLER muss alle Begründungen dafür, warum Anforderungen dieses Dokuments in einem bestimmten GESUNDHEITSSOFTWARE-Projekt nicht umgesetzt werden, auf Grundlage der Überprüfung und Abnahme durch Mitarbeiter mit der geeigneten IT-SICHERHEITsexpertise dokumentieren.

5.1.2 IT-SICHERHEIT der Entwicklungsumgebung

Der HERSTELLER muss risikobasierte Verfahrens- und technische Maßnahmen zum Schutz der für die Entwicklung, Produktionsauslieferung und Wartung verwendeten IT-Infrastruktur vor unberechtigtem Zugriff, Verfälschung und Löschung einrichten. Dies umfasst den Schutz der GESUNDHEITSSOFTWARE während des Entwurfs, der Implementierung, der Updates, der Prüfungen und der Freigabe.

5.1.3 Sichere Programmierstandards

Der HERSTELLER muss sichere Programmierstandards einführen und aufrechterhalten, die mit gegenwärtigen bewährten Verfahren in Bezug auf Entwurf und Implementierung sicherer Softwaresysteme übereinstimmen.

Siehe [Anhang A](#).

5.2 Anforderungsanalyse der GESUNDHEITSSOFTWARE

5.2.1 IT-SICHERHEITSanforderungen an GESUNDHEITSSOFTWARE

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, die sicherstellen, dass die IT-SICHERHEITSanforderungen an die GESUNDHEITSSOFTWARE dokumentiert werden, einschließlich der Anforderungen an die SICHERHEITSFUNKTIONEN in Bezug auf Installation, Betrieb, Wartung und Außerbetriebnahme.

ANMERKUNG 1 IEC TR 60601-4-5 gibt Hinweise zur Festlegung von SICHERHEITSFUNKTIONEN und deren Dokumentation in der BEGLEITDOKUMENTATION und stellt ein Verfahren zur Ermittlung von Anforderungen aus der SICHERHEITSFUNKTIONSstufe zur Verfügung.

ANMERKUNG 2 IEC TR 80001-2-2 legt Erfordernisse in Bezug auf die IT-SICHERHEIT, Risiken und Maßnahmen als Leitfaden für die Offenlegung und Kommunikation zwischen dem HERSTELLER und der GESUNDHEITSVERSORGUNGSORGANISATION fest.

ANMERKUNG 3 Der PROZESS der PRODUKTANFORDERUNGEN hat Schnittstellen zu den Anforderungen der GESUNDHEITSSOFTWARE. Einige technische Maßnahmen können auf PRODUKTEBENE implementiert werden (zum Beispiel durch Hardware). Siehe [Anhang E.2.1](#).

5.2.2 Überprüfung der IT-SICHERHEITSANFORDERUNGEN

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, die sicherstellen, dass die IT-SICHERHEITSANFORDERUNGEN

- a) die PRODUKTANFORDERUNGEN einschließlich der Anforderungen für die RISIKOBEHERRSCHUNG implementieren;
- b) sich nicht gegenseitig widersprechen;
- c) so formuliert sind, dass Mehrdeutigkeit vermieden wird; und
- d) so formuliert sind, dass sie die Festlegung von Prüfkriterien und die Durchführung von Prüfungen ermöglichen.

Der HERSTELLER muss den Grad der Unabhängigkeit der Gutachter dokumentieren. Jede der folgenden repräsentativen Disziplinen muss an dieser/diesen AKTIVITÄT(EN) teilnehmen:

- a) Architekten/Entwickler (die die Anforderungen implementieren);
- b) Prüfer (die bestätigen, dass die Anforderungen erfüllt wurden);
- c) funktionsübergreifende Experten (darf solche mit klinischem Fachwissen einschließen); und
- d) Berater für IT-SICHERHEIT.

ANMERKUNG 1 Eine einzelne Person kann für mehrere Disziplinen verantwortlich sein. Es ist nicht ratsam, dass eine einzige Person alle Disziplinen vertritt.

ANMERKUNG 2 Die Liste der Disziplinen muss mindestens einmal je Projekt dokumentiert werden.

ANMERKUNG 3 Ein Qualitätsmanagementsystem wie das von ISO 13485 erfordert die Beachtung der Unabhängigkeit der Gutachter.

5.2.3 IT-SICHERHEITSRISIKEN FÜR ERFORDERLICHE SOFTWARE

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, die die IT-SICHERHEITSRISIKEN der gesamten ERFORDERLICHEN SOFTWARE identifiziert und verwaltet.

ANMERKUNG 1 Diese AKTIVITÄT(EN) stellt (stellen) sicher, dass die Anforderungen an die GESUNDHEITSSOFTWARE die IT-SICHERHEITSERFORDERNISSE der ERFORDERLICHEN SOFTWARE kennen.

ANMERKUNG 2 Diese AKTIVITÄT(EN) kann/können Teil von IT-SICHERHEITSAKTIVITÄTEN der Lieferkette sein.

5.3 Entwurf der Software-Architektur

5.3.1 DEFENSE-IN-DEPTH-ARCHITEKTUR/-Entwurf

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, die eine sichere ARCHITEKTUR festlegen.

In jeder Entwicklungsphase sollte der HERSTELLER das DEFENSE-IN-DEPTH-KONZEPT berücksichtigen und jeder Verteidigungsschicht technische Anforderungen zuordnen.

Bei der Identifizierung der technischen MAßNAHMEN ZUR RISIKOBEHERRSCHUNG FÜR DIE IT-SICHERHEIT muss der HERSTELLER die Anforderungen an die SICHERHEIT oder die Leistung der GESUNDHEITSSOFTWARE berücksichtigen.

Anmerkung 2 DEFENSE-IN-DEPTH darf in der BEGLEITDOKUMENTATION IT-SICHERHEITSanforderungen enthalten, die vom HDO zu implementieren sind.

5.3.2 Dokumentation bewährter Verfahren für sicheren Entwurf

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, die bewährte Verfahren für sicheren Entwurf identifizieren, durchsetzen und aufrechterhalten. Der HERSTELLER muss bewährte Verfahren für sicheren Entwurf dokumentieren, was unter anderem einschließen sollte:

- a) die Dokumentation aller VERTRAUENSGRENZEN als Teil des Entwurfs;
- b) geringste Rechte (Vergabe nur der zur Durchführung vorgesehener Betriebsabläufe erforderlichen Rechte an Benutzer/Software);
- c) Verwendung nachweislich sicherer SOFTWAREKOMPONENTEN/-Entwürfe, wo möglich;
- d) Wirtschaftlichkeit der Mechanismen (Streben nach einfachen Entwürfen);
- e) Verwendung sicherer Entwurfsmuster;
- f) Verringerung der ANGRIFFSFLÄCHE;
- g) Entfernung von Hintertüren, Zugängen für die und Informationen zur Fehlerbeseitigung, die während der Entwicklung verwendet wurden, oder Dokumentation ihres Vorhandenseins und der Notwendigkeit, sie vor unberechtigtem Zugriff zu schützen; und
- h) Schutz jeglicher verbleibender Informationen zur Fehlerbeseitigung vor unberechtigtem Zugriff.

Als Teil von DEFENSE-IN-DEPTH sollte der HERSTELLER die IT-SICHERHEITSARCHITEKTUR der GESUNDHEITSSOFTWARE einbeziehen und insbesondere auch einen Softwareentwurf dokumentieren, wenn er für die IT-SICHERHEIT von Bedeutung ist.

ANMERKUNG Siehe [Anhang B](#).

5.3.3 Überprüfung des Entwurfs der IT-SICHERHEITSarchitektur

Der HERSTELLER muss eine Überprüfung der Architektur der GESUNDHEITSSOFTWARE im Hinblick auf das Verhalten unter widrigen Bedingungen implementieren:

- a) wirkungsvolle Trennung von SOFTWAREKOMPONENTEN;
- b) die bewährten Verfahren für einen sicheren Entwurf (siehe [5.3.2](#)); und
- c) mögliche durch die ARCHITEKTUR eingeführte Mängel der IT-SICHERHEIT.

Der HERSTELLER muss die Überprüfung des Entwurfs der Architektur dokumentieren und implementieren.

ANMERKUNG Die Trennung verwendet technische Maßnahmen in Entwurf und Implementierung, um sicherzustellen, dass SOFTWAREKOMPONENTEN nicht durch andere SOFTWAREKOMPONENTEN der GESUNDHEITSSOFTWARE in unbeabsichtigter Weise beeinflusst werden können.

5.4 Softwareentwurf

5.4.1 Bewährte Verfahren für den Softwareentwurf

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um einen sicheren Entwurf von GESUNDHEITSSOFTWARE zu entwickeln und zu dokumentieren sowie die Verwendung bewährter Verfahren für den sicheren Entwurf beizubehalten, unter Berücksichtigung von:

- a) Softwaretechnik auf Anwendungsebene (zum Beispiel Algorithmen, Methoden)
- b) die verwendete Programmiertechnik (zum Beispiel Programmiersprache)
- c) die bewährten Verfahren für einen sicheren Entwurf in 5.3.2.

5.4.2 Sicherer Entwurf

Der Entwurf der GESUNDHEITSSOFTWARE muss eine Beschreibung der im BEDROHUNGSMODELL identifizierten BEDROHUNGEN enthalten.

ANMERKUNG Das SICHERHEITSUMFELD für GESUNDHEITSSOFTWARE wird aus der VORGESEHENEN NUTZUNGSUMGEBUNG auf PRODUKTEBENE abgeleitet, wobei auch die Konfiguration und Integration der GESUNDHEITSSOFTWARE berücksichtigt wird.

5.4.3 Sichere Schnittstellen für GESUNDHEITSSOFTWARE

Der Entwurf der GESUNDHEITSSOFTWARE muss jede Schnittstelle der GESUNDHEITSSOFTWARE identifizieren und charakterisieren, einschließlich physischer und logischer Schnittstellen. Der HERSTELLER identifiziert gegebenenfalls als Teil des Entwurfs:

- a) ob die Schnittstelle von außen (durch andere PRODUKTE) oder intern - zwischen SOFTWAREKOMPONENTEN der GESUNDHEITSSOFTWARE - oder beides zugänglich ist;
- b) IT-SICHERHEITSAUSWIRKUNGEN des SICHERHEITSUMFELDES DER GESUNDHEITSSOFTWARE auf die externe Schnittstelle;
- c) mögliche Benutzer der Schnittstelle und die RESSOURCEN, auf die über die Schnittstellen (direkt oder indirekt) zugegriffen werden kann;
- d) ob der statische Entwurf den Zugriff auf Schnittstellen über VERTRAUENSGRENZEN hinweg einschließt;
- e) Erwägungen zur IT-SICHERHEIT, Annahmen und/oder Einschränkungen im Zusammenhang mit der Verwendung der Schnittstelle im SICHERHEITSUMFELD DER GESUNDHEITSSOFTWARE; einschließlich zutreffender BEDROHUNGEN;
- f) die IT-SICHERHEITSrollen, -privilegien/-rechte und Zugriffskontrollberechtigungen, die für die Verwendung der Schnittstelle und den Zugriff auf die unter c) definierten RESSOURCEN erforderlich sind;
- g) die IT-SICHERHEITSFUNKTIONEN und/oder kompensierenden Mechanismen, die zum Schutz der Schnittstelle und der unter c) identifizierten RESSOURCEN verwendet werden, einschließlich der Validierung von Eingaben zur Laufzeit sowie der Behandlung von Ausgaben und Fehlern;
- h) die Verwendung von SOFTWAREKOMPONENTEN von Drittanbietern zur Implementierung der Schnittstelle und deren IT-SICHERHEITSFUNKTIONEN;
- i) eine Dokumentation, die die Verwendung der Schnittstelle beschreibt, wenn sie von außen zugänglich ist, und

ANMERKUNG Das SICHERHEITSUMFELD für GESUNDHEITSSOFTWARE wird aus der VORGESEHENEN NUTZUNGSUMGEBUNG auf PRODUKTEBENE abgeleitet, wobei auch die Konfiguration und Integration der GESUNDHEITSSOFTWARE berücksichtigt wird.

5.4.4 VERIFIZIERUNG der IT-SICHERHEIT des detaillierten Entwurfs

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN zur Durchführung von Entwurfsüberprüfungen einrichten, um SCHWÄCHEN zu identifizieren, zu charakterisieren und bis zur Beseitigung zu verfolgen, die mit jeder signifikanten Revision des sicheren Entwurfs verbunden sind, einschließlich, aber nicht beschränkt auf:

- a) IT-SICHERHEITSanforderungen, die vom Entwurf nicht angemessen berücksichtigt wurden;
- b) BEDROHUNGEN und ihre Fähigkeit, SCHWACHSTELLEN in PRODUKTSchnittstellen, VERTRAUENSGRENZEN und RESSOURCEN auszunutzen;
- c) Identifizierung, Dokumentation und Charakterisierung von bewährten Verfahren des detaillierten Entwurfs, die nicht befolgt wurden (5.3.2 und 5.4.1).

ANMERKUNG Die Entwurfsüberprüfungen berücksichtigen auch jeden Softwaredienst, der von der GESUNDHEITSSOFTWARE verwendet wird, um die vorgesehene Funktionalität zu erreichen, zum Beispiel: Cloud, Software-/Infrastruktur-/ Plattform-as-a-Service.

5.5 Implementierung und VERIFIZIERUNG von Software-Einheiten

5.5.1 Sichere Programmierstandards

Der HERSTELLER muss eine oder mehrere ImplementierungsAKTIVITÄTEN unter Einhaltung sicherer Programmierstandards einrichten.

5.5.2 Überprüfung der IT-SICHERHEITSimplementierung

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um sicherzustellen, dass Implementierungsüberprüfungen durchgeführt werden, um alle Probleme in Bezug auf die IT-SICHERHEIT im Zusammenhang mit der Implementierung des sicheren Entwurfs zu identifizieren, zu beschreiben und in den ProblemlösungsPROZESS einfließen zu lassen, einschließlich:

- a) Identifizierung von IT-SICHERHEITSanforderungen (siehe 5.2), die durch die Implementierung nicht angemessen berücksichtigt wurden;

Anmerkung Die Zuordnung von Anforderungen, einschließlich IT-SICHERHEITSanforderungen, ist Teil typischer EntwurfsPROZESSE.

- b) Identifizierung der verwendeten sicheren Programmierstandards und Dokumentation aller Teile der sicheren Programmierstandards, die nicht befolgt wurden (zum Beispiel Verwendung von verbotenen Funktionen oder Nichtanwendung des Prinzips der geringsten Rechte);
- c) Statische Code-Analyse (SCA) für den Quellcode zur Ermittlung von Fehlern bei der sicheren Programmierung unter Verwendung des sicheren Programmierstandards für die unterstützte Programmiersprache, wie in 5.1.3 eingeführt. SCA wird oft durch Werkzeuge unterstützt, kann aber auch durch Code-Inspektionen und Code-Walkthroughs durchgeführt werden.
- d) Überprüfung der Implementierung und ihrer RÜCKVERFOLGBARKEIT auf die definierten SICHERHEITSFUNKTIONEN zur Unterstützung des IT-SICHERHEITSentwurfs (siehe 5.3 und 5.4); und
- e) Untersuchung von BEDROHUNGEN und ihrer Fähigkeit, Implementierungsschnittstellen, VERTRAUENSGRENZEN und RESSOURCEN auszunutzen (siehe 5.3 und 5.4).

5.6 Softwareintegrationsprüfung

Der HERSTELLER darf einen Teil der Prüfung des Softwaresystems als Teil der Softwareintegrationsprüfung durchführen (siehe 5.7).

Als Teil der Integrationsprüfung von GESUNDHEITSSOFTWARE sollte der HERSTELLER Unterschiede in den IT-SICHERHEITSrichtlinien über VERTRAUENSGRENZEN hinweg berücksichtigen.

5.7 Prüfung des Softwaresystems

5.7.1 Prüfung der Anforderungen an die IT-Sicherheit

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um zu verifizieren, dass die GESUNDHEITSSOFTWARE-IT-SICHERHEITSfunktionen die IT-SICHERHEITSanforderungen erfüllen und dass die GESUNDHEITSSOFTWARE Fehlerszenarien und ungültige Eingaben behandelt. Beruhend auf der VORGESEHENEN NUTZUNGsumgebung müssen die Arten der Prüfung einschließen:

- a) Funktionsprüfung von IT-SICHERHEITSanforderungen;
- b) Prüfung von Leistungsfähigkeit und Skalierbarkeit; und
- c) Prüfungen von Grenz-/Randbedingungen, Beanspruchung und fehlgeformten oder unerwarteten Eingaben mit potenziellen Folgen für die IT-SICHERHEIT.
- d) Prüfung jedes Softwaredienstes, der von der GESUNDHEITSSOFTWARE genutzt wird, um die beabsichtigte Funktionalität zu erreichen, im Rahmen von Verantwortungsvereinbarungen zwischen Dienstleistern, HERSTELLERN und Betreibern, zum Beispiel: Cloud-Dienste, Software/Infrastruktur/Platform-as-a-Service.

ANMERKUNG Siehe [Anhang B 7.3](#).

5.7.2 Prüfung der BEDROHUNGSabschwächung

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um die Wirksamkeit der Abschwächung für die im BEDROHUNGsmodell erkannten und bestätigten BEDROHUNGEN zu prüfen. AKTIVITÄTEN müssen einschließen:

- a) Erstellen und Durchführen angemessener Prüfungen für jede Abschwächungsmaßnahme, die zur Behandlung einer bestimmten BEDROHUNG implementiert wurde, um sicherzustellen, dass die Abschwächung wie vorgesehen funktioniert;
- b) Erstellen und Ausführen von Plänen, um zu versuchen, jede Abschwächungsmaßnahme zu vereiteln; und
- c) bringt keine weiteren SCHWACHSTELLEN in den Entwurf ein.

5.7.3 Prüfung auf SCHWACHSTELLEN

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN zur Durchführung von Prüfungen einrichten, die sich auf die Identifizierung und Charakterisierung potenzieller IT-SICHERHEITSSCHWACHSTELLEN in der GESUNDHEITSSOFTWARE konzentrieren. Die Prüfung auf bekannte SCHWACHSTELLEN muss mindestens auf den aktuellen Inhalten einer etablierten, von der Industrie anerkannten, öffentlichen Quelle für bekannte SCHWACHSTELLEN beruhen. Die Prüfungen müssen wie zutreffend umfassen:

- a) Missbrauchsfall für die Prüfung fehlgeformter oder unerwarteter Eingaben, der sich auf die Aufdeckung von Problemen der IT-SICHERHEIT konzentriert. Dies muss manuelle oder automatisierte Prüfungen von Missbrauchsfällen und spezielle Arten von Prüfungen von Missbrauchsfällen an allen externen Schnittstellen und Protokollen umfassen. Beispiele hierfür sind Fuzz-Prüfungen, Prüfungen der Netzwerkverkehrslast und Kapazitätsprüfungen;
- b) Prüfungen der ANGRIFFSFLÄCHE, um alle Ein- und Ausgänge zum und vom System, häufige SCHWACHSTELLEN einschließlich, aber nicht beschränkt auf schwache Zugriffskontrolllisten (ACL), ungeschützte Ports und Dienste, die mit erhöhten Rechten laufen, zu ermitteln;
- c) Black-Box-Scans auf bekannte SCHWACHSTELLEN, die sich auf die Erkennung bekannter SCHWACHSTELLEN in (falls zutreffend) Hardware, Host, Schnittstellen oder SOFTWAREKOMPONENTEN konzentrieren.

ANMERKUNG Zum Beispiel könnte dies ein netzwerkbasierter Scan auf bekannte SCHWACHSTELLEN sein.

- d) ANALYSE DER SOFTWAREZUSAMMENSETZUNG bei allen binären ausführbaren Dateien, einschließlich eingebetteter Firmware, die mit GESUNDHEITSSOFTWARE verwendet werden sollen und von einem Drittanbieter geliefert werden. Diese Analyse kann zur Erkennung verwendet werden von:

- 1) bekannte SCHWACHSTELLEN in den SOFTWAREKOMponenten;
- 2) Verknüpfung mit gefährdeten Bibliotheken;
- 3) Verletzung von IT-SICHERHEITSregeln; und
- 4) Compilereinstellungen, die zu SCHWACHSTELLEN führen können;
- 5) Vergleich der vorgefundenen Software mit der Software-Stückliste.

ANMERKUNG Werkzeuge können die ANALYSE DER SOFTWAREZUSAMMENSETZUNG unterstützen, indem sie eine Liste der enthaltenen Softwarepakete erstellen.

- e) Prüfung der dynamischen Laufzeit-Ressourcenverwaltung, die Fehler aufdeckt, die bei der statischen Codeanalyse nicht sichtbar sind, darunter Denial-of-Service-Bedingungen aufgrund der Nichtfreigabe von Laufzeit-Handles, Speicherlecks und Zugriffe auf gemeinsamen Speicher ohne Authentifizierung. Diese Prüfung muss durchgeführt werden, wenn solche Werkzeuge zur Verfügung stehen.

ANMERKUNG Dynamische Prüfungen zur Laufzeit können ohne Werkzeuge nicht effektiv durchgeführt werden.

5.7.4 Eindringprüfung

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN zur Identifizierung und Charakterisierung von SCHWÄCHEN mittels Prüfungen einrichten, die sich auf das Entdecken und Ausnutzen von IT-SICHERHEITSSCHWACHSTELLEN in der GESUNDHEITSSOFTWARE konzentrieren.

Siehe [Anhang B.5.7.4](#).

5.8 Softwarefreigabe

5.8.1 Beheben von Befunden vor der Freigabe

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um sicherzustellen, dass alle Erkenntnisse aus den Prüfungen des Systems im Rahmen des ProblemlösungsPROZESSES ([Abschnitt 9](#)) behandelt wurden.

5.8.2 Freigabedokumentation

Als Teil der AKTIVITÄT(EN) zur Softwarefreigabe muss der HERSTELLER Anforderungen an die BEGLEITDOKUMENTATION festlegen:

- a) Richtlinien für den sicheren Betrieb;
- b) Dokumentation der PROZESSstrenge und der Konformität, einschließlich der Prozesseingrenzung ([Abschnitt 4](#)), des Zuschneidens ([Abschnitt 5](#)) und der Informationen zum Umfang der Dokumentation ([Anhang E](#));

ANMERKUNG Diese Dokumente helfen bei der Erfüllung etwaiger gesetzlicher oder vertraglicher Verpflichtungen.

- c) Richtlinien zur Kontenverwaltung (falls zutreffend); und
- d) geeignete Informationen über relevante RESTRIKTIKEN für die IT-SICHERHEIT, die in der GESUNDHEITSSOFTWARE verbleiben.

Siehe [Anhang E](#) für eine informative Spezifikation des Inhalts der Dokumentation.

5.8.3 DateiINTEGRITÄT

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um einen Mechanismus zur VERIFIZIERUNG der INTEGRITÄT aller Skripte, ausführbaren Dateien und anderer für die IT-SICHERHEIT relevanten Dateien bereitzustellen, die mit einer GESUNDHEITSSOFTWARE verwendet werden.

Diese AKTIVITÄT(EN) ist (sind) erforderlich, um sicherzustellen, dass PRODUKTbenutzer verifizieren können, dass ausführbare Dateien, Skripte und andere wichtige Dateien, die sie vom HERSTELLER erhalten haben, nicht verändert wurden. Übliche Verfahren zur Erfüllung dieser Anforderung sind kryptografische Hashes und digitale Signaturen (die auch einen Herkunftsnachweis bereitstellen).

5.8.4 Maßnahmen für private Schlüssel

Der HERSTELLER muss Verfahrens- und technische Maßnahmen einsetzen, um die für die Codesignierung verwendeten privaten Schlüssel vor unberechtigtem Zugriff und vor Veränderung zu schützen.

ANMERKUNG Dies bezieht sich auf die Softwarelieferkette, und der Schwerpunkt liegt auf der Codesignierung zur Unterstützung der sicheren Verteilung und Auslieferung von GESUNDHEITSSOFTWARE.

5.8.5 Bewertung und Behandlung von auf die IT-SICHERHEIT bezogenen Problemen

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um zu verifizieren, dass die GESUNDHEITSSOFTWARE oder ein Update nicht freigegeben werden, bis ihre die IT-SICHERHEIT betreffenden Probleme behandelt und bis zur Beseitigung verfolgt wurden (siehe 9.5). Dies umfasst Probleme im Zusammenhang mit:

- a) Anforderungen (siehe 5.2);
- b) IT-SICHERHEIT durch Entwurf (siehe 5.3 und 5.4);
- c) Implementierung (siehe 5.5);
- d) VERIFIZIERUNG / VALIDIERUNG (siehe 5.5); und
- e) Verwaltung von IT-SICHERHEITSdefekten(siehe 9.4).

5.8.6 Abschluss der AKTIVITÄTEN

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um zu verifizieren, dass vor der Freigabe von GESUNDHEITSSOFTWARE alle anwendbaren, auf die IT-SICHERHEIT bezogenen PROZESSE, die von dieser Norm gefordert werden, abgeschlossen wurden, wobei Aufzeichnungen den Abschluss jeder AKTIVITÄT bzw. jedes PROZESSES dokumentieren.

5.8.7 Richtlinien für die SICHERE Außerbetriebnahme für GESUNDHEITSSOFTWARE

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN zur Erstellung einer PRODUKTbenutzerdokumentation einrichten, die Richtlinien für die Außerbetriebnahme der GESUNDHEITSSOFTWARE enthält.

6 SOFTWAREWARTUNGSPROZESS

6.1 Festlegung eines Plans für die SOFTWAREWARTUNG

6.1.1 Zeitnahe Auslieferung von IT-SICHERHEITS-Updates

Der HERSTELLER muss - als Teil der Update-AKTIVITÄTEN - eine Richtlinie festlegen, die die Zeitrahmen für die Auslieferung und Qualifizierung (siehe 6.1.1) von IT-SICHERHEITS-Updates an PRODUKTANWENDER festlegt. Diese Richtlinie muss mindestens die folgenden Faktoren berücksichtigen:

- a) die potenziellen Auswirkungen (technisch, für SICHERHEIT, Effektivität, IT-SICHERHEIT) der SCHWACHSTELLE;
- b) öffentliche Kenntnis der SCHWACHSTELLE;
- c) ob veröffentlichte EXPLOITS für die SCHWACHSTELLE existieren;
- d) die Menge der bereitgestellten PRODUKTE, die betroffen sind; und
- e) die Verfügbarkeit einer wirksamen externen Kontrolle, wenn kein Update der GESUNDHEITSSOFTWARE bereitgestellt wird.

ANMERKUNG 1 Einige Aufsichtsbehörden können spezifische Zeitrahmenanforderungen haben.

ANMERKUNG 2 Der HERSTELLER darf IT-SICHERHEITS-Updates kategorisieren (zum Beispiel nach möglichen Auswirkungen) und entsprechende Zeitrahmen festlegen. Siehe IEC 60601-4-5.

ANMERKUNG 3 Während eines akzeptablen Zeitintervalls, in dem der HERSTELLER eine technische Maßnahme entwickelt, können alle dokumentierten Abschwächungsmaßnahmen und Beschränkungen der ZWECKBESTIMMUNG auf dem RISIKOMANAGEMENT beruhen. Es ist ratsam, eine technische Abschwächung in GESUNDHEITSSOFTWARE zu entwickeln und bereitzustellen.

ANMERKUNG 4 IEC TR 60601-4-5 legt eine Mindestleistungsfähigkeit (Begriff der „wesentlichen Funktion“, (en: essential function), wie er in der Normenreihe IEC 62443 verwendet wird) fest, die bei Medizinprodukten im Falle relevanter IT-SICHERHEITS-ANGRIFFE auf das HDO-IT-Netzwerk vorhanden sein muss. Eine solche Mindestleistungsfähigkeit wird benötigt, um die Grundfunktionalität sicherzustellen, bis ein verifiziertes IT-SICHERHEITS-Update verfügbar ist, in Situationen, in denen alle Medizinprodukte desselben Typs in der Gesundheitsversorgungsorganisation (HDO) gleichzeitig von einem bestimmten IT-SICHERHEITS-ANGRIFF betroffen sein können. Daher sollten die Software-LEBENSZYKLUSAKTIVITÄTEN bei Medizinprodukten sicherstellen, dass:

- a) „wesentliche Funktionen“ für das Intervall sicher bleiben, bis ein IT-SICHERHEITS-Update installiert ist und
- b) IT-SICHERHEITS-Updates immer die SICHERHEITSFUNKTION, wie in der BEGLEITDOKUMENTATION festgelegt, neu einrichten sollten.

Zusätzliche Hinweise gibt IEC TR 60601-4-5.

6.2 Analyse von Problemen und Änderungen

6.2.1 Überwachung öffentlicher Vorfallsberichte

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um relevante Informationsquellen zu SCHWACHSTELLEN bezüglich UNTERSTÜTZTER SOFTWARE zu sammeln und zu überprüfen.

ANMERKUNG Dies schließt GESUNDHEITSSOFTWARE ein.

6.2.2 VERIFIZIERUNG von IT-SICHERHEITS-Updates

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um zu verifizieren, dass IT-SICHERHEITS-Updates des HERSTELLERS die vorgesehenen IT-SICHERHEITSSCHWACHSTELLEN behandeln.

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um zu verifizieren, dass IT-SICHERHEITS-Updates keine unbeabsichtigten Auswirkungen auf die Funktions- oder Qualitätseigenschaften der GESUNDHEITSSOFTWARE haben. Solche IT-SICHERHEITS-Updates umfassen unter anderem Updates, die erstellt wurden von:

- a) dem HERSTELLER der GESUNDHEITSSOFTWARE,
- b) Lieferanten von SOFTWAREKOMPONENTEN, die in der GESUNDHEITSSOFTWARE verwendet werden und
- c) Lieferanten von SOFTWAREKOMPONENTEN oder Plattformen, von denen die GESUNDHEITSSOFTWARE abhängt.

Der HERSTELLER darf festlegen, dass für bestimmte SOFTWAREKOMPONENTEN oder Plattformen eine gemeinsame Verantwortung für diese VERIFIZIERUNG besteht.

ANMERKUNG Siehe auch [Abschnitt 9](#), „ProblemlösungsPROZESS“.

6.3 Implementierung von Änderungen

6.3.1 Dokumentation von IT-SICHERHEITS-Updates für UNTERSTÜTZTE SOFTWARE

Der HERSTELLER muss eine Richtlinie zur Information von PRODUKTANWENDERN über Updates für UNTERSTÜTZTE SOFTWARE festlegen. Diese Informationen müssen umfassen:

- a) die Angabe, ob die GESUNDHEITSSOFTWARE mit dem IT-SICHERHEITS-Update für die UNTERSTÜTZTE SOFTWARE kompatibel ist; und
- b) bei IT-SICHERHEITS-Updates, die vom HERSTELLER der GESUNDHEITSSOFTWARE nicht zugelassen sind, die Abschwächungsmaßnahmen, die anstelle der Anwendung des Updates verwendet werden können.

6.3.2 Auslieferung von IT-SICHERHEITS-Updates für GEWARTETE SOFTWARE

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um sicherzustellen, dass IT-SICHERHEITS-Updates für die PRODUKTANWENDER von GEWARTETER SOFTWARE zur Verfügung gestellt werden.

Siehe [Anhang E.2.4](#).

6.3.3 INTEGRITÄT von IT-SICHERHEITS-Updates für GEWARTETE SOFTWARE

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um sicherzustellen, dass jedes anwendbare Update für GEWARTETE SOFTWARE den PRODUKTANWENDERN in einer Weise zur Verfügung gestellt wird, die eine VERIFIZIERUNG der INTEGRITÄT des IT-SICHERHEITS-Updates ermöglicht.

Diese AKTIVITÄT(EN) ist (sind) erforderlich, um sicherzustellen, dass Benutzer von GESUNDHEITSSOFTWARE anwendbare IT-SICHERHEITS-Patches für die GEWARTETE SOFTWARE rechtzeitig erhalten können und um die Möglichkeit zu verringern, dass die IT-SICHERHEITS-Patches betrügerisch sind. Mit dieser/diesen AKTIVITÄT(EN) stellt der HERSTELLER einen Mechanismus oder eine Technik zur Verfügung, die es Anwendern von GESUNDHEITSSOFTWARE ermöglicht, die Authentizität von Patches zu verifizieren. Die gleichzeitige Freigabe von Patches für die gesamte GEWARTETE SOFTWARE kann das Zeitfenster zwischen dem Bekanntwerden der SCHWACHSTELLE und der Verfügbarkeit von Patches verringern.

7 IT-SICHERHEITS-RISIKOMANAGEMENT

7.1 RISIKOMANAGEMENT-Kontext

Der HERSTELLER muss einen PROZESS für das Management von IT-SICHERHEITSrisiken im Zusammenhang mit GESUNDHEITSSOFTWARE als Teil seines Ansatzes für das RISIKOMANAGEMENT von PRODUKTEN einrichten und aufrechterhalten. Dieser PROZESS sollte aus den folgenden PROZESSschritten bestehen, die in [Abschnitt 7](#) weiter unten beschrieben werden.

Siehe [Anhang C](#).

7.1.1 SICHERHEITSUMFELD des PRODUKTS

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, die sicherstellen, dass das vorgesehene SICHERHEITSUMFELD des PRODUKTS dokumentiert ist. Diese AKTIVITÄT(EN) ist (sind) erforderlich, um sicherzustellen, dass die Mindestanforderungen der Umgebung und die Annahmen über diese Umgebung dokumentiert sind, um die IT-SICHERHEITSstufe zu erreichen, für die das PRODUKT entworfen wurde.

Der Zweck der Definition dieser Informationen ist, dass sowohl die Entwickler der GESUNDHEITSSOFTWARE als auch die Benutzer des PRODUKTS das gleiche Verständnis darüber haben, wie das PRODUKT verwendet werden soll. Dies hilft den Entwicklern, geeignete Entwurfsentscheidungen zu treffen, und den Anwendern, das PRODUKT so zu nutzen, wie es vorgesehen war.

Das SICHERHEITSUMFELD könnte einschließen:

- a) Standort im Netzwerk;
- b) physische oder IT-SICHERHEIT durch die Umgebung, in der das PRODUKT bereitgestellt wird;
- c) Trennung (aus einer Netzwerkperspektive);
- d) falls bekannt, mögliche Auswirkungen auf die SICHERHEIT durch Beeinträchtigung der IT-SICHERHEIT;
- e) IT-SICHERHEITSmaßnahmen, die in spezieller Hardware implementiert sind, mit der die GESUNDHEITSSOFTWARE verwendet werden soll.

Es ist zum Beispiel wichtig zu dokumentieren, ob physische IT-SICHERHEIT erforderlich ist. Wenn keine physische IT-SICHERHEIT erwartet wird, kann dies eine Reihe von Anforderungen mit sich bringen, wie die Nichtzulassung der Konfiguration auf Knopfdruck am PRODUKT. Ein anderes Beispiel ist, dass das PRODUKT, wenn zu erwarten ist, dass es durch eine vom Anwender bereitgestellte Firewall geschützt wird, üblicherweise keine eigene Firewall benötigt.

Die Dokumentation dieser externen IT-SICHERHEITseigenschaften für das PRODUKT (sein SICHERHEITSUMFELD) ermöglicht es den Entwicklern, eine DEFENSE-IN-DEPTH-Strategie zu entwerfen, die dieses SICHERHEITSUMFELD ergänzt, und den Prüfern, die IT-SICHERHEIT eines PRODUKTS in einer Umgebung zu validieren und zu verifizieren, die derjenigen ähnelt, in der es bereitgestellt werden soll.

Dieser PROZESS bedeutet, dass die Bereitstellungsumgebung, in der das PRODUKT verwendet werden soll, in allen an der Entwicklung und Prüfung dieses PRODUKTS beteiligten PROZESSEN korrekt abgebildet und dokumentiert wird.

7.2 Identifizierung von SCHWACHSTELLEN, BEDROHUNGEN und damit verbundenen negativen Auswirkungen

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN zur Identifizierung und Dokumentierung jeglicher SCHWACHSTELLEN, BEDROHUNGEN und damit zusammenhängender negativer Auswirkungen einrichten, die die

VERTRAULICHKEIT, INTEGRITÄT, VERFÜGBARKEIT von RESSOURCEN der GESUNDHEITSSOFTWARE beeinflussen. Diese AKTIVITÄT(EN) muss/müssen die ZWECKBESTIMMUNG und die VORGESEHENE NUTZUNGsumgebung im Hinblick auf das SICHERHEITsumfeld berücksichtigen.

Diese AKTIVITÄT(EN) muss/müssen sicherstellen, dass alle PRODUKTE über ein BEDROHUNGSMODELL verfügen, das für den aktuellen Entwicklungsbereich des PRODUKTS spezifisch ist und die folgenden Merkmale aufweist (falls zutreffend):

- a) korrekter Fluss klassifizierter Informationen durch das gesamte System;
- b) VERTRAUENSGRENZEN;
- c) PROZESSE;
- d) Datenspeicher;
- e) Wechselwirkung mit externen Einheiten;
- f) Implementierung interner und externer Kommunikationsprotokolle in dem PRODUKT;
- g) von außen zugängliche physische Anschlüsse, einschließlich Debuganschlüsse;
- h) Leiterplattenanschlüsse wie JTAG-Verbindungen oder Debug-Header, die zum ANGRIFF auf die Hardware genutzt werden könnten;
- i) potentielle ANGRIFFSvektoren, einschließlich ANGRIFFEN auf die (vorgesehene) Hardware;
- j) mögliche BEDROHUNGEN;
- k) identifizierte Probleme bezüglich der IT-SICHERHEIT; und
- l) externe Abhängigkeiten in Form von Treibern oder Drittanbieter-Anwendungen (nicht vom Lieferanten entwickelter Code), die in die Anwendung eingebunden sind.

Das BEDROHUNGSMODELL muss vom Entwicklungsteam überprüft und verifiziert werden, um sicherzustellen, dass es korrekt ist und verstanden wird.

Das BEDROHUNGSMODELL muss regelmäßig (mindestens einmal jährlich) für freigegebene PRODUKTE überprüft und erforderlichenfalls als Reaktion auf das Auftreten neuer BEDROHUNGEN für das PRODUKT aktualisiert werden, auch wenn sich der Entwurf nicht ändert.

Alle im BEDROHUNGSMODELL identifizierten Probleme müssen wie in 9.4 und 9.5 definiert behandelt werden.

7.3 Einschätzung und Bewertung des IT-Sicherheitsrisikos

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, um:

- a) das Risiko der oben identifizierten SCHWACHSTELLEN einzuschätzen. Die Risikoeinschätzung geschieht, indem die negativen Auswirkungen dieser SCHWACHSTELLE auf die IT-SICHERHEIT erwogen werden. Diese Einschätzung kann durch die Verwendung von SCHWACHSTELLENbewertung wie dem *Common Vulnerability Scoring System* (CVSS) oder *MITRE Scoring Rubric for Medical Devices* unterstützt werden. Das Bewertungssystem darf auch auf einem Wahrscheinlichkeits-/Schweregrad-Schema beruhen, das der HERSTELLER für andere Risiken verwendet (siehe z. B. IEC/ISO Guide 51 oder ISO 14971).
- b) die geschätzten Risiken zu bewerten und - beruhend auf der Bewertung - zu bestimmen, ob das Risiko akzeptabel ist oder nicht;
- c) den RISIKOMANAGEMENTPROZESS des PRODUKTS über alle Aktualisierungen des BEDROHUNGSMODELLS informieren.

7.4 IT-Sicherheitsrisikobeherrschung

Der HERSTELLER muss bestimmen, ob die Maßnahmen zur BEHERRSCHUNG DES IT-SICHERHEITSRISIKOS geeignet sind, die IT-Sicherheitsrisiken auf der Grundlage der Richtlinien zur Akzeptanz von IT-Sicherheitsrisiken auf ein akzeptables Niveau zu verringern. Wenn MAßNAHMEN ZUR RISIKOBEHERRSCHUNG als angemessen erachtet werden, muss der HERSTELLER:

- geeignete Abschwächungsmaßnahmen wählen;
- bestimmen, ob diese Abschwächungsmaßnahmen zu neuen Risiken führen oder andere Risiken erhöhen;
- gewählte Abschwächungsmaßnahmen implementieren; und
- die Wirksamkeit der implementierten Maßnahmen prüfen.

Der HERSTELLER muss die Ergebnisse dieser AKTIVITÄTEN dokumentieren.

Die Behandlung von RESTRIKEN für die IT-SICHERHEIT muss in Zusammenarbeit mit dem PRODUKTRISIKOMANAGEMENT erfolgen.

ANMERKUNG Die Bewertung von IT-Sicherheitsrisiken wird durch das SICHERHEITSUMFELD beeinflusst. Die Akzeptanz von IT-Sicherheitsrisiken beruht auf der jeweiligen Wertung und der Akzeptanzschwelle für IT-Sicherheitsrisiken. Siehe auch 4.2.

7.5 Überwachung der Wirksamkeit von MAßNAHMEN ZUR RISIKOBEHERRSCHUNG

Der HERSTELLER muss die Wirksamkeit der MAßNAHMEN ZUR RISIKOBEHERRSCHUNG durch Sammeln und Überprüfen von Informationen in der Phase nach der Markteinführung überwachen.

Diese AKTIVITÄT(EN) muss/müssen auch andere AKTIVITÄTEN und PROZESSE über das Problem oder damit zusammenhängende Probleme informieren, einschließlich PROZESSEN für andere PRODUKTE/Revisionen; und Dritte (z. B. Lieferanten) informieren, wenn Probleme im Quellcode von Drittanbietern gefunden wurden, der mit der GESUNDHEITSSOFTWARE verwendet werden soll.

Alle im BEDROHUNGSMODELL freigegebener GESUNDHEITSSOFTWARE identifizierten Probleme werden wie in 9.4 und 9.5 definiert behandelt.

8 Software-KONFIGURATIONSMANAGEMENTPROZESS

Der HERSTELLER muss einen allgemeinen PRODUKTENTWICKLUNGS-/wartungs-/unterstützungsPROZESS einrichten, der ein KONFIGURATIONSMANAGEMENT mit Änderungskontrolle und Änderungshistorie umfasst.

Für IT-Sicherheitsverpflichtungen bei bereits freigegebener oder auf dem Markt befindlicher GESUNDHEITSSOFTWARE muss das KONFIGURATIONSMANAGEMENT die Fähigkeit besitzen, eine Liste der enthaltenen externen Komponenten zu reproduzieren, die anfällig für SCHWACHSTELLEN sind oder werden könnten.

9 ProblemlösungsPROZESS für Software

9.1 Überblick

Die in diesem Abschnitt festgelegten AKTIVITÄTEN dienen dem Umgang mit auf die IT-SICHERHEIT bezogenen Problemen von GESUNDHEITSSOFTWARE.

9.2 Empfang von Benachrichtigungen über SCHWACHSTELLEN

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, die es ermöglichen, Informationen über SCHWACHSTELLEN an den HERSTELLER zu melden - unabhängig davon, ob sie von einer internen Stelle, einer externen Stelle oder über ein System zur Bearbeitung von Beschwerden kommen.

Diese EmpfangsAKTIVITÄT(EN) muss/müssen Berichte über Probleme bezüglich der IT-SICHERHEIT in der GESUNDHEITSSOFTWARE von mindestens den folgenden Quellen empfangen und bis zum Abschluss verfolgen:

- a) Prüfer für VERIFIZIERUNG und VALIDIERUNG der IT-SICHERHEIT;
- b) Lieferanten von Komponenten von Drittanbietern, die in dem PRODUKT verwendet werden;
- c) PRODUKTentwickler und -prüfer;
- d) PRODUKTanwender einschließlich Einrichtern, Bedienern, Administratoren und Wartungspersonal;
- e) Daten, die aus Audit-Ereignisprotokollinformationen kommen;
- f) IT-SICHERHEITSforscher (Melder von IT-SICHERHEITSSCHWACHSTELLEN), siehe auch ISO/IEC 29147;
- g) Daten oder Benachrichtigungen über weitverbreitete SCHWACHSTELLEN, die die GESUNDHEITSSOFTWARE beeinflussen können - siehe 6.2.

ANMERKUNG 1 Üblicherweise stammen solche Informationen aus Veröffentlichungen, Berichten, unabhängiger IT-SICHERHEITSforschung, internen Untersuchungen, CERTs und Information Sharing and Analysis Organizations (ISAO).

9.3 Überprüfen von SCHWACHSTELLEN

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN einrichten, die die rechtzeitige Untersuchung von SCHWACHSTELLEN ermöglicht, um folgendes zu bestimmen:

- e) ihre Gültigkeit für das PRODUKT;
- f) ihre Verifizierbarkeit; und
- g) verwandte BEDROHUNGEN.

ANMERKUNG 1 Die Rechtzeitigkeit wird von den Behörden, der geltenden Gesetzgebung, der Regulierungspolitik und den Marktkräften bestimmt.

ANMERKUNG 2 Dieser PROZESS darf zum Beispiel als Teil der PROZESSE nach ISO 13485:2016, 8.2.1, Rückmeldungen, 8.2.2, Reklamationsbearbeitung und 8.2.3, Meldung an Regulierungsbehörden, implementiert werden.

9.4 Analyse von SCHWACHSTELLEN

Der HERSTELLER muss eine oder mehrere AKTIVITÄTEN zur Analyse von SCHWACHSTELLEN im PRODUKT einrichten, die einschließen:

- a) die Bewertung ihrer Auswirkungen in Bezug auf:
 - 1) das technische SICHERHEITSUMFELD, in dem sie entdeckt wurden; (siehe IEC 62443-4-1, Abschnitt 6, Ansatz 2 – Spezifikation der IT-SICHERHEITSanforderungen);
 - 2) die VORGESEHENE NUTZUNGsumgebung des PRODUKTS; und
 - 3) die DEFENSE-IN-DEPTH-Strategie des PRODUKTS;
- b) die Auswirkung, wie durch ein SCHWACHSTELLENbewertungssystem (zum Beispiel CVSS) definiert;
- c) die Identifizierung aller anderen PRODUKTE / PRODUKTversionen, die das Problem in Bezug auf die IT-SICHERHEIT enthalten (falls vorhanden);
- d) die Identifizierung der Ursache des Problems;