Allgemeine Einführung TD, MDR - Technische Dokumentation Anhang 2 und 3

Security Anforderungen

REGULATORY KONFERENZ
FÜR MEDIZINPRODUKTE & IVD

WIEN, 3.12.2019

Volker Sudmann
mdc medical device certification GmbH

mdc medical device certification GmbH

Benannte Stelle / Notified Body 0483

- Richtlinie 93/42/EEC - MDD
- Richtlinie 98/79/EC - IVDD

Candidate Notified Body

- Verordnung (EU) 2017/745 - MDR
- Verordnung (EU) 2017/746 - IVDR

Akkreditierte Zertifizierungsstelle

- EN ISO 13485
- EN ISO 9001

Internationale Verfahren

- Medical Device Single Audit Program (MDSAP)
  (mit Kooperationspartner)
- Taiwan TCP II

mdc medical device certification GmbH
Zweigniederlassung Austria

Wienerbergstraße 11/A/18
1100 Wien

Informationssicherheit …

WARUM?

- **Anlässe gibt es genug …**

Anlässe gibt es genug …

FDA U.S. FOOD & DRUG ADMINISTRATION

Date Issued: June 27, 2019

The FDA is warning patients and health care providers that certain Medtronic MiniMed™ insulin pumps have potential cybersecurity risks. Patients with diabetes using these models should switch their insulin pump to models that are better equipped to protect against these potential risks.

Medtronic is recalling the following affected MiniMed pumps and providing alternative insulin pumps to patients.

Pump Model	Software Version
MiniMed™ 508	All versions
MiniMed™ Paradigm™ 511	All versions

https://www.fda.gov/medical-devices/safety-communications/certain-medtronic-minimed-insulin-pumps-have-potential-cybersecurity-risks-fda-safety-communication

Anlässe gibt es genug …

U.S. FOOD & DRUG ADMINISTRATION

URGENT/11 Cybersecurity Vulnerabilities in a Widely-Used Third-Party Software Component May Introduce Risks During Use of Certain Medical Devices: FDA Safety Communication

Share Tweet LinkedIn Email Print

Date Issued: October 1, 2019

The U.S. Food and Drug Administration (FDA) is informing patients,

https://www.fda.gov/medical-devices/safety-communications/certain-medtronic-minimed-insulin-pumps-have-potential-cybersecurity-risks-fda-safety-communication

Anlässe gibt es genug …

Bundesinstitut
für Arzneimittel
und Medizinprodukte

Maßnahmen von Herstellern mit Bezug Cybersicherheit

Datum	Titel	
	1	
18.10.2019	**Dringende Sicherheitsinformation zu GSS67H von Getinge Sterilization AB** Allgemeine med. Behandlungseinrichtungen /-geräte /-hilfsmittel - Reinigung / Desinfektion / Sterilisation	PDF 50KB
02.08.2019	**Dringende Sicherheitsinformation zu IONTRIS von Siemens Healthcare GmbH, Advanced Therapies, Particle Therapy** Strahlentherapie / Strahlenschutz - Nuklearmedizinische Geräte f. d. Therapie	PDF 151KB
18.07.2019	**Dringende Sicherheitsinformation zu CareLink Programmer; CareLink Encore Programmer von Medtronic Inc** Aktive implantierbare medizinische Geräte - Defibrillatoren	PDF 1MB
11.07.2019	**Dringende Sicherheitsinformation zu Medtronic MiniMed Paradigm Infusion Pumps; Medtronic MiniMed Paradigm VEOTM;**	PDF 342KB

https://www.bfarm.de/DE/Medizinprodukte/RisikoerfassungUndBewertung/Cybersicherheit/kundeninfos_cybersicherheit_node.html

Anlässe gibt es genug …

https://www.heise.de/ct/artikel/Massive-Datenschutzmaengel-in-der-Gesundheits-App-Ada-4549354.html

Informationssicherheit …

WARUM?

- Anlässe gibt es genug …
- **wird vom Gesetz gefordert …**

Verordnung (EU) 2017 / 745 – Medizinprodukteverordnung
Anhang I – Grundlegende Sicherheits- und Leistungsanforderungen

- **14.1.** Wenn ein Produkt zur Verwendung in **Kombination mit anderen Produkten** (…) bestimmt ist, muss die **Kombination (…) sicher** sein und darf die **vorgesehene Leistung der Produkte nicht beeinträchtigen**. (…)
- **14.2.** Die Produkte werden so ausgelegt und hergestellt, dass folgende Risiken ausgeschlossen oder so weit wie möglich reduziert werden:
  - (…)
  - **d)** Risiken im Zusammenhang mit der **möglichen negativen Wechselwirkung zwischen Software und der IT- Umgebung**, in der sie eingesetzt wird und mit der sie in Wechselwirkung steht;
  - (…)

Verordnung (EU) 2017 / 745 – Medizinprodukteverordnung
Anhang I – Grundlegende Sicherheits- und Leistungsanforderungen

- **17.** Programmierbare Elektroniksysteme - Produkte, zu deren Bestandteilen programmierbare Elektroniksysteme gehören und (…) Software:
  - **17.2.** Bei Produkten, zu deren Bestandteilen Software gehört (…) wird die Software entsprechend dem Stand der Technik entwickelt (…), wobei die Grundsätze (…) des **Risikomanagements** einschließlich der **Informationssicherheit (…)** zu berücksichtigen sind.
  - **17.4.** Die **Hersteller legen Mindestanforderungen** bezüglich **Hardware, Eigenschaften von IT-Netzen** und **IT-Sicherheitsmaßnahmen** einschließlich des **Schutzes vor unbefugtem Zugriff** fest, die für den bestimmungsgemäßen Einsatz der Software erforderlich sind.

Verordnung (EU) 2017 / 746 – In-Vitro-Diagnostika-Verordnung
Anhang I – Grundlegende Sicherheits- und Leistungsanforderungen

- **13.1.** Wenn ein Produkt zur Verwendung in **Kombination mit anderen Produkten** (…) bestimmt ist, muss die **Kombination (…) sicher** sein und darf die **vorgesehene Leistung der Produkte nicht beeinträchtigen**. (…)
- **13.2.** Die Produkte werden so ausgelegt und hergestellt, dass folgende Risiken ausgeschlossen oder so weit wie möglich reduziert werden:
  - (…)
  - **d)** Risiken im Zusammenhang mit der **möglichen negativen Wechselwirkung zwischen Software und der IT- Umgebung**, in der sie eingesetzt wird und mit der sie in Wechselwirkung steht;
  - (…)

Verordnung (EU) 2017 / 746 – In-Vitro-Diagnostika-Verordnung
Anhang I – Grundlegende Sicherheits- und Leistungsanforderungen

- **16.** Programmierbare Elektroniksysteme - Produkte, zu deren Bestandteilen programmierbare Elektroniksysteme gehören und (…) Software:
  - **16.2.** Bei Produkten, zu deren Bestandteilen Software gehört (…) wird die Software entsprechend dem Stand der Technik entwickelt (…), wobei die Grundsätze (…) des **Risikomanagements** einschließlich der **Informationssicherheit (…)** zu berücksichtigen sind.
  - **16.4.** Die **Hersteller legen Mindestanforderungen** bezüglich **Hardware, Eigenschaften von IT-Netzen** und **IT-Sicherheitsmaßnahmen** einschließlich des **Schutzes vor unbefugtem Zugriff** fest, die für den bestimmungsgemäßen Einsatz der Software erforderlich sind.

US Food & Drug Administration

- **Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software**
  Jan 14, 2005
- **Content of Premarket Submissions for Management of Cybersecurity in Medical Devices**
  Oct 2, 2014 / Draft Oct 18, 2018
- **Postmarket Management of Cybersecurity in Medical Devices**
  2016 Dec 28

Informationssicherheit …

WARUM?

- Anlässe gibt es genug …
- Wird vom Gesetz gefordert …

um WAS geht es?

- **Schutzziele**

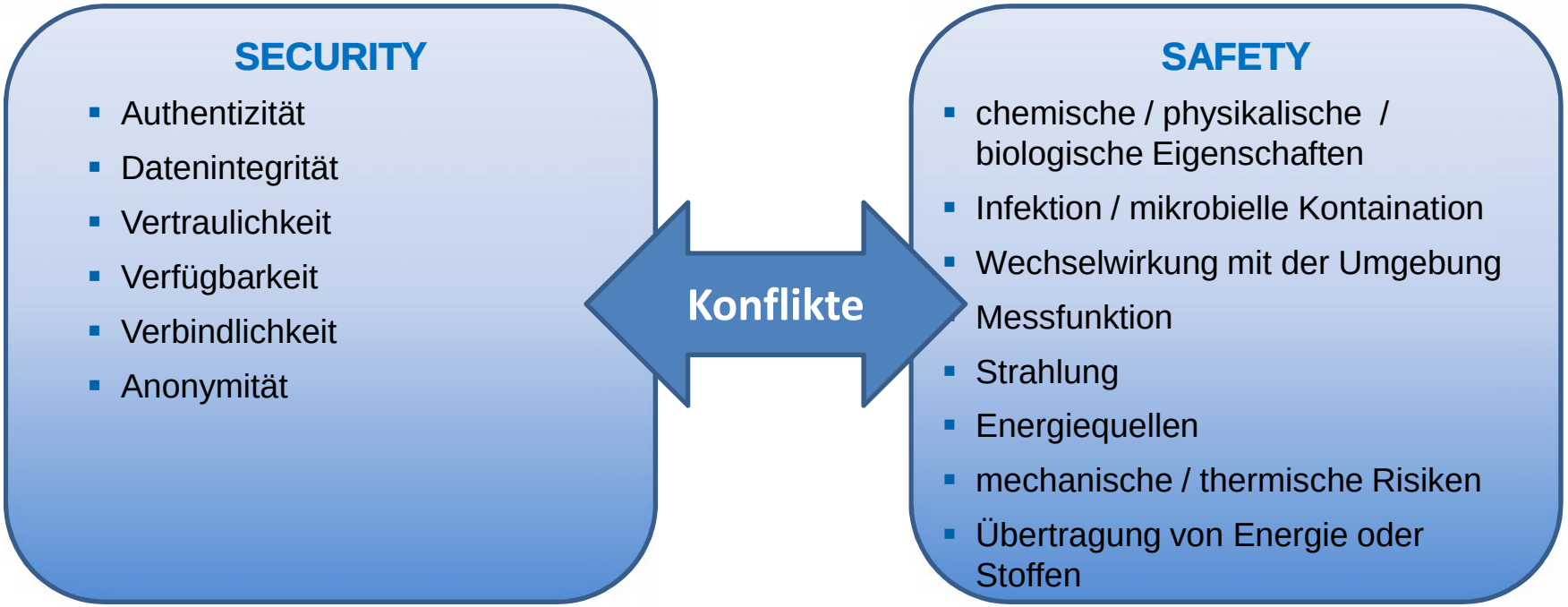
Schutzziele Informationssicherheit

- **Authentizität / *Authenticity***
  … sicherstellen dass die Echtheit / Glaubwürdigkeit eines Objekts / Subjekts anhand von eindeutigen Merkmalen überprüfbar ist …
- **Datenintegrität / *Integrity***
  … sicherstellen dass Daten nicht unautorisiert und unbemerkt manipuliert werden …
- **Informationsvertraulichkeit / *Confidentiality***
  … sicherstellen dass keine unautorisierte Informationsgewinnung stattfindet …

Schutzziele Informationssicherheit

- **Verfügbarkeit / *Availability***
  … sicherstellen, dass authentifizierte und autorisierte Subjekte in der Wahrnehmung ihrer Berechtigungen nicht unautorisiert beeinträchtigt werden …
- **Verbindlichkeit / *Non repudiation***
  … sicherstellen, dass die Durchführung einer Aktion nachträglich nicht abstreitbar ist …
- **Anonymität / *Anonymity***
  … sicherstellen, dass Veränderungen personenbezogener Daten nicht mehr (oder nur mit unverhältnismäßig hohem Aufwand) einer bestimmten Person zugeordnet werden können …

Zielkonflikte



Informationssicherheit …

WARUM?

- Anlässe gibt es genug …
- Wird vom Gesetz gefordert …

um WAS geht es?

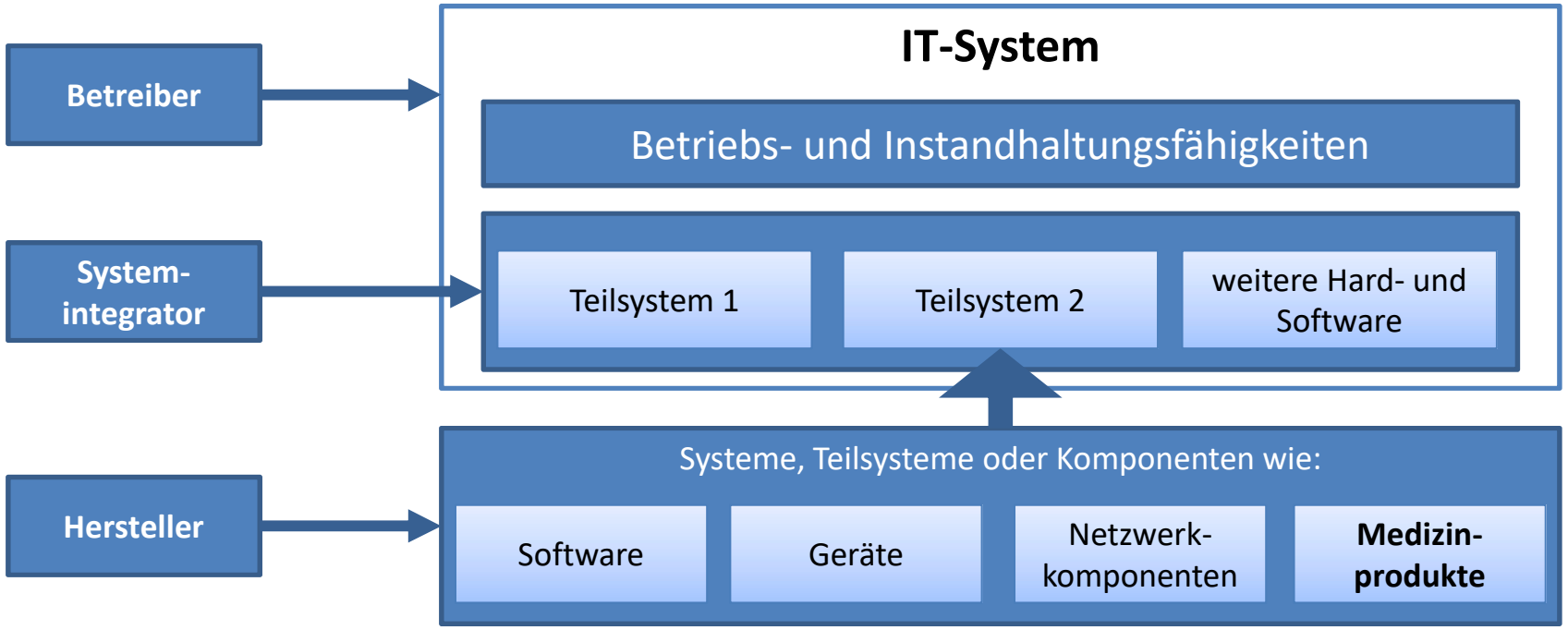
- Schutzziele

WORIN liegt die Heausforderung?

- **Informationssicherheit als Gemeinschaftsaufgabe**

Tiefgestaffelte Verteidigung

Informationssicherheit als Gemeinschaftsaufgabe



Informationssicherheit …

WARUM?

- Anlässe gibt es genug …
- Wird vom Gesetz gefordert …

um WAS geht es?

- Schutzziele

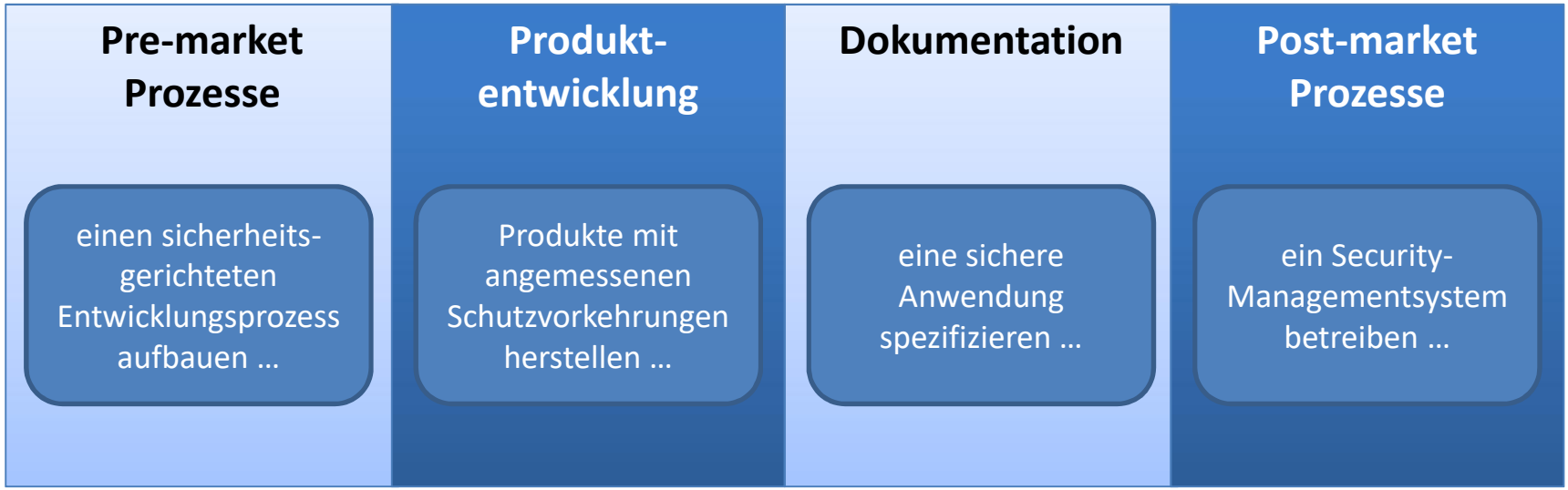
WORIN liegt die Heausforderung?

- Informationssicherheit als Gemeinschaftsaufgabe

WAS muss ein Hersteller tun?

- **Aufgaben**

Aufgaben für den Hersteller …



Informationssicherheit …

WARUM?

- Anlässe gibt es genug …
- Wird vom Gesetz gefordert …

um WAS geht es?

- Schutzziele

WORIN liegt die Heausforderung?

- Informationssicherheit als Gemeinschaftsaufgabe

WAS muss ein Hersteller tun?

- Aufgaben

WIE kann ein Hersteller das tun?

- **Normen**

Software-Lebenszyklus-Prozesse

- **IEC 62304 (*)**
  Medizingeräte-Software - Software-Lebenszyklus-Prozesse
- **IEC 82304**
  Gesundheitssoftware - Teil 1: Allgemeine Anforderungen für die Produktsicherheit
- **IEC 80001-5-1 (*)**
  Safety, security and effectiveness in the implementation and use of connected medical devices or connected health software,
  Part 5-1: Security - Activities in the product lifecycle
- IEC 62443-4-1
  IT-Sicherheit für industrielle Automatisierungssysteme,
  Teil 4-1: Anforderungen an den Lebenszyklus für eine sichere Produktentwicklung
- ISO 27034
  Information technology. Security techniques.

(*) im Entwurf oder in Überarbeitung

Pre-market Prozesse: anwendbare Standards …

Gefahren- und Risikoanalyse

- **ISO 14971 (*)**
  Risikomanagements auf Medizinprodukte
- IEC 62443-3-2
  Sicherheitsrisikobeurteilung und Systemgestaltung
- ISO 27005
  Informationssicherheits-Risikomanagement
- ISO/IEC 15408
  Evaluationskriterien für IT-Sicherheit
- ISO/IEC 18045
  Methodik für die Bewertung der IT-Sicherheit

Lifecycle

- ISO 270xx
  Informationstechnik
- IEC 12207
  Prozesse im Lebenszyklus von Software
- NIST SP800-160
  Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems
- …

(*) im Entwurf oder in Überarbeitung

Produktentwicklung: anwendbare Standards …

- **IEC 60601-x-x**
  Medizinische elektrische
- **EN 45501**
  Aktive implantierbare medizinische Geräte
- **IEC 60601-4-5 (*)**
  Safety related technical security specifications for medical devices
- **ISO 22696 (*)**
  Guidance for identification and authentication for connectable personal healthcare devices
- **ISO 11633**
  Fernwartung von Medizinprodukten und Informationssystemen im Gesundheitswesen
- **UL 2900-2-1**
  Standard for Software Cybersecurity for Network-Connectable Products, Part 2-1 Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems
- ISO 18033
  Verschlüsselungsalgorithmen
- ISO 18367
  Konformitätsprüfung für kryptographische Algorithmen und Sicherheitsmechanismen
- ISO 19772
  Authentifizierte Verschlüsselung
- ISO 27040
  Speichersicherheit

Dokumentation: anwendbare Standards …

- **IEC 80001-2-2**
  Leitfaden zur Angabe von Bedingungen für die Kommunikationssicherheit von Medizinprodukten, Risiken und Risikobeherrschung
- **IEC 80001-2-8**
  Leitfaden für die Tauglichkeit von Normen um die Security, wie in IEC TR 80001-2-2 festgelegt, nachzuweisen
- **IEC 80001-2-9**
  Leitfaden für die Verwendung von Assurance Cases zur Bestätigung der Übereinstimmung mit IEC/TR 80001-2-2 Kommunikationssicherheit
- ISO 15026
  System- und Software-Zusicherung
- ISO 15443
  IT-Sicherheitsverfahren - Rahmenwerk zur Zusicherung der Sicherheit
- ISO 18367
  Konformitätsprüfung für kryptographische Algorithmen und Sicherheitsmechanismen

Security Management: anwendbare Standards …

- ISO 29147
  Bekanntgabe von Sicherheitslücken
- ISO 30111
  Prozesse für die Behandlung von Schwachstellen
- ISO 27000 (*)
  Informationssicherheits-Managementsysteme

(*) im Entwurf oder in Überarbeitung

Informationssicherheit …

WARUM?

- Anlässe gibt es genug …
- Wird vom Gesetz gefordert …

um WAS geht es?

- Schutzziele

WORIN liegt die Heausforderung?

- Informationssicherheit als Gemeinschaftsaufgabe

WAS muss ein Hersteller tun?

- Aufgaben

WIE kann ein Hersteller das tun?

- **Normen**
- **Leitfäden**

Leitfäden und Hilfestellungen

- **Cyber-Sicherheitsanforderungen an netzwerkfähige Medizinprodukte**
  Bundesamt für Sicherheit in der Informationstechnik (BSI), Deutschland
  BSI-CS 132, Ver. 1.0 vom 02.05.2018
- **Leitfaden IT-Sicherheit für Medizinprodukte**
  Johner-Institut, Prof. Dr. Christian Johner

Informationssicherheit …

WARUM?

- Anlässe gibt es genug …
- Wird vom Gesetz gefordert …

um WAS geht es?

- Schutzziele

WORIN liegt die Heausforderung?

- Informationssicherheit als Gemeinschaftsaufgabe

WAS muss ein Hersteller tun?

- Aufgaben

WIE kann ein Hersteller das tun?

- Normen
- Leitfäden

WAS erwartet Sie im Audit?

Was wird im Audit gefragt werden?

- **Kompetenz,** Aus- und Weiterbildung in Bezug auf Informationssicherheit
  - Festlegungen von Anforderungen, Nachweise
- Einbindung **externer Kompetenzen** betreffend Informationssicherheit
  - Anforderungen, Nachweise, Lenkung als kritische Lieferanten
- **Entwicklungsprozess**
  - Berücksichtigung von IT-Sicherheit bei der Entwicklung (Security by design)
  - Coding Guidelines ausgerichtet auf IT-Sicherheit
  - Deployment-Prozess für Updates, Patches usw., Schnittstelle zum Viglinanz-Prozess

Was wird im Audit gefragt werden?

- **Produktentwicklung**
  - Nachbarsysteme (Medizinprodukte, IT-Systeme), Nutzungsumgebung (Hard- und Software)
  - Analyse von Gefährdungen in Bezug auf Nutzer und Umgebung:
    - unberechtigter Zugriff, Verwendung in nicht spezifizierter Umgebung
  - Bedrohungen IT-Sicherheit → Gefährdungen für Patienten, Anwender und Dritte
  - Schnittstellen zum Benutzer
  - Datenschnittstellen, Protokolle und Standards
    - Wer darf wann auf welche Funktionen des Produkts zugreifen?
    - Wie werden Angriffe über diese Schnittstellen beherrscht
  - Authentifizierung und Autorisierung, Angemessenheit → Auswirkungen auf Patientensicherheit

Was wird im Audit gefragt werden?

- **Produktentwicklung**
  - Daten: Schutzwürdigkeit, Datenverlust, Validität der Daten
  - Kommunikation: Überlastung des Systems, Verfügbarkeit des Netzwerks
  - Dienste die das Produkt anbietet oder nutzt
    - Welcher Dienst ist warum und wie lange nach aussen sichtbar?
    - Wer realisiert diesen Dienst?
  - SOUP- / OTS Komponenten im Produkt
    - Analyse und Bewertung von Risiken
    - Programmiersprache
    - Betriebssystem
    - Risiken, wenn diese Komponenten sich nicht spezifikationsgemäß verhalten, identifiziert und bewertet?

Was wird im Audit gefragt werden?

- **Produktentwicklung**
  - Angriffe / Kompromittierung erkennen
    - Wie wird dies festgestellt und dokumentiert?
    - Wie wird darauf reagiert?
    - Funktionalität, die auch im Falle der Kompromittierung gewährleistet sein muss
  - Software- und Systemtests
    - Eignung des Tests, die Umsetzung der Anforderungen zur IT-Sicherheit zu belegen.
    - Maßnahmen zur Risikobeherrschung wirksam umgesetzt?
    - Vollständigkeit, wurden alle Software- und Systemanforderungen überprüft

Was wird im Audit gefragt werden?

- **Produktentwicklung**
  - Sicherstellung der Freiheit von Schadcode bei den Entwicklungswerkzeugen
  - Freiheit von Schadcode im Produkt sicherstellen
    - vor Auslieferung prüfen
    - Produktionssystems von Malware schützen
    - Integrität des Verteilungsweges sicherstellen
- **Produktion, Distribution, Installation**
  - Auslieferung der vorgesehenen Dateien in den vorgesehenen Versionen
  - … und wissen die Verantwortlichen für die Installation davon?
  - Werden die Voraussetzungen für Installation und Inbetriebnahme erfüllt?

Was wird im Audit gefragt werden?

- **Marktbeobachtung**
  - Adressiert der Post Market Surveillance Plan auch IT-Sicherheit angemessen:
    - Welche Informationen müssen gesammelt werden (versuchte oder erfolgreiche Kompromittierung)?
      - Über welche Kanäle geschieht dies?
    - Wie werden diese Informationen analysiert und bewertet?
    - Welche Maßnahmen resultieren daraus?
    - Sind für jede SOUP- / OTS-Komponente Informationsquellen und Überwachungsfrequenzen hinsichtlich IT-Sicherheitsbezogenen Informationen festgelegt?
      - Wer wertet mit welchen Werkzeugen diese Informationen aus?
      - Wie wird überwacht, welche Technologien und Verfahren noch sicher sind?

Was wird im Audit gefragt werden?

- **Incident Response:**
  - Ist das IT-Security-Incident-Handling des Herstellers geeignet, innerhalb angemessener Zeiträume zu reagieren?
  - Können alle betroffenen Anwender und Betreiber zu erreichen werden?
- **Außerbetriebnahme**
  - Existiert ein Life-Cycle-Konzept für Patientendaten welches u.a. folgende Aspekte einschließt?
    - Schutz vor ungewollter Löschung
    - Schutz vor Nutzungsänderung
    - Endgültige Löschung

Fazit …

Informationssicherheit bei Medizinprodukten …

… eine Herausforderung für Hersteller und benannte Stellen!

Herzlichen Dank für Ihre Aufmerksamkeit!

mdc medical device certification GmbH
Kriegerstr. 6
70191 Stuttgart

Phone: +49 (0) 7 11 / 25 35 97-0
Telefax: +49 (0) 7 11 / 25 35 97-10
Email: mdc@mdc-ce.de

mdc medical device certification GmbH
Berlin branche office
Ernst-Augustin-Str. 2
12489 Berlin

Phone: +49 (0) 30 / 31879830 - 300
Telefax: +49 (0) 30 / 31879830 - 309
Email : mdc@mdc-ce.de

mdc medical device certification GmbH
Branch office austria
Wienerbergstr. 11 / A 18
1100 Wien, Österreich

Phone: +43 (1) / 388 0483-0
Telefax: +43 (1) / 388 0483-590
Email : mdc@mdc-ce.at

mdc medical device certification GmbH
Tuttlingen branche office
Rathausstr. 5
78532 Tuttlingen

Phone: +49 (0) 7 11 / 25 35 97-0
Telefax: +49 (0) 7 11 / 25 35 97-10
Email : mdc@mdc-ce.de