Federal Office
for Information Security

RECOMMENDATION: MANUFACTURERS

Cyber Security Requirements for Network-Connected Medical Devices[1]

1 Introduction

Many medical devices follow the trend towards digitization, and offer an option to operate with other devices over an information network. This often involves the use of technologies that have already been proven to be effective in other areas. Manufacturers have to pay special attention to the resulting cyber security challenges while considering the specific conditions for medical devices, such as long product life cycles and the intended use in areas that are directly critical to patient safety. Therefore, this document summarises best practices for manufacturers of network-connected medical devices. These recommendations accompany regulatory requirements and are intended to support implementation and maintenance at an appropriate level of cyber security according to the current state of the art.

In order to meet one of the essential requirements of the Medical Device Directive[2] currently in force, manufacturers must perform a risk analysis during the conformity assessment procedure. The identified risks must be minimised and documented. This cyber security recommendations provide practical assistance on how the therein identified cyber security issues can be reduced in detail.

Since the generic term "Medical Devices" cover a large number of different products, this document has a very generic structure. Instead of providing specific instructions which may not be applicable in the same way to all products, the sections below deal with questions related to cyber security within each area that has an impact on such devices. These questions are designed to enable manufacturers to produce the instructions necessary for their devices.

This document differentiates between the following operating modes:

A) Medical operation mode according to intended medical purpose
In this operating mode, the product is being used for its intended medical purpose.

1 This document was derived from the cyber security recommendations “Requirements for Network-Connected Industrial Products” (https://www.allianz-fuer-cybersicherheit.de/dok/6603528) and contains many of the suggestions already described therein. It was created in close cooperation with the Medical Engineering Division of the German Electrical and Electronic Manufacturers’ Association (ZVEI) and the Federal Institute for Drugs and Medical Devices (BfArM).

2 Council Directive 93/42/EEC

B) Configuration of the device
In this operating mode, the device is being configured for its medical purpose. This includes both cyber security configurations that ensure a secure technical operation as well as the settings necessary for medical operation mode (for example, parameters adapted to the patient).

C) Technical maintenance
In this operating mode, updates from the manufacturer or third-party providers are being installed and necessary basic calibrations or adjustments are being made.

From a cyber security point of view, however, there is no clear separation among these operating modes. If for example malware has been installed on a software-supported device in technical maintenance mode this can have an impact on the mode of medical operation mode according to the intended medical purpose, even if the device has no network-connection in this mode. For this reason, all recommendations are always valid in all operating modes. This document only differentiates among operating modes to enable manufacturers to discern the purpose of the recommendations more easily.

From an IT security point of view, manufacturers must take as a basic principle all possible precautions to provide IT security for their devices according to the current state of the art. However, it will not always be possible to implement all the recommendations listed in the sections below – for example, if a cyber security measure would have a negative impact on patient safety. In this case, a rationale for the decisions must be given and after a detailed risk analysis an alternative solution must be provided which protects against the existing threats. It is important, that the required security measures must not have a negative impact on the safety functions of the medical devices and therefore on the lives of patients.

2 Organisational Measures

2.1 Product life cycle

Establishing a secure development life cycle fundamentally improves the security of a product. The questions below offer some guidance in this context.

- Are there consistent and mandatory development policies for a secure implementation that reflect the current state of the art? These may include the following:
  - Policies for selecting and configuring trustworthy tools
  - Policies for separating software units
  - Policies for using secure programming techniques and tools.
- Are cyber security threat and risk analyses made regarding
  - system boundaries
  - intended purposes
  - the intended operating environment

  and are corresponding countermeasures specified and implemented?
- Are mandatory security gates defined in which for example a software review or a holistic cyber security assessment is made?
- If technically feasible, are automated code reviews an integral part of the development cycle for software components?

- Are targeted searches for known vulnerabilities (such as buffer overflows and unhandled exceptions) performed on software components during the development process? Are there also additional precautions which prevent code from being executed within memory areas that are not intended for this purpose?
- Are technical security analyses (penetration tests) made on the products? Do this include efforts to identify unknown vulnerabilities, as well? Are checks performed for unknown vulnerabilities (e.g. through fuzz testing) or for alternative entry points (e.g. by reading hidden files, configurations, data streams, or hardware registers)?
- Is a final purge performed on the product to ensure that it doesn't contain test code or undocumented entry points?
- Are processes established for handling vulnerabilities in operating systems, third-party and in-house developed components? Such processes include the following:
  - The vulnerability assessment, including its impact on in-house products (in different versions, if necessary)
  - The specification of countermeasures
  - The remediation or mitigation of the vulnerability
- Are additional cyber security precautions (such as application whitelisting or anti-virus solutions) taken into consideration from the beginning of the design phase (e.g. by including them into certification) instead of being forbidden (by excluding the warranty, for example)?
- Are there consistent rules for handling vulnerabilities after the product is delivered? Have appropriate response times and emergency procedures been defined (cf. BSI's recommendation on vulnerability handling[3])?
- Are products provided with patches and updates (or compensatory countermeasures) as quickly as possible over a sufficient time period in order to eliminate detected vulnerabilities, or at least mitigate their consequences? Is the update process as simple and efficient as possible for customers?
- Are updates, patches, and workarounds tested prior to release? Is it guaranteed that users can continue to use the devices for their intended purposes?
- How does the manufacturer deliver updates, patches, and other software required to run the product? Is the supply chain sufficiently secured for updates, patches, and other software required for operation (e.g. by using signatures to ensure authenticity and integrity)? Has the download portal been tested for security vulnerabilities, whereby the content could be changed or manipulated (WebCheck[4])?
- Are processes in place that define which log data is collected and how it is analysed? Are there specifications which log entries are requiring a response?

Specific assistance regarding the requirements that should be taken into account for a secure development process can be found (for example) in the NIST Special Publication 800-160[5] or in IEC 62443-4-1[6].

3 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_019E.pdf
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/

2.2 Communication

Vulnerabilities in IT products are being identified on an almost daily basis. Manufacturers are responsible for providing appropriate information on how their products may be affected. Providing related patches and other compensatory countermeasures (for example, deactivating a service) help keeping products secure. Manufacturers of medical devices are being obliged[7] to carry out the corrective measures provided and communicate the corresponding recommendations to their users in a comprehensible and effective manner. They must also ensure the proper implementation of the precautions and monitor their effectiveness.

The following questions include some matters to be considered regarding the practical implementation of these policies:

- Is information, particularly with regard to product cyber security, communicated as openly as possible? Is a policy to do this already been implemented?
- In case vulnerabilities were detected in products, have processes for communicating with third-party providers been defined?
- Have contact persons/-entities been specified to address cyber security questions/incidents (to ensure coordinated disclosure)?
- Do the processes for detecting, reporting, and assessing/handling potential incidents related to the security (safety, protection against threats) of patients, users, and third parties also consider cyber security questions? Are relevant criteria and reporting channels established in this regard, both internally and for working with customers?
- Do the safety-incident reporting processes also take cyber security incidents into account? Are relevant criteria and reporting channels established in this regard internally and for working with customers? Note: Such processes typically cover detecting, reporting, and assessing/handling actual incidents involving the safety of patients, users, and third parties as required by law (e.g. German MPSV[8]). These processes typically include reporting to relevant authorities, e.g. to the federal authorities responsible for medical devices, which in Germany usually is the Federal Institute for Drugs and Medical Devices, BfArM)?
- Is there a consolidated tracking system (e.g. within the quality assurance system) that collects information from different communication channels – such as hotlines, support or other panels – which may provide indications on cyber security related events, vulnerabilities, or other incidents concerning medical devices (e.g. messages such as “A .dll file was replaced on my system”) that must be reported according to law (e.g. MPSV)?
- Are customers being informed, how critical certain patches are for product security and for the intended use of the product?

3 Product Features

A secure operation of medical devices according to the point of view of cyber security can only be guaranteed if the devices have cyber security features pursuant to the intended purpose and if cyber security measures can be ensured by the operator. The section below describes cyber security requirements for the product features of network-connected medical devices. The various aspects of cyber security can be grouped by different criteria in order to achieve a

7 In Germany according to Section 14 of Germany's Medical Devices Act (MPSV)
8 Ordinance on the identification, assessment, and prevention of risks presented by medical devices (https://www.gesetze-im-internet.de/mpsv/index.html)

structured approach. On the one hand, there are specific recommendations for some operating modes that can be considered separately; on the other hand, it is possible to differentiate between cyber security recommendations that guard against given security incidents or cyber security measures designed to detect and assess incidents that have already occurred. The technical documentation is a separate topic that covers all the cases.

3.1 Cyber security recommendations for all operating modes

The first step is a systematic threat and risk analysis to identify the interfaces of the product and the therefore resulting threats to which it is exposed. For a network-connected medical device, this entails:

1. Documentation of all interfaces
2. Determining the maximum damage that can be caused by attacks via each interface

The following questions should be asked in this step:

- What interfaces does the product have? What happens if the interfaces receive unexpected signals?
- What other components can be connected? What happens if wrong components are connected?
- How are the components connected (for example, via Ethernet, a wireless connection, USB, or another plugged-in signal line)? What risk(s) does the deployed technology bear?
- In which direction does the data/signal flow? Can data also be transferred in other directions?
- What data/signals are being transmitted? Can the data/signals be changed, deleted, or new data be added? How is the data protected from unauthorized access?
- What related risks (probability of occurrence and damage potential) can arise for patients, users, or third parties (risk analysis of the medical device)? Are these risks[9] acceptable, or are mitigating measures required?

The second step involves defining cyber security-specific product features that reduce the risks identified in the first step according to the state of the art. The following questions can be used for this purpose:

- Cyber security measures to protect data/signals
    - Has the deployed operating system, including all the applications in use, been subject to an essential system hardening? Are only operationally essential applications being used, or does the documentation advise users (for example) to deactivate the applications that are not required in their particular scenarios? Are secure, established versions of specific common protocols in use where available? (SSH instead of Telnet, for example, or HTTPS instead of HTTP)
    - Are only those technologies being used that can be protected according to the state of the art?
    - Have the implementation of communication protocols been tested in terms of its fault tolerance and robustness?

9 According to DIN EN ISO 14971

- Is the use of standard implementations preferred to in-house development of services and protocols?
- Has sensitive data been protected during transfers and storage?
  - Have generally accepted algorithms and standard implementations for cryptographic procedures been used rather than in-house developed variants?
  - Is BSI Technical Guideline TR-02102 (on cryptographic methods[10]) met during the implementation and use?
  - Are integrity checks in place, especially for data that can affect safety?
  - Have all interfaces to the device been secured with sufficient input validation to prevent manipulation?
- Has the network been designed to be operated hardened?
  - Have the networks which are part of the product been segmented by default, or is information available for users on how to operate the network segmented? Is configuration data kept separate from the device's medical functions?
  - Is it possible to deactivate certain services (HTTP(S), FTP, etc.) and technologies (e.g. WLAN, Bluetooth) if users do not need them for their particular scenarios?
  - Have all deployed services (for example, HTTP/HTTPS) and technologies (e.g. WLAN, Bluetooth) been hardened to the greatest possible extent according to the state of the art, or are users given information on how this can be achieved?
- In cases of client/server configurations, are these configurations operating secure according to the state of the art?
  - Will all parameters that are used as cyber security measures (such as session cookies) be calculated or be validated on the server side?
  - Will all client input be validated on the server side?
- Is a granular access control (login/authentication) in place to protect sensitive data from unauthorized access? Are sufficient user management mechanisms in place (e.g. multiple users with different roles and authorisations)?
  - Will credentials (especially passwords) be stored in an encrypted manner according to the state of the art rather than as plain text?
  - If a login fails, will the resulting error message be of a general nature – such that it does not specify for example that the username was correct while the password was incorrect?
  - Is it possible to restrict access via the network interfaces to specific MAC addresses, IP addresses or IP-ranges?
  - Are any additional mechanisms in place that ensure security when an operator intervenes (such as the dual-control principle)?
  - Are there applications or processes running with system privileges? Are they protected against attackers?
- Is secure session management in place when several persons have access?

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

        - Is it technically ensured that critical functions can only be executed with the required rights?
        - Are different sessions being protected among each other during operation?
        - Do sessions time out, or can they be configured to do so?
        - Are measures in place that make it difficult to perform a denial-of-service attack by opening many connections or sessions?
    - Other cyber security functions
        - In cases where malware poses a risk, have detection and protection measures been established?
        - In case of a denial-of-service attack, are measures in place that will preserve the basic functionality of the component and ensure its ability to resume normal operations with full functionality after the attack?
        - Have update mechanisms (e.g. for firmware updates) been sufficiently secured, especially in case of those that are being made via a network instead of locally on the device? In addition to integrity checks using checksums, it is particularly necessary to provide appropriate authentication or protection via signatures.
        - Are secure, user-friendly mechanisms or corresponding interfaces available and documented for standard backup and restore procedures?
- Cyber security measures for detecting attacks
    - Logging
        - Will all critical actions – such as configuration changes, failed login attempts, the removal or replacement of storage media, or USB device connections – be logged?
        - Are measures in place to prevent unprotected access to critical or confidential information (e.g. login or patient data) via log data?
    - Evaluation of log data
        - Is it possible to automatically trigger an alarm in case of critical system events or states?
        - Are warning messages issued if a brute force attack occurs on a login mechanism?

3.2 Cyber security recommendations for product configuration

Configuration options are particularly important to a component's cyber security because they are used among other aspects to control and parametrize security mechanisms. The following central questions must be taken into account.

- Is authentication required prior to modify the configuration?
- Is the delivered configuration “secure by default”?
- Are the credentials, certificates, etc. changeable for all services?
- Is the configuration protected against unauthorized manipulation (e.g. by checksums or cryptographic signatures)?

- In cases where standard IT is being used for configuration interfaces, is it sufficiently protected? Have the available recommendations and technical guidelines been implemented properly? If, for example, a web interface is being used, will the connections be made available exclusively in encrypted form? Is compliance with the BSI's minimum requirements on the use of TLS[11] ensured, and are such web servers operating according to the cyber security recommendations for secure web server operations?[12]
- Is there an automatic logoff process that prevents unauthorized persons from making configuration changes in case someone forgot to log out?

3.3 Cyber security recommendations for maintenance operations

As with any technical equipment, medical devices require maintenance. Depending on the intended purpose, it may e.g. be necessary to calibrate devices or install related updates.

- Have all interfaces that are used for maintenance purposes been protected against unauthorized access?
- If remote maintenance is performed, are measures in place to ensure that the components being used for this purpose do not affect the device's actual operation in any way?
- Will remote maintenance or write access to a device or component only be possible if it is explicitly activated for a limited time and with an explicit authorization (e.g. through activation or confirmation)?

3.4 Technical documentation

In addition to the manual for the medical device, the technical documentation for installation, configuration of the device as well as the technical requirements for their operating environments are particularly important for a safe and secure use by the customer.

The following questions are suitable as an orientation guide for preparing and checking technical documentation on cyber security issues.

- Will IT personnel on the user side be provided with technical documentation that clearly illustrates how to operate the device in a technically secure manner?
- Are target groups specified which are to be informed about specific technical information related to cyber security?
- Does the documentation contain information that customers can use as a basis for creating an IT security concept?[13]
    - Have all interfaces, access points and functions been documented?
    - Have the component's cyber security features and functions been described?
    - Does the documentation identify the risks/threats which are covered by the component itself?
    - Have those threats been documented that should be considered in the context of a cyber security assessment or cyber security management?

11 The minimum standard https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_BSI_TLS_1_2_Version_1_0.pdf has been published for German federal authorities. We recommend implementing these requirements in the area of network-connected medical devices, as well.

12 Further recommendations – especially for an HTTP(S) interface (web interface) – are found in the BSI recommendation "Development of Secure Web Applications"; the "Development Phase" section is particularly relevant.

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

  - Does the documentation also cover countermeasures for relevant threats ?
  - Does the documentation cover the services which cannot be secured (with the mechanisms integrated in the product) and thus require additional technical or organisational cyber security measures?
- Are there any recommendations regarding configurations that ensure secure operations (e.g. a guide for hardening the system)? For example:
  - Is there sufficient information on changing default passwords and deactivating unnecessary accounts?
  - Does a checklist exist to help maintain an overview about the configuration and its cyber security-specific implications? Are the cyber security-specific consequences of the possible configuration options/alternatives documented? Is there any indication of the settings which are to be considered critical and may lead to increased risk?
  - Are there references to further information on security measures or for secure operations?

Additional useful information regarding information and guidelines to be considered in the context of the basic requirements of medical devices, the relevant harmonised standards and the legal reporting obligations for manufacturers, operators, and professional users of medical devices can be found (for example) on the websites of the Federal Institute for Drugs and Medical Devices (BfArM).[14]

Additional useful requirements to be considered in the context of IT security requirements for individual devices or technologies can be found, for example, in IT-Grundschutz[15] and the cyber security recommendations of the BSI[16].

By means of the BSI publications, the Federal Office for Information Security (BSI) publishes documents about current topics in the field of cyber security. Comments and advice from readers can be sent to **info@cyber-allianz.de**.

14 https://www.bfarm.de/EN/Home/home_node.html
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