Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: HERSTELLER

Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte[1]

1 Einleitung

Viele Medizinprodukte folgen dem Trend zur Digitalisierung und besitzen die Möglichkeit zur Vernetzung. Hierbei werden häufig Technologien eingesetzt, die sich in anderen Bereichen bereits bewährt haben. Die daraus resultierenden Herausforderungen an die Cyber-Sicherheit unter Berücksichtigung besonderer Rahmenbedingungen – wie beispielsweise der langen Lebensdauer dieser Produkte oder deren Einsatz in unmittelbar patientensicherheitskritischen Bereichen – müssen von den Herstellern besonders berücksichtigt werden. Daher wurden in diesem Dokument zentrale Best Practices für Hersteller von netzwerkfähigen Medizinprodukten zusammengestellt. Die Empfehlungen sollen flankierend zu den regulatorischen Vorgaben bei Implementierung und Aufrechterhaltung eines angemessenen Cyber-Sicherheitsniveaus nach dem Stand der Technik unterstützen.

Im Hinblick auf die Erfüllung der grundlegenden Anforderungen der aktuell gültigen Richtlinien zu Medizinprodukten[2] müssen Hersteller im Rahmen des Konformitätsbewertungsverfahrens u.a. eine Risikoanalyse erstellen und die dort identifizierten Risiken, zu denen auch Cyber-Sicherheitsaspekte zählen, minimieren und dokumentieren. Die vorliegende Cyber-Sicherheitsempfehlung gibt eine praxisnahe Hilfestellung, wie dies im Einzelnen technisch umgesetzt werden kann.

Da unter den Oberbegriff Medizinprodukte eine Vielzahl unterschiedlicher Geräte fallen, ist das Dokument sehr generisch aufgebaut. Statt konkreter Handlungsanweisungen, die möglicherweise nicht auf alle Produkte gleichermaßen übertragen werden können, werden in den folgenden Kapiteln zu jedem Bereich, der Einfluss auf ein Gerät hat, cyber-sicherheitsrelevante Fragen gestellt. Die Fragen sollen es dem Hersteller ermöglichen, die für sein Produkt notwendigen Handlungsanweisungen zu generieren.

Im vorliegenden Dokument wird zwischen folgenden Betriebsarten unterschieden

A) Medizinischer Betrieb nach Zweckbestimmung

   In dieser Betriebsart wird das Produkt für den vorgesehenen medizinischen Zweck eingesetzt.

B) Konfiguration des Produktes

   In dieser Betriebsart wird das Gerät für den medizinischen Zweck konfiguriert.

1 Das Dokument wurde von den Cyber-Sicherheitsempfehlungen „Anforderung an netzwerkfähige Industrieprodukte“ https://www.allianz-fuer-cybersicherheit.de/dok/6603528 abgeleitet und enthält viele der bereits darin beschriebenen Empfehlungen. Es wurde in enger Zusammenarbeit mit dem ZVEI-Fachverband Elektromedizinische Technik und dem Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) erstellt.

2 Richtlinie 93/42/EWG

Dies umfasst sowohl Cyber-Sicherheitskonfigurationen, die einen sicheren Betrieb ermöglichen als auch für den medizinischen Betrieb notwendige Einstellungen (Beispielsweise auf den Patienten abgestimmte Parameter).

C) Technischer Servicebetrieb

In dieser Betriebsart werden Updates vom Hersteller oder Drittanbietern eingespielt sowie notwendige grundlegende Kalibrierungen oder Eichungen vorgenommen.

Aus Cyber-Sicherheitssicht sind die Betriebsarten nicht voneinander trennbar, da beispielsweise bei einem softwareunterstützten Gerät ein im technischen Servicebetrieb aufgespieltes Schadprogramm Auswirkungen auf den medizinischen Betrieb nach Zweckbestimmung haben kann, auch wenn die Vernetzung in dieser Betriebsart nicht besteht. Daher gelten immer alle Empfehlungen für alle Betriebsarten. Die Trennung nach den Betriebsarten erfolgt lediglich, damit der Hersteller den Zweck der Empfehlungen leichter zuordnen kann.

Grundsätzlich sind aus IT-Sicherheitssicht alle nach Stand der Technik möglichen Vorkehrungen zur Absicherung des Gerätes durch den Hersteller zu treffen. Nicht immer wird es jedoch möglich sein, alle in den folgenden Kapiteln aufgelisteten Empfehlungen in Maßnahmen umzusetzen, beispielsweise wenn eine Cyber-Sicherheitsmaßnahme einen negativen Einfluss auf die Patientensicherheit hätte. In diesem Fall ist die Entscheidung zu begründen und nach ausführlicher Risikoanalyse eine alternative Lösung zu schaffen, die vor den existierenden Gefährdungen schützt. Beim Ableiten von Maßnahmen muss darauf geachtet werden, dass die Sicherheitsmaßnahmen keinen störenden Einfluss auf die Safety-Funktionen der medizinischen Geräte und damit auf das Leben der Patienten nehmen dürfen.

2 Organisatorische Maßnahmen

2.1 Product Lifecycle

Eine grundlegende Verbesserung der Sicherheit eines Produktes wird durch das Etablieren eines sicheren Entwicklungszyklus (Secure Software Development Lifecycle) erzielt. Bezogen auf die Cyber-Sicherheit sind bei der Umsetzung unter anderem folgende Fragen zu stellen:

- Gibt es einheitliche und verbindliche, dem aktuellen Stand der Technik entsprechende Vorgaben zur sicheren Implementierung (Development Policies)? Dies können beispielsweise sein:
  - Maßnahmen zur Auswahl und Einrichtung vertrauenswürdiger Werkzeuge,
  - Maßnahmen der Trennung von Software Units und
  - Maßnahmen zum Einsatz von sicheren Programmiertechniken und -werkzeugen.
- Werden Cyber-Sicherheitsanalysen zu Bedrohungen und Risiken bzgl. Systemgrenzen, Zweckbestimmung und der vorgesehenen Betriebsumgebung durchgeführt und Gegenmaßnahmen festgelegt und umgesetzt?
- Werden verbindliche Prüfabschnitte (Security Gates) vorgeschrieben, in denen beispielsweise ein Review der Software oder eine ganzheitliche Cyber-Sicherheitsbetrachtung erfolgen?
- Sind bei Softwarekomponenten– sofern technisch möglich – automatisierte Codeanalysen fester Bestandteil des Entwicklungszyklus?
- Wird bei Softwarekomponenten während des Entwicklungsprozesses gezielt nach bekannten Schwachstellen wie buffer overflows und unhandled exceptions gesucht? Werden flankierende Maßnahmen eingebaut, die verhindern, dass innerhalb von Speicherbereichen, die nicht dafür vorgesehen sind, Code ausgeführt wird?

- Werden Produkte einer technischen Sicherheitsanalyse (Penetrationstests) unterzogen? Wird hierbei auch nach nicht bekannten Schwachstellen gesucht? Wird beispielsweise auf bisher unbekannte Verwundbarkeiten (z. B. durch Fuzzing-Tests) oder alternative Zugriffsmöglichkeiten (beispielsweise durch Auslesen von versteckten Dateien, Konfigurationen, Datenströmen oder Hardwareregistern) geprüft?
- Werden Produkte abschließend bereinigt, sodass kein Test-Code oder undokumentierte Zugänge mehr enthalten sind?
- Sind Prozesse für den Umgang mit Schwachstellen in verwendeten Betriebssystemen, Drittkomponenten oder Eigenentwicklungen etabliert? Dazu gehören,
  - die Bewertung einer Schwachstelle einschließlich ihrer Auswirkung auf eigene Produkte (ggf. in verschiedenen Versionsständen)
  - die Festlegung von Gegenmaßnahmen
  - die Behebung der Schwachstelle.
- Sind flankierende Cyber-Sicherheitsmechanismen, beispielsweise Application Whitelisting oder Antivirenlösungen zum Schutz vor Schadsoftware, von Beginn der Konzeptionsphase an mitberücksichtigt (beispielsweise durch Einbinden in eine Zertifizierung) statt deren Einsatz z. B. durch einen Ausschluss der Gewährleistung zu untersagen?
- Gibt es einheitliche Regelungen zum Umgang mit Schwachstellen nach der Auslieferung des Produktes? Sind angemessene Reaktionszeiten und Notfallprozeduren definiert (vgl. BSI-Empfehlung „Handhabung von Schwachstellen“[3])?
- Werden Produkte über einen hinreichend langen Zeitraum möglichst zeitnah mit Patches und Updates bzw. Workarounds versorgt, um entdeckte Schwachstellen zu beheben oder zumindest zu deren Wirkung abzuschwächen? Ist der Update-Prozess für die Kunden möglichst einfach und effizient durchzuführen?
- Werden Updates, Patches und Workarounds vor der Bereitstellung getestet und ist für den Anwender garantiert, dass die Zweckbestimmung der Geräte dadurch erhalten bleibt?
- Wie werden Updates, Patches oder für den Betrieb des Produktes benötigte Software ausgeliefert? Ist die Auslieferungskette für Updates, Patches oder für eventuell für den Betrieb benötigte Software ausreichend gesichert (bsp. Sicherstellen der Authentizität und Integrität über Signaturen)? Wurde das Downloadportal einer Cyber-Sicherheitsüberprüfung (Webcheck[4]) unterzogen, die Schwachstellen identifiziert, über die Inhalte verändert oder manipuliert werden könnten?
- Gibt es Prozesse, die regeln, welche Logdaten erhoben und wie diese ausgewertet werden? Werden Vorgaben gemacht, bei welchen Einträgen eine Reaktion erfolgen muss?

Konkrete Hilfestellungen, welche Anforderungen im Rahmen eines sicheren Entwicklungsprozesses berücksichtigt werden sollten, finden sich u. a. im NIST Special Publication 800-160[5] in IEC 62443-4-1[6].

2.2 Kommunikation

Schwachstellen in IT-Produkten werden nahezu täglich bekannt. Es ist Aufgabe des Herstellers, deren eventuelle Auswirkungen auf seine Produkte angemessen zu kommunizieren. Das Bereitstellen eines Patches sowie auch andere, kompensierende Maßnahmen (beispielsweise Ab-

3 https://www.allianz-fuer-cybersicherheit.de/dok/6603524
4 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Dienstleistungen/ISPentest_ISWebcheck/ispentest_iswebcheck_node.html#doc6600926bodyText6
5 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
6 http://webstore.iec.ch/

schalten eines Dienstes) tragen zum Schutz des Produktes bei. Hersteller von Medizinprodukten sind verpflichtet[7], die gebotenen korrektiven Maßnahmen durchzuführen und diese gegenüber ihren Anwendern mittels einer Maßnahmenempfehlung nachvollziehbar und effektiv mitzuteilen. Sie haben die ordnungsgemäße Durchführung der Maßnahmen sicherzustellen und deren Wirksamkeit zu überwachen.

Für die praktische Umsetzung sind unter anderem die folgenden Fragestellungen zu betrachten.

- Erfolgt - gerade mit Blick auf die Cyber-Sicherheit der Produkte - eine möglichst offene Kommunikation? Ist diese bereits implementiert?
- Gibt es definierte Prozesse für die Kommunikation mit Drittanbietern bei Schwachstellen in deren Produkten?
- Gibt es Ansprechpartner oder Kontaktmöglichkeiten für Cyber-Sicherheitsfragen / -vorfälle (coordinated disclosure)?
- Betrachten die Prozesse zur Erkennung, Meldung und Bewertung/Behandlung von potentiellen Vorkommnissen im Bereich der Sicherheit (Gefährdungsfreiheit, Safety) von Patienten, Anwendern und Dritten auch potentielle Vorkommnisse im Bereich Cyber-Sicherheit? Sind hier firmenintern sowie in der Zusammenarbeit mit den Kunden entsprechende Kriterien und Meldewege etabliert?
- Betrachten die gemäß MPSV[8] etablierten Prozesse zur Erkennung, Meldung und Bewertung/Behandlung von tatsächlichen Vorkommnissen gegenüber der für die jeweiligen Medizinprodukte zuständigen Bundesoberbehörde (hier im Regelfall das BfArM) im Bereich der Sicherheit von Patienten, Anwendern und Dritten auch Vorkommnisse im Bereich Cyber-Sicherheit? Sind auch hier firmenintern sowie in der Zusammenarbeit mit den Kunden entsprechende Kriterien und Meldewege etabliert?
- Gibt es (z.B. im Rahmen des Qualitätssicherungssystems) ein konsolidiertes Tracking-System, das Informationen aus den unterschiedlichen Kommunikationskanälen, wie Hotline, Support, Foren, etc. zusammenführt, die evtl. auf gem. MPSV meldepflichtige Ereignisse, Schwachstellen oder sonstige Vorfälle mit Bezug zur Cyber-Sicherheit von Medizinprodukten hinweisen könnten (z. B. Meldungen, wie „Auf meinem System wurde eine .dll-Datei ausgetauscht“)?
- Werden Kunden darüber informiert, welche Patches mit welcher Kritikalität zu bewerten sind?

3 Produkteigenschaften

Ein sicherer Betrieb von Medizinprodukten kann nur gewährleistet sein, wenn die Produkte gemäß Zweckbestimmung Sicherheitseigenschaften besitzen oder die Absicherung vom Betreiber gewährleistet werden kann. Im Folgenden werden Cyber-Sicherheitsanforderungen an die Produkteigenschaften netzwerkfähiger Medizinprodukte beschrieben. Für eine strukturierte Vorgehensweise können die Cyber-Sicherheitseigenschaften nach verschiedenen Kriterien sortiert werden. Zum einen gibt es spezielle Empfehlungen für einige Betriebsarten, die separat betrachtet werden können, zum anderen kann zwischen Cyber-Sicherheitsempfehlungen zum Schutz vor einem Sicherheitsvorfall und Cyber-Sicherheitsmaßnahmen zum Detektieren und der Auswertung von bereits erfolgten Vorfällen unterschieden werden. Ein separates Thema stellt die technische Dokumentation dar, die alle Fälle betrifft.

7 gemäß § 14 der Medizinprodukte-Sicherheitsplanverordnung (MPSV)

8 Verordnung über die Erfassung, Bewertung und Abwehr von Risiken bei Medizinprodukten (https://www.gesetze-im-internet.de/mpsv/index.html)

3.1 Cyber-Sicherheitsempfehlungen für alle Betriebsarten

Im ersten Schritt sollten die Schnittstellen des Produktes und die Gefährdungen, die damit für das Gerät entstehen, identifiziert werden. Bei einem netzwerkfähigen Medizinprodukt bedeutet dies, dass

1. alle Schnittstellen dokumentiert werden und
2. der maximal mögliche Schaden bestimmt wird, der durch Angriffe über diese Schnittstelle entstehen kann.

Folgende Fragen sollten in diesem Schritt gestellt werden.

- Welche Schnittstellen hat das Produkt? Was ist die Folge, wenn unerwartete Signale auf die Schnittstellen gegeben werden?
- Welche anderen Komponenten können angeschlossen werden? Was passiert, wenn falsche Komponenten angeschlossen werden?
- Wie werden die Komponenten angeschlossen (Beispiel Ethernet, Funk, USB, andere Signalleitung über Stecker)? Welches Risiko geht von der eingesetzten Technologie aus?
- In welche Richtung geht der Daten-/Signalfluss? Können auch in andere Richtungen Daten übertragen werden?
- Welche Daten/Signale fließen? Können die Daten/Signale verändert, gelöscht oder andere hinzugefügt werden? Wie sind die Daten vor dem Zugriff durch Unberechtigte geschützt?
- Welche Risiken (Auftretenswahrscheinlichkeit, Schadensausmaß) können daraus für Patienten, Anwender oder Dritte erwachsen (Risikoanalyse des Medizinproduktes)? Liegen diese Risiken[9] im akzeptablen Bereich oder sind risikomindernde Maßnahmen erforderlich?

Im zweiten Schritt werden cyber-sicherheitsspezifische Produkteigenschaften festgelegt, welche die im ersten Schritt identifizierten Gefahren nach dem Stand der Technik reduzieren. Folgende Fragen können hierzu verwendet werden.

- Cyber-Sicherheitsmaßnahmen zum Schutz von Daten/Signalen
    - Ist das verwendete Betriebssystem inklusive aller verwendeten Anwendungen einer grundlegenden Systemhärtung unterzogen worden? Werden nur für den Betrieb benötigte Anwendungen betrieben oder wird der Anwender beispielsweise in der Dokumentation darauf hingewiesen, für seinen Anwendungsfall unnötige Anwendungen abzuschalten? Werden - soweit verfügbar - sichere, etablierte Alternativen von verbreiteten spezifischen Protokollen verwendet? (beispielsweise ssh statt telnet, https statt http)
    - Werden nur nach dem Stand der Technik absicherbare Technologien eingesetzt?
    - Wird die Implementierung insbesondere der grundlegenden Kommunikationsprotokolle hinsichtlich ihrer Fehlertoleranz und Robustheit getestet?
    - Wird die Nutzung von Standardimplementierungen einer Eigenentwicklung von Diensten und Protokollen bevorzugt?
    - Werden sensible Daten geschützt übertragen und vorgehalten?
        - Werden allgemein anerkannte Algorithmen und Standardimplementierungen für kryptografische Verfahren genutzt, statt selbst entwickelte?
        - Wird bei deren Implementierung und Verwendung die Technische Richtlinie

9 gemäß DIN EN ISO 14971

TR-02102 des BSI zu Kryptoverfahren[10] eingehalten?

- Gibt es Integritäts-Checks, insbesondere bei Daten, die die Safety beeinträchtigen können?
- Werden sämtliche Schnittstellen zum Gerät mit einer hinreichenden Eingabevalidierung abgesichert, um Manipulationen zu verhindern?

- Sieht das Design vor, dass das Netzwerk gehärtet betrieben werden kann?
  - Ist das zu verwendende Netzwerk per Auslieferung segmentiert oder gibt es Hinweise für den Anwender, wie er das Netzwerk segmentiert betreiben kann? Werden Konfigurationsdaten von dem medizinischen Betrieb getrennt?
  - Ist das Abschalten von eventuell verfügbaren Diensten (z. B. HTTP(S), FTP, etc.) und Technologien (z. B. WLAN, Bluetooth) möglich, wenn diese vom Anwender für seinen Anwendungsfall nicht benötigt werden?
  - Werden alle verwendeten Dienste (beispielsweise HTTP/HTTPS) und verwendete Technologien (z.B. WLAN, Bluetooth) nach dem Stand der Technik bestmöglich gehärtet betrieben oder werden dem Anwender Hinweise gegeben, wie dies umzusetzen ist?
- Wird im Falle eines Client-/Serverbetrieb dieser nach dem Stand der Technik abgesichert betrieben?
  - Werden alle als Cyber-Sicherheitsmaßnahme verwendeten Parameter (wie beispielsweise Session-Cookies) serverseitig berechnet bzw. geprüft?
  - Werden alle Eingaben des Clients serverseitig validiert?
- Gibt es eine feingranulare Zugriffskontrolle (Login/Authentisierung), die sensible Daten vor unberechtigtem Zugriff schützt? Gibt es eine hinreichende Benutzerverwaltung (d. h. mehrere Nutzer mit unterschiedlichen Rollen und Berechtigungen)?
  - Werden Zugangsdaten (insbesondere Passwörter) statt als Klartext kryptografisch gemäß dem aktuellen Stand der Technik geschützt gespeichert?
  - Werden bei einem fehlgeschlagenen Login nur allgemeine Fehlermeldungen ausgegeben, die beispielsweise keinen Rückschluss darauf geben, dass der Username korrekt aber das Passwort falsch war?
  - Kann der Zugriff über die Netzwerkschnittstellen auf bestimmte MAC-Adressen oder IP-Adressen bzw. IP-Adressbereiche beschränkt werden?
  - Gibt es ergänzende Mechanismen, die einen Eingriff durch einen Bediener absichern, wie z. B. Vier-Augen-Prinzip?
  - Gibt es Software oder Prozesse, die mit System-Privilegien laufen? Sind diese vor Angreifern geschützt?
- Gibt es ein abgesichertes Session-Management, wenn mehrere Personen Zugriff besitzen?
  - Ist technisch ausgeschlossen, dass ggf. kritische Aktionen ohne das Vorhandensein der dazu erforderlichen Rechte ausgeführt werden können?
  - Sind im Betrieb verwendete Sessions untereinander geschützt?
  - Erfolgt ein Timeout von Sessions bzw. kann dieser konfiguriert werden?
  - Gibt es Vorkehrungen, um einen Angriff auf die Verfügbarkeit von Diensten durch Öffnen von vielen Verbindungen bzw. Sitzungen zu erschweren?

10 https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

- Sonstige Cyber-Sicherheitsfunktionen
  - Ist eine Erkennung und ein Schutz gegen Schadprogramme eingerichtet, sofern eine Gefährdung dafür besteht?
  - Ist sichergestellt, dass bei einem Denial-of-Service Angriff die grundlegende Funktionalität der Komponente erhalten bleibt und die Komponente nach einem solchen Angriff den normalen Betrieb mit dem vollständigen Funktionsumfang eigenständig wieder aufnimmt?
  - Sind Update-Mechanismen (z. B. für Firmware-Updates), insbesondere die über ein Netzwerk statt lokal am Gerät erfolgen, hinreichend abgesichert? Neben Integritätsprüfungen mittels Prüfsummen ist insbesondere eine geeignete Authentifizierung oder eine Absicherung über Signaturen vorzusehen.
  - Sind sichere und nutzerfreundliche Mechanismen oder entsprechende Schnittstellen zu Standardverfahren für Backup und Wiederherstellung vorhanden und dokumentiert?

- Cyber-Sicherheitsmaßnahmen zum Detektieren von Angriffen
  - Logging
    - Werden alle ggf. kritischen Aktionen in Logdateien vermerkt wie z. B. die Änderung der Konfiguration, fehlgeschlagene Login-Versuche, das Entfernen oder der Austausch von Speichermedien oder das Anschließen eines USB-Geräts?
    - Wird verhindert, dass über Logdaten ungeschützt auf kritische oder vertrauliche Informationen (z. B. Login- oder Patientendaten) zugegriffen werden kann?
  - Auswertung von Logdaten
    - Gibt es eine Möglichkeit zur automatischen Alarmierung im Falle von kritischen Systemereignissen oder -zuständen?
    - Gibt es Warnmeldungen, wenn ein Brute-Force-Angriff auf einen Login-Mechanismus erfolgt?

3.2 Cyber-Sicherheitsempfehlungen für die Produktkonfiguration

Die Konfigurationsmöglichkeiten sind von besonderer Bedeutung für die Cyber-Sicherheit einer Komponente, da hierüber u. a. Sicherheitsmechanismen gesteuert und parametriert werden. Hierzu sind insbesondere die folgenden Leitfragen zu beachten.

- Kann die Konfiguration nur nach vorheriger Authentifizierung modifiziert werden?
- Erfolgt die Auslieferung in einer sicheren Standardkonfiguration („Secure by Default“)?
- Sind die Passwörter, Zertifikate usw. für sämtliche Dienste austauschbar?
- Ist die Konfiguration gegen nicht autorisierte Manipulation geschützt, beispielsweise durch Prüfsummen oder Signaturen?
- Sofern Standard-IT für Konfigurationsoberflächen verwendet wird, ist diese ausreichend abgesichert? Werden verfügbare Empfehlungen und Technische Richtlinien sauber implementiert? Sollte beispielsweise eine Weboberfläche verwendet werden, wird die Verbindung hierzu ausschließlich verschlüsselt zur Verfügung gestellt? Können technisch die Mindestanforderungen des BSI für den Einsatz von TLS[11] eingehalten werden und kann der Webserver nach den Cyber-Sicherheitsempfehlungen für den si-

11 Der Mindeststandard https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf wurde für Bundesbehörden erhoben. Es wird empfohlen, dass die Vorgaben auch im Bereich der netzwerkfähigen Medizinprodukte umgesetzt werden.

cheren Betrieb eines Webservers[12] betrieben werden?

- Gibt es einen automatischen Logoff-Prozess, der verhindert, dass unberechtigte Personen nach einer vergessenen Abmeldung in der Lage sind, Konfigurationsänderungen vorzunehmen?

3.3 Cyber-Sicherheitsempfehlungen für den Servicebetrieb

Wie bei jedem technischen Gerät gibt es auch bei Medizingeräten Wartungsaufgaben zu erfüllen. Je nach Zweckbestimmung kann es beispielsweise notwendig sein, dass Geräte kalibriert oder auch Updates aufgespielt werden müssen.

- Sind alle Schnittstellen, die für Servicezwecke verwendet werden, gegen den Zugriff durch Unberechtigte geschützt?
- Wenn eine Fernwartung durchgeführt wird, ist gesichert, dass die dafür eingerichteten Komponenten den eigentlichen Betrieb in keinster Weise beeinträchtigen?
- Kann eine Fernwartung bzw. ein Schreibzugriff auf ein Produkt oder eine Komponente nur dann erfolgen, wenn diese explizit aktiviert wird, mit zeitlicher Beschränkung und expliziter Willenserklärung (Beispielsweise durch einen Bestätigungsdialog, Freischaltung)?

3.4 Technische Dokumentation

Von besonderer Bedeutung für den sicheren Einsatz beim Kunden bzw. bei der Weiterverwendung für Installation und Konfiguration sind neben der Gebrauchsanweisung die technische Dokumentation des Produktes und die technischen Anforderungen an seine Einsatzumgebung.

Die folgenden Prüffragen sind als Orientierungshilfe bei der Erstellung und Überprüfung der technischen Dokumentation auf Cyber-Sicherheitsfragen geeignet.

- Wird IT-Kräften auf Anwenderseite eine technische Dokumentation übermittelt, die ihnen verständlich dokumentiert, wie das Gerät technisch sicher zu betreiben ist?
- Werden die Zielgruppen genannt, die aus cyber-sicherheitsspezifischen Überlegungen über bestimmte technische Informationen in Kenntnis gesetzt werden sollten?
- Enthält die Dokumentation Informationen, auf deren Grundlage der Kunde ein IT-Sicherheitskonzept erstellen kann?[13]
    - Sind sämtliche Schnittstellen, Zugänge und Funktionen dokumentiert?
    - Werden die Cyber-Sicherheitseigenschaften bzw. -funktionen der Komponente beschrieben?
    - Wird dargestellt, welche Risiken / Bedrohungen durch die Komponente selbst abgedeckt werden?
    - Ist dokumentiert, welche Bedrohungen im Rahmen einer Cyber-Sicherheitsbewertung bzw. eines Cyber-Sicherheitsmanagements zu beachten sind?
    - Ist dokumentiert, wie diesen Bedrohungen entgegengewirkt werden kann?
    - Ist dokumentiert, welche Dienste (mit den im Produkt integrierten Mechanismen) nicht abgesichert werden können und daher ergänzende technische oder organisatorische Cyber-Sicherheitsmaßnahmen erfordern?
- Gibt es Empfehlungen bzgl. der Konfiguration für einen sicheren Betrieb (z. B. Leitfaden

12 Weitere Empfehlungen – insbesondere für eine HTTP(S)-Schnittstelle (Weboberfläche) – finden sich in der BSI-Empfehlung „Entwicklung sicherer Webanwendungen“, wobei dort insbesondere der Abschnitt "Entwicklungsphase" relevant ist.

13 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m02/m02195.html

zur Systemhärtung)? Beispielsweise:

- Gibt es ausreichende Hinweise für die Änderung von Standardpasswörtern und zum Deaktivieren von nicht benötigten Accounts?
- Gibt es eine Checkliste zur Übersicht über die Konfiguration und deren cyber-sicherheitsspezifische Implikationen? Sind die cyber-sicherheitsspezifischen Konsequenzen der möglichen Konfigurationsoptionen / -alternativen dokumentiert? Gibt es Hinweise darauf, welche Einstellungen als kritisch zu betrachten sind und ggf. zu einer erhöhten Gefährdung führen?
- Gibt es Referenzen auf weiterführende Informationen zur Absicherung bzw. zum sicheren Betrieb?

Hilfestellungen und Erläuterungen zu den grundlegenden Anforderungen an Medizinprodukte, den entsprechenden harmonisierten Normen sowie den gesetzlichen Meldeverpflichtungen für Hersteller, Betreiber und professionelle Anwender von Medizinprodukten finden sich u.a. auf den Webseiten des BfArM.[14]

Hilfestellungen, wie IT-Sicherheitsanforderungen an einzelne Produkte oder Technologien umgesetzt werden können, finden sich u. a. im IT-Grundschutz[15] oder in den Cyber-Sicherheitsempfehlungen des BSI[16].

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

14 https://www.bfarm.de
15 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/grundschutz.html
16 https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/empfehlungen_node.html