Your Regulatory Partner

Regulatory Summit 2022
Cybersecurity for Medical Devices

Nils Lidström & Per Sundström, Qadvis AB

UKRPA
UK Responsible Person Association

European Commission

sis STANDARD DEVELOPER 2019

SEK SVENSK ELSTANDARD

EAAR European Association of Authorised Representatives

Di GASELL

SWEDISH Medtech

QAdvis

A few of this week's headlines

Cyberkriget eskalerar – svenska företag i fara

Sjukhusen i Västerbotten förstärker säkerheten mot cyberattacker

FI ska föreslå åtgärder för stärkt cybersäkerhet

"Vi har en cybersäkerhetsskuld som vi inte betalat av"

QAdvis

Definitions

Cybersecurity

Application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks

Cyber attack

An attempt to disable computers, steal data, or use a breached computer system to launch additional attacks (including malware, phishing, ransomware, man-in-the-middle attack, or other methods)

QAdvis

Cybercrime is big business

- Estimated cost up from 6 trillion in 2021 to 10,5 trillion USD in 2025*
- Ransomware attacks on healthcare organizations estimated to quadruple from 2017 to 2021*
- More profitable than the global trade of major illegal drugs*

** 2022 Cybercrime Report from Cybersecurity Ventures*

QAdvis

Your Regulatory Partner

A few examples

QAdvis

Ransomware

First death reported following a ransomware attack on a German hospital

Death occurred after a patient was diverted to a nearby hospital after the Duesseldorf University Hospital suffered a ransomware attack.

- The patient, identified only as a woman who needed urgent medical care, died after being re-routed to a hospital in the city of Wuppertal, more than 30 km away from her initial intended destination, the Düsseldorf University Hospital.
- The Düsseldorf hospital was unable to receive her as it was in the midst of dealing with a ransomware attack that hit its network and infected more than 30 internal servers on September 10, last week.
- The incident marks the first-ever reported human death indirectly caused by a ransomware attack.

QAdvis

Spectacular device hack #1

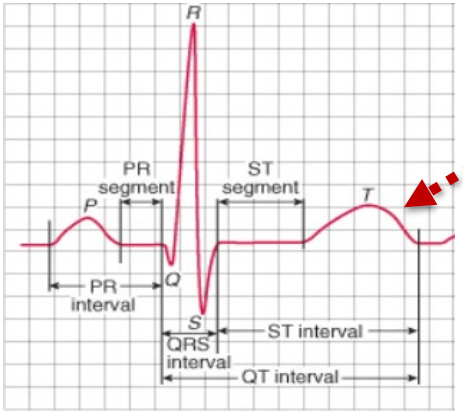
- FDA safety communication during 2017
- Implantable cardiac devices are vulnerable to cybersecurity intrusions and exploits

08/29/2017	Firmware Update to Address Cybersecurity Vulnerabilities Identified in [redacted] Implantable Cardiac Pacemakers	[redacted] released a firmware update to address cybersecurity vulnerabilities identified in [redacted] implantable cardiac pacemakers. The firmware update continues [redacted] efforts to mitigate confirmed vulnerabilities discovered by an independent research firm in 2016.
01/09/2017	Cybersecurity Vulnerabilities Identified in [redacted] Implantable Cardiac Devices and [redacted] Transmitter	The FDA became aware of cybersecurity vulnerabilities in these devices after an independent research firm released information about these vulnerabilities.

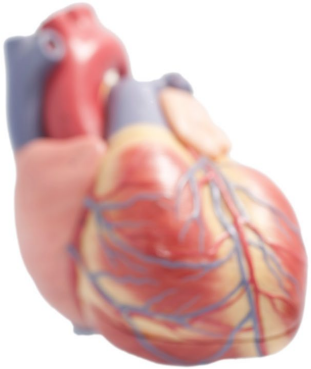
QAdvis

Spectacular device hack #1

- MedSec (the “independent research firm”) hacks the home transmitter during 2016
- Demonstrates with a pacemaker programmer
- Delivers “shock on T”



- Vulnerable period
- Induces ventricular fibrillation
- Used to test the device



Spectacular device hack #1

- Short seller Muddy Waters Capital, holds a short position in the pacemaker company
- Muddy Waters publishes the info
- Stock value drops for the pacemaker company
- Muddy Waters makes a profit
- Pacemaker company sues Muddy Waters

www.profitsoverpatients.com

Sök

Profits Over Patients

ABOUT CYBER SECURITY RESEARCH

Is your heart hackable?

Some implantable medical devices, such as pacemakers, defibrillators and resynchronization devices, can be hacked for malicious intent. If you have an implanted device made by and use the transmitter, this is for you.

In early January 2017, both the **Food & Drug Administration** and the **Department of Homeland Security** **issued warnings about the implanted devices made by**

At the same time, introduced a software patch to rectify the problem, **while we warned that this patch only fixed one of the most serious vulnerabilities.**.

QAdvis

Spectacular device hack #2

- IOActive researcher Barnaby Jack has reverse-engineered a pacemaker transmitter to make it possible to deliver deadly electric shocks to pacemakers within 30 feet and rewrite their firmware.
- Barnaby Jack:
  “Yeah, the software I developed allows the shutting off of the pacemaker or ICD, reading and writing to the memory of the device, and in the case of ICDs it allows the delivering of a high voltage shock of up to 830 volts.”

http://www.itnews.com.au/news/researcher-finds-pacemakers-open-to-deadly-hack-320156#ixzz3kfVi1atM

QAdvis

Different types of attacks affecting medical devices 1(2)

- Hijacking medical devices intending to harm patients
  - Devices can be disabled or be controlled to harm patients
  - Pacemakers, implantable defibrillators and insulin pumps
  - No real attacks have been publicly reported
  - High media interest (“It is a good story”)
  - Can even be connected to stock market manipulation ← $$$
- Ransomware attacks
  - Several reported attacks
  - Visibility of attack is high
  - Fast payback when ransom is payed ← $$$

QAdvis

Different types of attacks affecting medical devices 2(2)

- Healthcare data breaches
  - During 2021 appr. 2 data breaches with 500 records or more per day in the US
  - In 2015 Anthem Inc was breached and affected 78 million (!) individuals
  - Questionable payback, possibly using blackmailing ← $$$
- Theft of other types of data through medical devices
  - Credit card and health insurance credentials
  - Established value in the black market
  - Large scale thefts have been publicly disclosed
  - Mid-term value if used for other types of fraud ← $$$
- Denial-of-service attacks to disrupt hospital operations
  - Few reported attacks
  - Questionable payback, possibly using blackmailing ← $$$

QAdvis

Your Regulatory Partner

Cybersecurity frameworks

QAdvis

The cybersecurity universe

TÜV SÜD

UL 2900 series

Test houses

Guidances

Regulatory authorities

- EU: MDCG 2019-16
- FDA pre/post-market
- BSI (Germany)
- Health Canada
- CFDA (China)
- TGA (AUS)
- …

Government

NIST SP 800-series

NIST Cybersecurity Framework

Information security

Commercial

HITRUST framework

Standards

ISO 27000 series

Information security

Industrial automation

IEC 62443 series

IEC 81001-5-1

Security lifecycle Process requirements

IEC/TR 60601-4-5

Product requirements

NEW

IEC TR 80001-2-x

Risk management for IT-networks incorporating medical devices

MDS²

Industry organizations

ISO 14971

AAMI TIR-57/-97

Medical sector Risk management

QAdvis

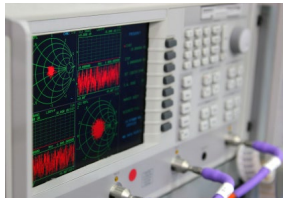
The Trinity

Development process

Secure development lifecycle
IEC 81001-5-1

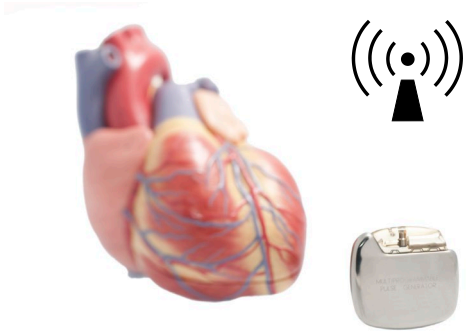
Product properties

Security requirements
IEC 60601-4-5



Secure infrastructure and organization

Information management system
ISO 27001



IEC 81001-5-1

Health software and health IT systems safety, effectiveness and security
Part 5-1: Security - Activities in the product life cycle

- Transposition of the Industrial Automation standard IEC-62443-4-1
  - Security for industrial automation and control systems - Part 4-1: Secure product development lifecycle requirements
- Complements IEC 62304 with tasks related to cyber security

QAdvis

Which processes are affected?

- Risk management
- Software development
- Customer complaints
- Incident reporting
- Supplier management

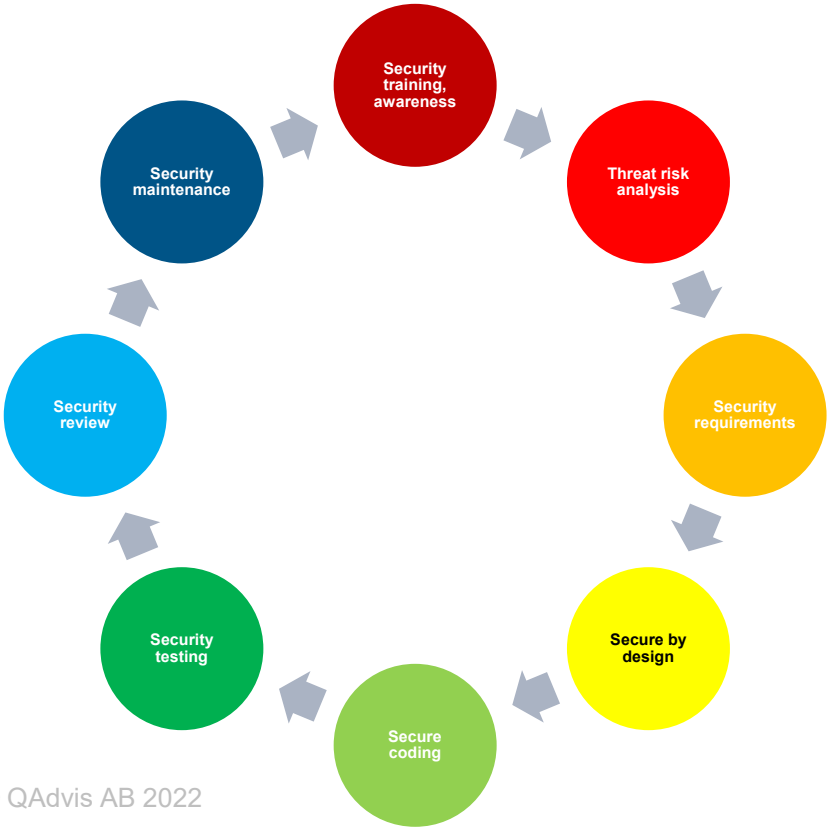
- New: Vulnerability management

QAdvis

Secure product lifecycle

Security related tasks during the entire product life cycle

- Security-focused risk analysis
- Security best practices
- Secure coding standards
- Static code analysis
- Penetration testing
- Track vulnerabilities
- Monitor supply chain vulnerabilities
- …



Your Regulatory Partner

Outlook for the future

QAdvis

Drivers shaping the future of healthcare*

- The need to act agile
  - Cybercrime actors are not resting, and manufacturers must adapt
- Ecosystem coordination
  - Collaboration with vendors and business partners requires new solutions
- Increase in number of devices
  - Smart sensors, health wearables must be registered and linked to consumers
- Data explosion
  - With lots of devices, lots of data and lots of sharing, data privacy becomes high(er) priority
- Artificial intelligence
  - Protection against counterfeit functionality, malicious model manipulation, malicious training
- Usability
  - Cybersecurity solutions must be manageable by consumers and healthcare users

** The future of cyber in the future of health – Deloitte, 2022*

QAdvis

Cybersecurity is not an optional feature

- The world, including health care, is digitalized
  - Development accelerated by the Covid-19 pandemic
- Cybercrime costs expected to increase with 15% per year*
- Act now, don't sit on your hands
  - Use the standards and tools that are available
  - Focus on risk management, not just compliance
  - Build a team with skills that go beyond traditional "security thinking"
  - Effectively integrate security and privacy capabilities
  - Identify ecosystems of partners to collaborate with

** 2016 Cybercrime Report from Cybersecurity Ventures*

QAdvis

QAdvis

Your
Regulatory
Partner