ZVEI:
Die Elektroindustrie

Position Paper

Medical Devices need Cybersecurity

August 2017

German Electrical and Electronic Manufacturers' Association

Connected medical devices

Medical devices and systems in hospitals and medical practices are commonly integrated in IT networks to enable data transmission and reception and to facilitate IT-based processes. Moreover, many devices need a permanent internet connection for operation and maintenance purposes. Hence, cybersecurity requirements need to be consistently addressed throughout.

Connectivity will continue to transform healthcare in the years to come. As digitization proceeds, software is likely to become an increasingly important component of medical devices, calling for increasingly sophisticated software programming, testing, implementation, and after sales service. As healthcare interconnectivity and digital transformation proceeds, the cybersecurity attributes of medical devices and systems will require continuous scrutiny and further development. Manufacturers can do this – but only in the intended operating environment and when used for the intended purpose. The key elements involved are set out in the following.

Medical Devices need Cybersecurity

1. Cybersecurity is an integral requirement for medical devices

Cybersecurity encompasses all the technical (hardware and software) and organizational measures required to protect medical devices from attack and unauthorized access. This includes both the integration of the device in existing hospital IT architecture and the features of the device itself. A lot is at stake. Unauthorized access or unintended operation may result in medical device data, services and software being disclosed, manipulated, damaged or deleted to the point where the medical device is no longer fit to meet its intended purpose.

These threats can be counteracted by implementing cybersecurity measures designed to respond to different levels of risk so as to protect the confidentiality, integrity and availability of the data, communication and functional features of the medical device.

2. Cybersecurity throughout the product life cycle

Medical device cybersecurity must be guaranteed throughout the product life cycle. This includes routine cybersecurity specifications and testing in the development and production process. The organizational readiness of a company in terms of cybersecurity is therefore crucial to the consistent and comprehensive cybersecurity and reliability of a product. CE marking of medical devices addresses cybersecurity aspects at every stage from product development to production and installation at the customer's premises. The current state of the art is addressed and medical devices are consistently upgraded to meet the latest standards. The state of the art necessarily continues to develop and advance. Similarly, awareness of new threats and risks needs to be addressed in product stewardship efforts.

Industry associations, the research community and official agencies need to engage in ongoing dialogue with each other. Industry associations can amplify the results of this process by issuing sector recommendations.

The ZVEI actively supports the efforts of the German Federal Office for Safety in Information Technology (BSI) to establish recommendations for measures to be implemented by manufacturers for enhanced cybersecurity in the product life cycle.

Measures to improve security levels and in particular to fix existing vulnerabilities in cybersecurity should be actively offered to all device and system users as soon as possible. Patching and upgrading to improve the security levels of already installed devices should be viewed as a separate task.

3. Cybersecurity is a system-wide challenge

Medical device cybersecurity cannot be the sole responsibility of manufacturers. Apart from making sure medical devices are secure, cybersecurity also calls for appropriate security measures in the operating and network architecture in which the medical devices are employed. In addition, users should practice security-aware behavior and observe the recommendations of medical device manufacturers. Manufacturers support users in this task.

Manufacturers, professional medical users – and to an increasing extent, patients as well – must act together to ensure safe operation.

4. Information-sharing and knowledge transfer

Manufacturers should develop processes allowing them to obtain and act on information from users, researchers or other stakeholders about security vulnerabilities or new hazards. A joint information pool of medical device manufacturers can help to ensure that any such information is shared quickly so that all parties concerned can take appropriate corrective action swiftly.

Structured information-sharing with official agencies and healthcare stakeholders, e.g. via UP KRITIS (a public-private partnership for protection of critical infrastructures in Germany), can contribute to further improvement of security levels. Joint analysis of security risks and the underlying hardware and software systems also forms a sound basis for joint development of norms and standards as part of a security architecture.

Medical device manufacturers should therefore seek regular dialogue with users on cybersecurity issues. The insights thus obtained should feed back into product development and product stewardship.

5. Identifying unavoidable risks

CE marking for medical devices involves risk analysis including cybersecurity factors, based on the intended purpose of the device and its probable use in practice. Manufacturers must make users aware of any operational risks identified in this process that cannot be excluded by modifying device design.

Manufacturers are also required to propose ways to prevent or reduce risks in product manuals and during device training.

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e.V.
German Electrical and Electronic Manufacturers´ Association
Medical Engineering Division
Lyoner Strasse 9
60529 Frankfurt am Main, Germany

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

www.zvei.org

August 2017