ZVEI:
Die Elektroindustrie

Position Paper

IT Security in Medical Technology and Hospital IT

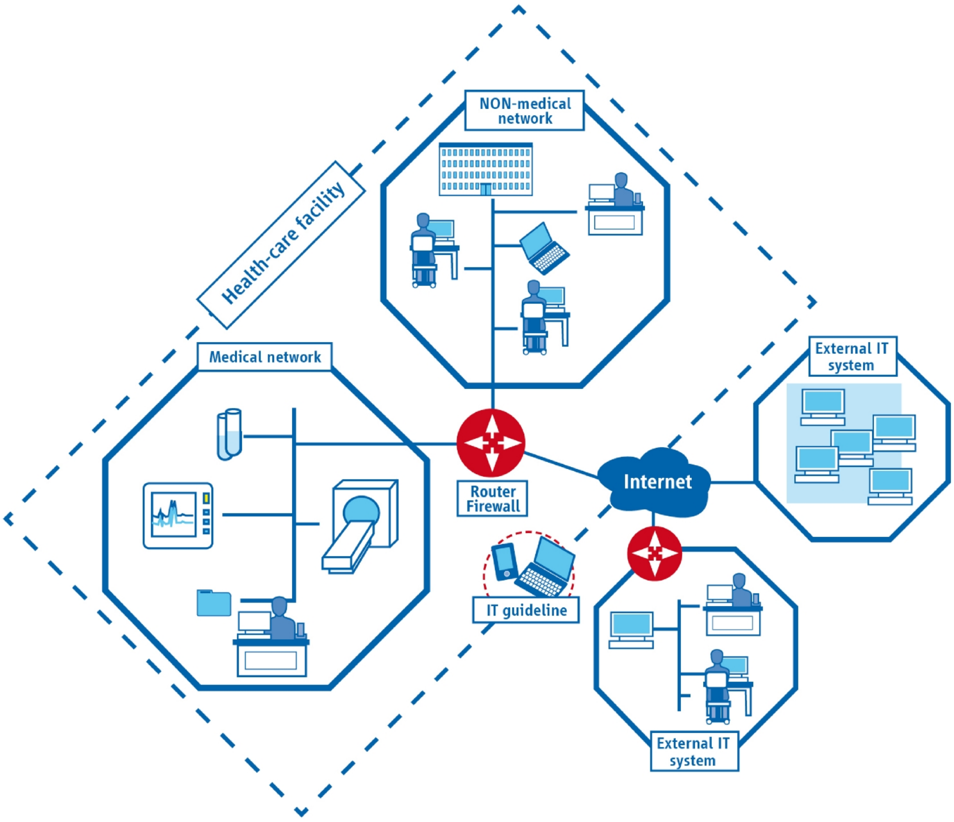
January 2017
German Electrical and Electronic Manufacturers' Association

Data and system security

Many enterprises in the health-care sector have automated and networked their systems and equipment.

The advantages are clear – by fostering open exchange between administrators and service providers and increasing transparency and consistency in data streams, service provision can be made more efficient. However, this kind of automation and networking also harbors risks; this becomes evident when considering the various installations that are used in a wide range of environments.

A distinction is typically made between external IT systems, internal IT systems and systems with integrated medical devices.



Source: ZVEI

As a rule, internal IT systems are located inside the health-care facility and are connected to the IT network of that facility. This includes administration systems, archiving systems and general communication systems (RIS, HIS, PACS).

External IT systems are not located solely inside the health-care facility – they can be operated from different locations, i.e. inside or outside the health-care facility, and use a wide range of IT networks, e.g. the IT system of a health-care facility or a mobile network. Examples include IT devices with remote access, portable data carriers, external storage media and similar devices.

Systems with integrated medical devices include, among others, PC-based medical devices, medical software products and other active medical devices.

Two things that these systems all have in common are that their openness generally makes them potential gateways for malware and that their automated networking characteristics enable such malware to spread widely.

In this context, malware is any software that has an unwanted effect on an IT system or medical device and could thereby lead to patient harm.

Entry points for malware

Malware can enter a medical network in various ways. Often the users themselves are responsible, for example through CDs, DVDs or USB storage devices, in e-mail attachments or over an Internet connection with insufficient virus protection. If the medical network is not securely isolated from the rest of the IT infrastructure or from external systems, malware can also enter the medical network through these channels.

In order to counter these dangers, operators often resort to their own protective measures, without realising that such actions can jeopardise the normal operation of the IT systems.

Uncontrolled or automatic software updates that have not been authorised by the medical device manufacturer (e.g., for virus protection, operating systems or other application software) can affect the function of the medical devices integrated into the network, and thus potentially endanger patient health.

Legal background

In principle, products can be placed on the market in Europe only if they satisfy the requirements of the applicable EU directives (e.g. MDD, R&TTED, RED, LVD). In accordance with Annex I (1) of the MDD, medical devices may be placed on the market in Europe only if their use under the conditions and for the purposes intended will not compromise the safety and health of patients, users and third parties. This principle applies accordingly in all EU member states. In addition, the relevant regulations regarding product liability and the protection of personal data also apply (95/46/EC).

Obligations for manufacturers

Medical device manufacturers who expect or intend their medical devices to be used in IT networks must, starting in the design phase, assess possible risks that could arise at the interfaces with regard to their potential danger, and define and implement appropriate minimisation measures. If this is not possible for technical reasons, the user or patient must be adequately informed of these dangers, e.g. in the instructions for use.

Obligations for operators

Operators of these medical devices and IT networks (e.g. hospitals, health-care facilities and medical practices) must seek information about possible dangers of any kind from the relevant manufacturers (e.g., network components, software, and medical device) during installation and putting into service; they must develop, specify and implement suitable measures in their own organisations. This includes both technical and organisational measures, for example determining and implementing IT usage guidelines.

Network security measures

Threats to the IT network can be countered using a wide range of measures without violating the legal provisions for medical devices or becoming a manufacturer as defined in the MDD.

The measures can be divided into organisational measures, adjustments to the network architecture and system protection. Examples include:

- Regular staff training – increasing risk awareness in order to reduce the likelihood of malware attacks.
- Clear network structuring in order to separate medical and non-medical network areas. Necessary connections should be made using a few well-maintained gateways. See the box to the right.
- Installing protective software (virus scanner, firewall, etc.) on non-medical systems in order to prevent them from becoming infected and subsequently spreading malware to the medical network.
- Installing port blockers at the interfaces between individual systems, e.g. USB interfaces, so that only devices that are absolutely necessary can gain access. This also applies to medical devices.
- Using FMEAs or relevant risk management processes as a suitable, tried-and-tested methodical approach.

For the safe operation of networked medical devices, we particularly recommend establishing isolated, secure medical subnetworks. As part of a comprehensive security concept (for example, in accordance with one of the following standards: ISO/IEC 27002/ISO 27799/IEC 62443/IT-Grundschutz (baseline protection)) for the clinical IT network, the following security procedures should be implemented for each "secure medical subnetwork":

IDENTIFY: Recognition of protected assets in medical subnetworks
PROTECT: Protection against unauthorised or undesired scenarios
DETECT: Detection of unauthorised or undesired scenarios
RESPOND: Response to unauthorised or undesired scenarios
RECOVER: Recovery after unauthorised or undesired scenarios

For further information, please refer to the position paper regarding secure medical subnetworks.

These are some essential measures that should, in principle, be implemented in every medical IT environment. However, every infrastructure is different – individual consultation is necessary to develop an optimal solution.

The IEC 80001-1 standard, in conjunction with the ISO/IEC 27001 (information technology – information security management systems) and ISO/IEC 29100 (information technology – security framework) standards, provides support for risk-aware integration of medical devices into IT networks. The IEC 80001-1 standard describes how a risk analysis and the measures derived therefrom can minimise the risks of malware attacks and the spread of malware in an IT network, and describes how emergency procedures are defined. Some important constraints:

- When establishing a list of measures, legal requirements must be taken into account, (in Germany, for example, the Medical Devices Operator Ordinance).
- The technical capabilities must always be matched to the intended use and the legal requirements.

It is important to note that every update to the software or hardware of a medical device requires renewed verification and validation before the product can be used or operated in an IT network again.

Summary

IT systems and their networking have become an integral part of the public health sector and our daily lives. However, in the clinical environment, they can pose particular risks and dangers for patients, users and third parties, requiring extra attention, especially on the part of the system operator.

Special care must be taken with the definition and implementation of security concepts based on local regulations and initiatives. These must not diminish the inherent security of medical devices or render them incompatible with other regulations. These security concepts must first be developed transparently, taking into account all involved parties and organisations, with the aim of reaching a consensus. They must then be regularly maintained, reviewed and, where necessary, improved in order to continue to satisfy the requirements. The required level of security can be achieved only if all involved parties fulfill their obligations and have the right to address directly any issues they have.

Abbreviations

R&TTED	Radio and Telecommunication Terminal Equipment (R&TTE) Directive (1999/5/EC)
RED	Radio Equipment Directive (RED) (2014/53/EU)
LVD	Low Voltage Directive (2006/95/EC) and (2014/35/EC)
MDD	Medical Device Directive (93/42/EC)
MPG	Medizinproduktegesetz (Medical Devices Act)
FMEA	Failure Mode and Effects Analysis

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 (0) 69 6302-206
E-mail: bursig@zvei.org
www.zvei.org

1st issue, 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.

While every care has been taken during the creation of this flyer, ZVEI assumes no liability for its content. The use of all or part of the text is permitted provided that the source is acknowledged. We request sample copies.