ZVEI:
Die Elektroindustrie

Position Paper

Secure Medical Subnetworks

January 2017

German Electrical and Electronic Manufacturers' Association

Networking Medical Devices

Networked medical devices use clinical IT networks to communicate orders, messages, images and reports, for example. Operating errors, misuse, malware and attacks can disrupt not only this communication, but also the essential functions of the medical device, depending on the device. Under certain circumstances, incidents of this kind can even interfere with the safety of the medical device, even if its manufacturer implemented the appropriate measures derived from the risk assessment during the development process.

Although the regulatory framework places specific obligations on manufacturers of networkable medical devices in the context of their analysis, such manufacturers are largely limited to technical solutions in individual networked components. The effectiveness of such technical measures always depends on a suitable environment and proper use that is, on people and processes. These, in turn, can be influenced only by the operator.

This paper describes the measures that can be implemented by medical engineers or clinical IT experts, acting as network administrators, in order to network medical devices securely. The present specification describes protective measures in accordance with IEC 80001 that can be taken by the operator for this purpose. It thus remains independent of platforms and manufacturers, and attempts to be technology-neutral wherever possible.

In this context, "information security" is understood to mean risk management in order to counter unauthorised and undesired scenarios in clinical IT networks.

The structure of this specification is based on the "cybersecurity framework" created by the American National Institute of Standards and Technology (NIST), which separates the technical and procedural elements needed to achieve the objectives into the following steps.

- Identifying risks
- Protecting IT assets
- Recognising incidents
- Responding to and recovering from incidents

Using this list, operators define key implementation steps based on their own priorities and the expected types of incidents. In the simplest case, this specification can be used as a checklist.

Security process

The standard IEC 80001-1:2010 identifies the fundamental responsibility of clinic management for the secure operation of its network. Similarly, in accordance with clause 14.13 of IEC 60601-1, the manufacturer of the networked medical device establishes that the operator is responsible for the influence of the network on the safe operation of the device. However, neither of these standards provides a coordinated, practical list of protective measures for medical devices.

The defensive measures listed below cannot replace a fundamental security process on the part of the operating organisation. Technical measures can only ever be effective if the operator uses the devices in a secure, responsible manner as part of a security process (for instance, in accordance with one of the following standards: ISO/IEC 27002, ISO 27799, IEC 62443, BSI IT-Grundschutz (baseline protection)). In addition to the defensive measures described below, these comprehensive elements are defined, for example, by a security process in accordance with ISO 27799 (as a translation of ISO/IEC 27002 for clinical IT networks).

- Company information security policy
- Analysing the extent of damage caused by incidents
- Organising information security
- Information security procedures
- Information security tools and software
- IT acquisition
- Personnel policy, selection and management, and contractual conditions
- Supplier management
- Physical access constraints (buildings, rooms, authorisation concept)
- Compliance
- Monitoring, improving and auditing the security system

Furthermore, "incident management" is established, in which responsibilities and procedures for defending against and dealing with unauthorised and undesired incidents are determined.

- Responsibilities and procedures for planning damage prevention
- Responsibilities and procedures for reacting to incidents
- Responsibilities and procedures for recovery

Operating secure medical subnetworks

Medical engineers and clinical IT administrators who wish to operate networked medical devices in a secure medical subnetwork are the primary target groups of this specification. Depending on the organisation, it can be useful to establish one or more secure medical subnetworks.

1. IDENTIFY: Recognition and classification of protected IT assets

IT inventory: The operator draws up a directory of IT assets (data, servers, workstations, services, applications) that are important to the medical subnetwork in question. Classification also includes precise details of the associated organisation and information regarding operational responsibilities.

Example of a radiology subnetwork: Imaging modality, RIS server, possible HIS interface (ADT, ORU), RIS workstations.

Classification according to criticality: The operator documents devices and relevant IT applications in the particular medical subnetwork and classifies them according to their criticality (for instance, according to their response times or risk potential).

Example: On a three-level criticality scale (planned/critical/real-time), radiology is deemed "time-critical" because it also supports emergency care. For this reason, the function of all applications and devices function is time-critical (intermediate level), with only the modality being a potential source of risk.

The classification is indicated by labeling the devices, operator interfaces and technical identifiers.

Responsibilities: The operator documents

a) responsibilities and procedures for the set-up and operation of the medical subnetwork in question.
b) non-disclosure agreements or contracts relating to the handling of confidential data and devices.

Example: The "medical engineering expert" role takes on the task of administering the radiology subnetwork. The network is self-contained, with the exception of defined, protected interfaces.

2. PROTECT: Restricting access to the relevant protected assets

Using the following measures, operators can reduce the probability of an incident.

Organisational protective measures

- Requirements and policy for access protection
- Informing and training personnel
- Stipulations for installing devices, memory and consoles (incl. mobile use)
- Rules for data- and device-handling
- Disposal regulations for data carriers and devices with data storage
- User management (login, role-based permissions)
- Simulated attacks
- Rules for installing, storing, transferring and destroying removable storage devices
- Documentation of procedures, as well as of the configuration of applications, systems and networks, maintenance procedures and maintenance tasks

Technical protective measures

- Separating medical subnetworks using firewalls
- Physically protecting the secure, separate cabling and installed devices
- Deletion procedures for data carriers and devices with data storage
- Technical access protection for accounts (login with restricted permissions)
- Technical restriction of the installation and use of unknown interfaces, devices, software functions and IT tools
- Virtualisation of particularly exposed applications such as e-mail and Internet browsers, in secure environments ("container", "sandbox", "secure compartment", "virtual client")
- Technical restriction or protection of interfaces (USB, Wi-Fi, NFC, file sharing, etc.)
- Encrypting data and messages
- Restricting communication to known (authenticated) nodes and applications
- Systematically updating security for platforms, middleware and applications

3. DETECT: Detection and evaluation of unauthorised or undesired activity

Organisational measures help operators to improve recognition of unintended activity in secure subnetworks.

- Learning process to update suspicious anomalies
- Maintenance of a list of suspicious anomalies that indicate an incident

Operators can recognise unintentional activities in subnetworks using technical measures:

- Monitoring functions to recognise and assess incidents (e.g. firewall)
- Recording events, admin/user log files, protecting log files
- Technical capability to update the list of (and rules for) suspicious anomalies

4. RESPOND: Response to unauthorised or undesired scenarios

Operators can use organisational measures to limit the damaging effects of unauthorised or unintentional activities in secure subnetworks:

- Documenting analysis methods (how severe is the incident?)
- Documenting response procedures (collecting evidence; what is the response?)
- Improving processes by learning from analysis and response

Technical procedures support the organisational measures:

- Establishing technical restrictions and defensive procedures (firewall "stop all" function)
- Establishing technical notification paths

5. RECOVER: Establishing procedures to restore the data and functions of the secure medical subnetwork after an attack

Technical measures enable operators to compensate for the damage after unauthorised or unintentional activity in the secure subnetwork.

Organisational restoration measures:

- Documenting security and restoration procedures
- Improvement process for the above procedures
- Preventive drills for severe outages ("disaster recovery").

Technical restoration measures:

- Scripts/services to secure identified data. This should systematically omit malicious code and corrupted data
- Measures to protect archived data stores, for instance, by revoking write permissions
- Scripts/services to restore secured data. This should systematically avoid retrieving malicious code and corrupted data from the backup
- Redundant platforms for critical applications

Notes

It is the responsibility of the operator to ensure the continued functioning of the networked medical devices when implementing the above measures. The instructions for use from the relevant manufacturer are crucial to this effort.

Although technical security measures (for instance, in networked medical devices) can increase response times and reduce throughput, they should not be bypassed or deactivated by the operator.

The above list can never be exhaustive. In the future, there may be unforeseeable attacks or new types of attacks that cannot be prevented using the above measures. Additional measures may become necessary.

The measures described can in no way replace a comprehensive IT security process on the part of the operator, for instance in accordance with ISO/IEC 27002 or ISO 27799.

References

BSI: IT-Grundschutz (baseline protection) Standard 100-2: IT-Grundschutz (baseline protection) Methodology – Bundesamt für Sicherheit in der Informationstechnik (BSI – German Federal Office for Information Security), Bonn, 2008

Canavan J. E.: Fundamentals of Network Security, Artech House Publishers, Boston, 2001

NIST: Framework for Improving Critical Infrastructure Cybersecurity, NIST, also available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf, 2014

ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security management. Geneva, ISO, 2013

ISO 27799:2016: Health informatics – Information security management in health using ISO/IEC 27002. Geneva, ISO, 2016

IEC 62443-3-3:2013: Industrial communication networks – Network and system security – Part 3-3: System security requirements and security levels, Geneva, IEC, 2013

IEC 80001-1:2010: Application of risk management for IT-networks incorporating medical devices – Part 1: Roles, responsibilities and activities, Geneva, IEC, 2010

ZVEI - German Electrical and Electronic
Manufacturers' Association
Medical Engineering Division
Lyoner Strasse 9
60528 Frankfurt am Main, Germany

Contact:
Hans-Peter Bursig, ZVEI
Phone: +49 69 6302-206
E-mail: bursig@zvei.org
www.zvei.org

1st edition, January 2017

The creation of this flyer was managed by the Medical IT & Communication Systems (MICS) working group in the Medical Engineering Division of ZVEI.