Cyber Security für implantierbare Medizinprodukte

Dr. V. Lang, Aug 2018

BIOTRONIK
excellence for life

URGENT FIELD SAFETY NOTICE

Information About Cybersecurity Update for Accent™/ Anthem™, Accent MRI™/ Accent ST™, Assurity™/ Allure™ and Assurity MRI™ devices

28 August, 2017

Dear Doctor,

We are advising you of the availability of new pacemaker firmware (a type of software) that is intended to address the risk of unauthorized access to our pacemakers that utilize radio frequency

Bloomberg Markets

Radio controlled p… hard to hack

Flaws

SCIENCE TECH CYBERSECURITY

need a firmware

APRIL 23, 2018 CYBERSECURITY ICD AND CRT-D FIRMWARE RELEASE UPDATE

Abbott released a planned upgrade to the firmware installed on certain implantable cardioverter defibrillator (ICD) or cardiac resynchronization therapy defibrillator (CRT-D) devices. This firmware upgrade incorporates two updates to improve performance and strengthen the security of these devices. These updates are part of Abbott's ongoing commitment to continuously improve patient care.

WHAT IS THE PURPOSE OF THE NEW UPDATE?

The ICD and CRT-D firmware upgrade incorporates two updates designed to strengthen the security and improve the performance of your ICD or CRT-D. The security update provides an additional layer of protection against unauthorized access to your device. It is intended to prevent anyone other than your doctor from changing your device settings. Abbott has had no reports of hacking or unauthorized access to any patient's implanted device.

LILY HAY NEWMAN SECURITY 08.09.18 12:30 PM

A NEW PACEMAKER HACK PUTS MALWARE DIRECTLY ON THE DEVICE

10. August 2018

heise Security

News ▾ Hintergrund Events

Security > 7-Tage-News > 08/2018 > Möchten Sie sterben? Malware gegen Herzschrittmacher lässt Hersteller...

Möchten Sie sterben? Malware gegen Herzschrittmacher lässt Hersteller kalt

10.08.2018 17:18 Uhr – Uli Ries

Ein Schrittmacher des US-Herstellers Medtronic (Bild: Medtronic)

Die Firma Medtronic sieht kein Problem darin, dass Hacker die Software in ihren Herzschrittmachern nach belieben manipulieren können.

Zwei Hacker haben einen Hersteller von Herzschrittmachern und Insulinpumpen auf schwere Sicherheitslücken in dessen Produkten aufmerksam gemacht. Das Spektrum der Lücken

ICS-CERT Flags Medtronic Devices for Cybersecurity Vulnerabilities

A Medtronic patient monitor and an insulin pump were flagged this week by ICS-CERT for cybersecurity vulnerabilities that could expose sensitive data to attackers.

excellence for life

Cyber Security = Informationssicherheit

Cyber Security oder Informationssicherheit bezeichnet die Eigenschaften zum Schutz von IT-Systemen von Diebstahl oder Beschädigung von Hardware, Software oder Informationen. Darüber hinaus der Schutz von Unterbrechung oder Veränderung der IT Dienste*.

Sicherheit

- Beschädigung von HW oder SW
- Unterbrechung oder Veränderung von IT Diensten**

Vertraulichkeit

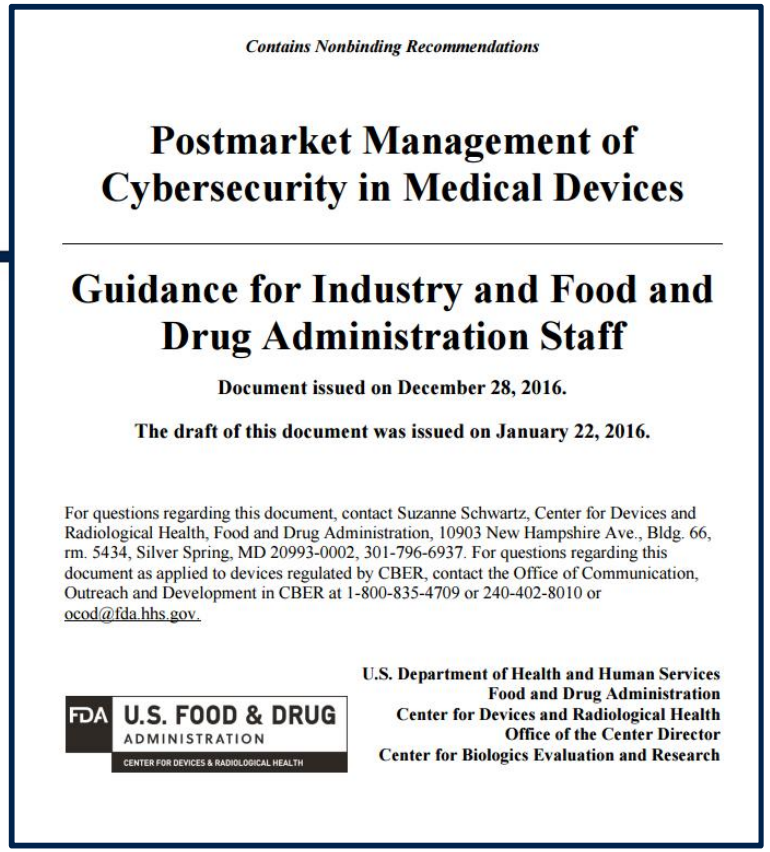
- Diebstahl von Daten
- Datenmissbrauch (Erpressung)

*https://en.wikipedia.org/wiki/Computer_security
**http://www.profitsoverpatients.com/

BIOTRONIK
excellence for life

Cyber Security für Medizinprodukte - Zulassungsanforderungen

- Externe Anforderungen
  - FDA Pre-market und Post-market Guidance = Regelsatz zur Zulassung von Medizinprodukte in USA
  - NIST* Framework Empfehlungen der US Standardisierungsbehörde
    - Werte festlegen
    - Werte schützen
    - Angriffe detektieren
    - Reagieren
    - Wiederherstellen



Contains Nonbinding Recommendations

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

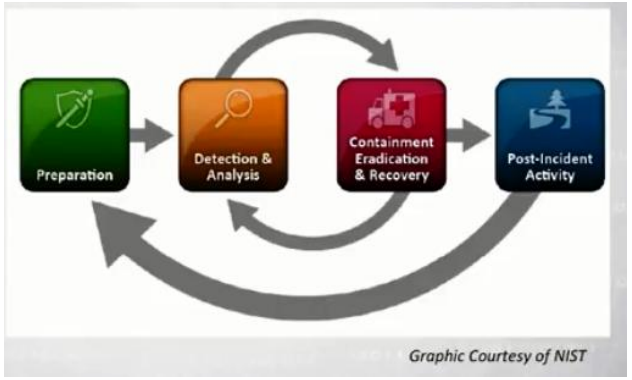
Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

For questions regarding this document, contact Suzanne Schwartz, Center for Devices and Radiological Health, Food and Drug Administration, 10903 New Hampshire Ave., Bldg. 66, rm. 5434, Silver Spring, MD 20993-0002, 301-796-6937. For questions regarding this document as applied to devices regulated by CBER, contact the Office of Communication, Outreach and Development in CBER at 1-800-835-4709 or 240-402-8010 or ocod@fda.hhs.gov.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research

FDA U.S. FOOD & DRUG ADMINISTRATION
CENTER FOR DEVICES & RADIOLOGICAL HEALTH



*NIST: National Institute for Standards and Technology

BIOTRONIK
excellence for life

Cyber Security für Medizinprodukte
… integriert sich in das Risikomanagement

- Interne Anforderungen
  - Teil des existierenden Risiko Management Prozesses (ISO 14971)
  - Cyber Security Prozess hat Rückkopplung zum Risiko Management

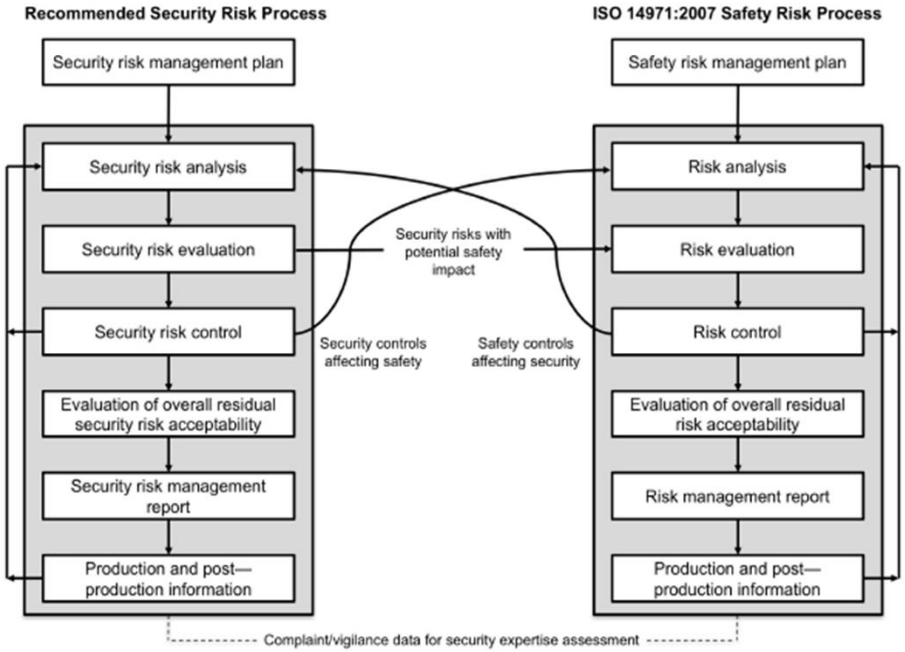
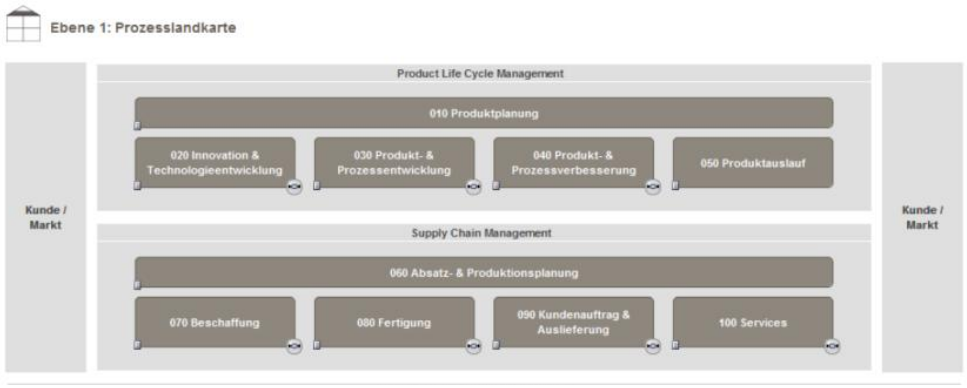


Figure 4 – Relationships between the security risk and safety risk management processes

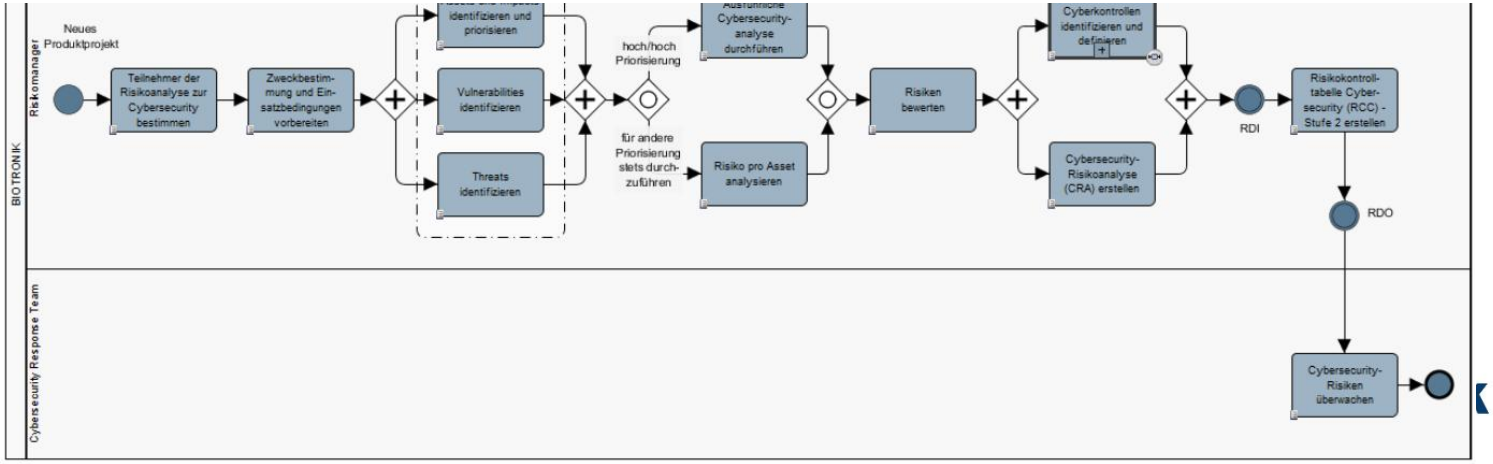
- Risiko Bestimmung Bedrohung → Verwundbarkeit → Lücke ist ähnlich zu Funktion → Gefährdung → Grund

BIOTRONIK
excellence for life

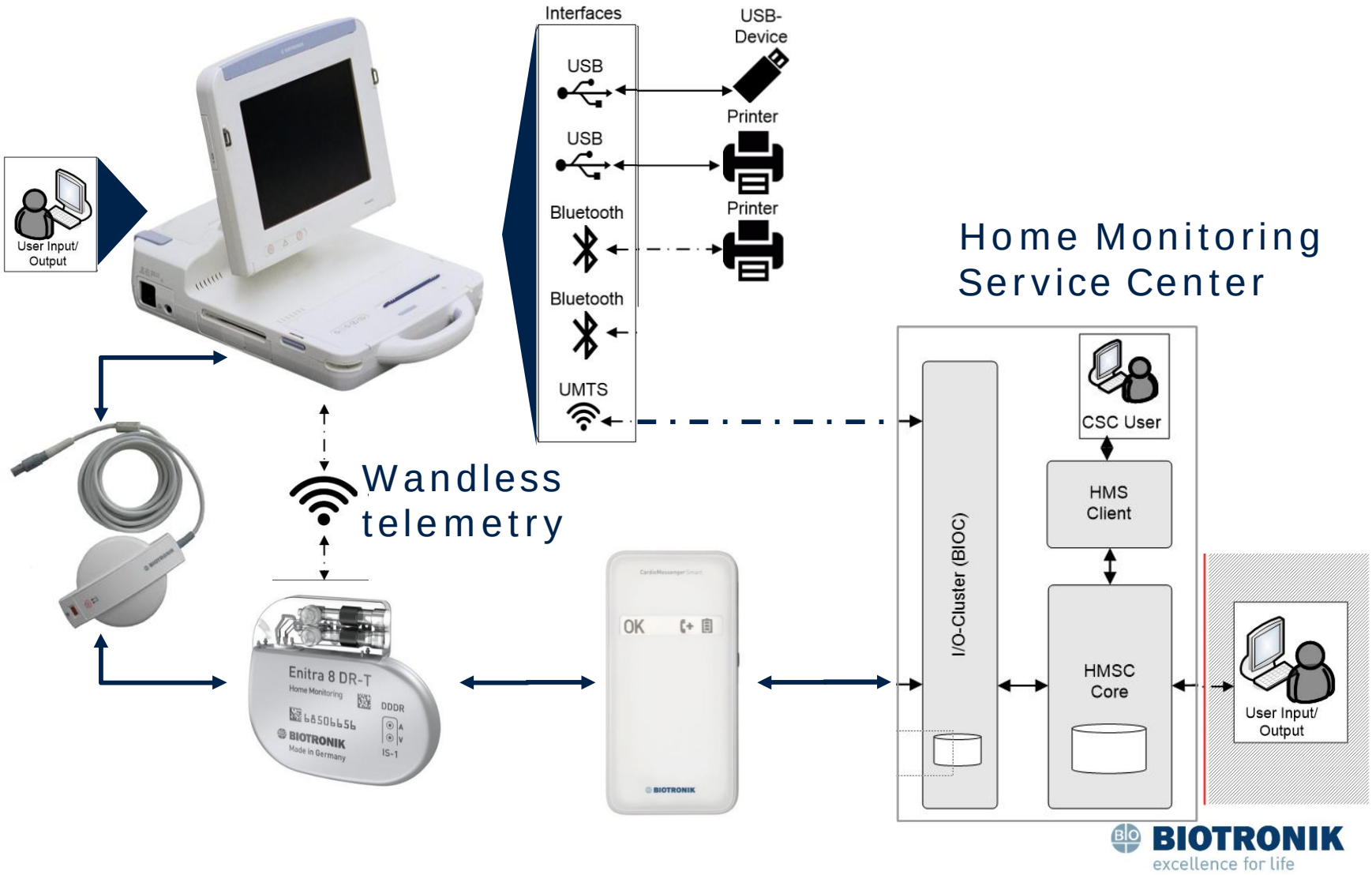
CS für Medizinprodukte im QM System ISO13485



Cyber Security ist ein Prozess



Cyber Security für Medizinprodukte
CS Werte bei BIOTRONIK



BIOTRONIK
excellence for life

Cyber Security für Medizinprodukte
BIOTRONIK Prozess zur CS Risikobestimmung

	Assets Werte	Threats Be-drohung	Adversary Interest Interesse des Gegners	Assess-ment Be-wertung	CS Risk Controls Maßnahmen
BIOTRONIK Prozess	Asset list in CRA*	STRIDE threat model**	CVSS Score***	CVSS Score	Risk Control in CRA
Beispiel	Wandless Telemetry	Spoofing identity Identitäts-täuschung	Medium (Short Range)	High	*Wandless telemetry* nur aktivieren, wenn (1) Spulentelemetrie aktiviert und (2) Schlüsseltausch erfolgt ist

* Cyber Security Risk Analysis
**https://msdn.microsoft.com/en-us/library/ee798544(v=cs.20).aspx
***https://www.first.org/cvss/

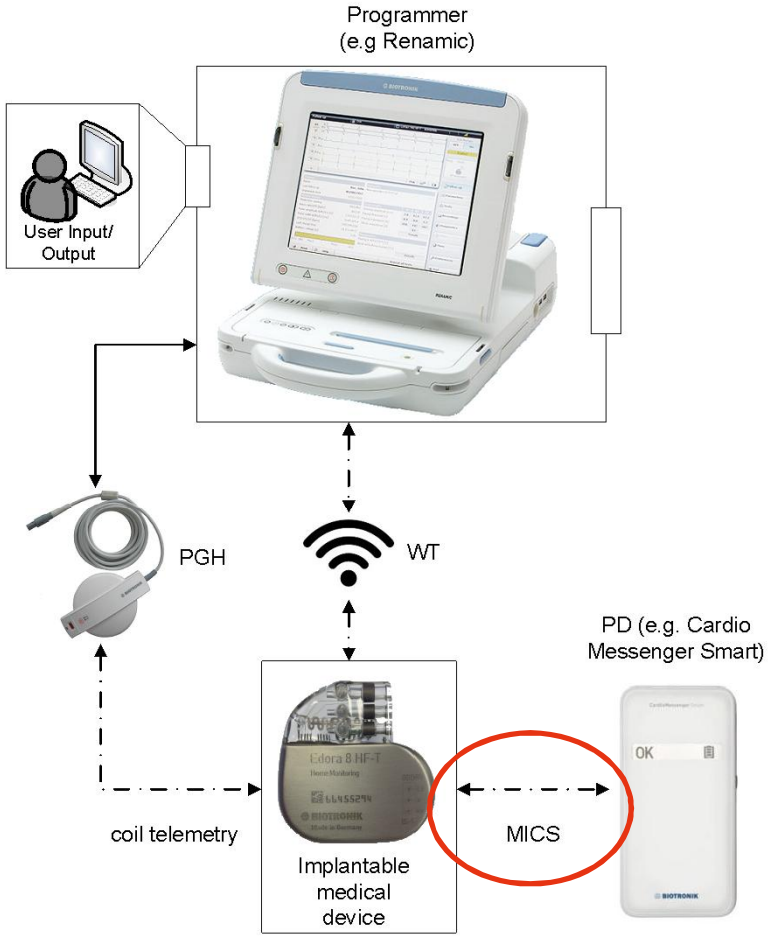
Cyber Security für Medizinprodukte in BIOTRONIK's QM System

- Betroffene Medizingeräte
- Vorhergesehener Gebrauch
- Umfeld
- Cyber Security Prozess
- Identifizierung der Assets / Werte
- CS Risikoanalyse
- CS Gebrauchsanweisungen
- CS Vorfall
  - Entdeckung
  - Reaktion
  - Wiederherstellung

QM = Qualitätsmanagement

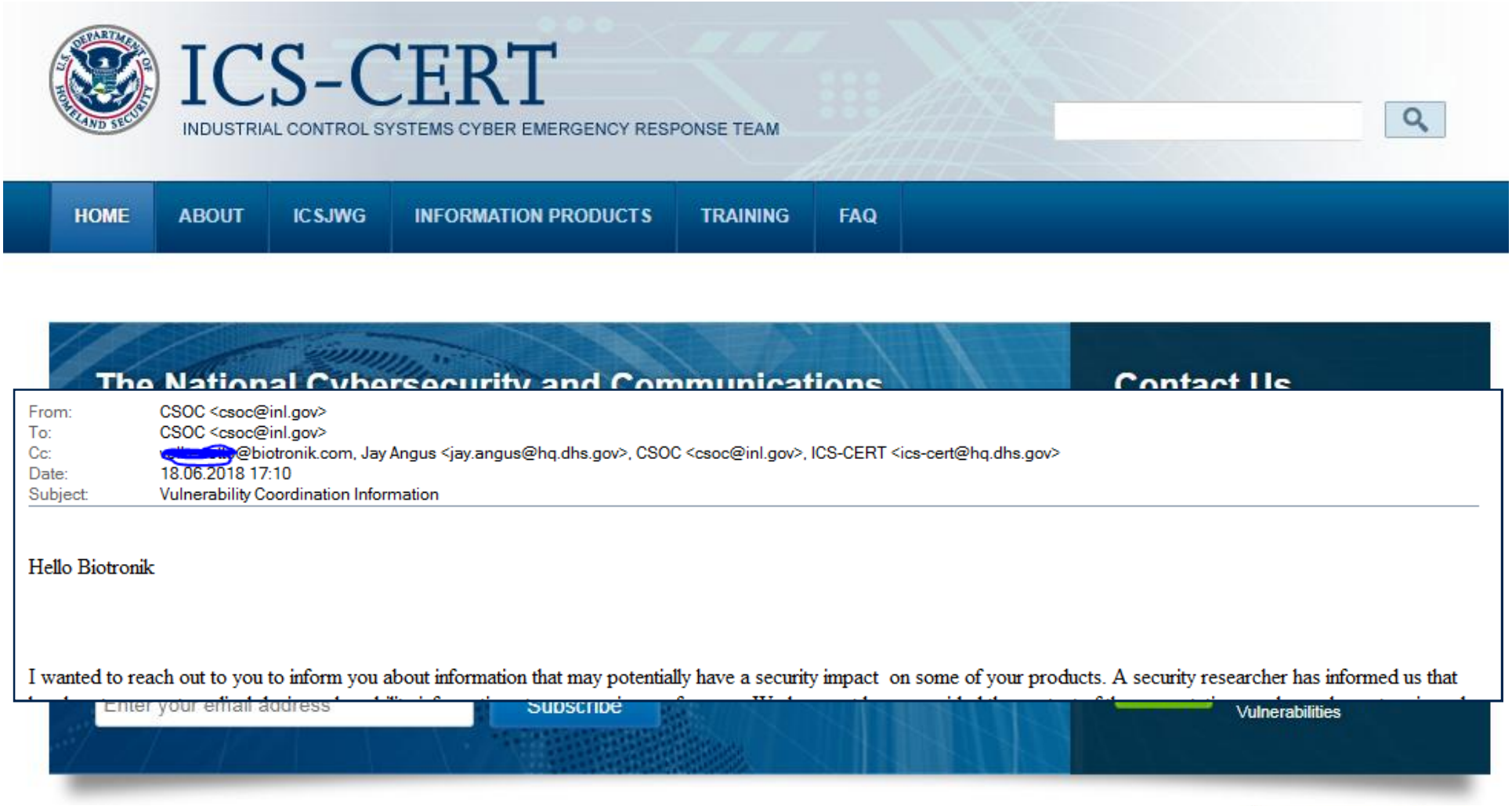
Cyber Security für Medizinprodukte
Risikokontrollmaßnahmen – Home Monitoring

- Home Monitoring
  - Risiko (beispielhaft)
    - Denial-of-service (Batterie leeren)
    - Identitätstäuschung (Parametereinstellung von einer unberechtigten Person)
    - Patientendaten lesbar
  - Kontrollmaßnahmen (beispielhaft)
    - Implantat kontrolliert Kommunikationsstart und -dauer (keine externe Initiierung)
    - Implantat kann durch HM nicht umprogrammiert werden
    - Verschlüsselung



BIOTRONIK
excellence for life

Prozess bei Cyber Security Vorfällen



BIOTRONIK
excellence for life

Prozess bei Cyber Security Vorfällen

- Personal bereitstellen
- Notfallteam festlegen
- Erreichbarkeit 24 / 7

BIOTRONIK
excellence for life

Weiterbildung

...mit Hilfe von Fachverbänden

Cybersecurity vulnerabilities of cardiac implantable electronic devices: Communication strategies for clinicians—Proceedings of the Heart Rhythm Society's Leadership Summit

David J. Slotwiner, MD, FHRS,[*,†] Thomas F. Deering, MD, FHRS, CCDS,[‡] Kevin Fu, PhD,[§] Andrea M. Russo, MD, FHRS,[¶] Mary N. Walsh, MD, FACC,[‖] George F. Van Hare, MD, FHRS, CCDS, CEPS-PC[**]

*From the *New York-Presbyterian Queens, New York, New York, †Cardiology Division, Weill Cornell Medical College, New York, New York, ‡Arrhythmia Center, Piedmont Heart Institute, Atlanta, Georgia, §College of Engineering, University of Michigan, Ann Arbor, Michigan, ¶Cooper Medical School of Rowan University, Camden, New Jersey, ‖St. Vincent Heart Center, Indianapolis, Indiana, and **Division of Pediatric Cardiology, Washington University in St. Louis School of Medicine, St. Louis, Missouri.*

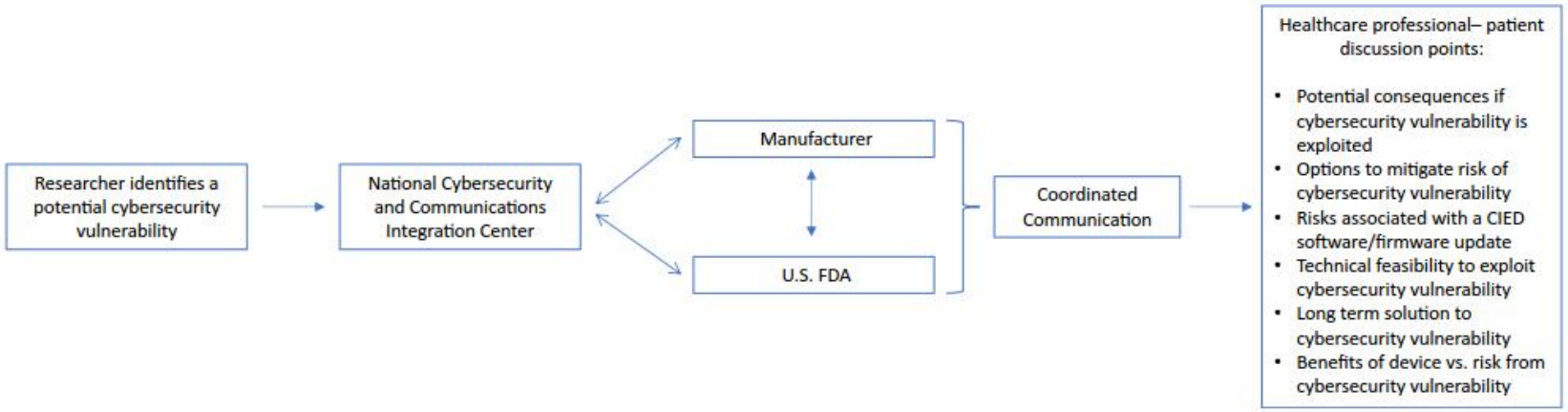


Figure 1 Evaluation and notification sequence of a new cybersecurity vulnerability threat: Assessment of a potential cybersecurity vulnerability requires expertise from the Department of Homeland Security's National Cybersecurity and Communications Integration Center and the manufacturer. The Federal Bureau of Investigation becomes involved if there is potential criminal activity. If the vulnerability is validated, the discussion between health care professionals and patients should consider these 6 topics. If the claim of a new vulnerability is released directly to the public, there will be a period of uncertainty and anxiety while the claim is being evaluated. FDA = Food and Drug Administration.

CS für Medizinprodukte bei BIOTRONIK
Zusammenfassung

BIOTRONIK Systeme haben keine unkontrollierten Risiken*

- BIOTRONIK hat einen adäquaten Cyber Security Prozess als Teil des QM Systems etabliert, das alle regulatorischen Anforderungen erfüllt und nach ISO27001 zertifiziert ist.

- Alle BIOTRONIK Produkte, die CS Relevanz haben, wurden vollständig analysiert und bewertet nach einem den Produkten angepassten Gefährdungsmodell und state-of-the-art CS Bewertungskriterien.

- Kontrollmaßnahmen wurden identifiziert, bewertet und umgesetzt. Diese sind verifiziert bezüglich Wirksamkeit. Spezifisch, alle Maßnahmen bezüglich Patientensicherheit sind im CS Bericht gelistet.

- Alle identifizierten Cyber Security Risiken sind somit kontrolliert.

* as of 09. Aug 2018

Danke für Ihre Aufmerksamkeit

BIOTRONIK
excellence for life