Medical devices and in-vitro diagnostics 6 September 2023

TÜV SÜD calls for EU-wide standard for cyber security tests

Munich. TÜV SÜD is calling for further advancement of the procedure used for mandatory penetration testing for medical devices and in-vitro diagnostics (IVD), and is publishing a new white paper on the subject. Neither the EU's regulatory specifications nor the associated guidance documents have set out concrete policies guidelines to date. A standard addressing the subject is hoped to clarify testing requirements needs for the future, setting out what needs to be tested as well as where and how plus the scope of testing. This will enable the cyber security of connected networked devices to be guaranteed in the patients' interests.

Jan Küfner
Senior Product Specialist (SPS)
Cyber Security

Dr Abtin Rad
Global Director Functional Safety,
Software and Digitisation,

Dr Alexander Stock
Project Manager IVD Medical
Device Testing

"There is still a lack of precise information as to whether the depth of testing for medical devices and lower-risk IVDs should be reduced, although this would be an obvious benefit", says Jan Küfner, Senior Product Specialist for Cybersecurity at TÜV SÜD. For example, is full penetration testing really necessary for every new release of a software program? What kind of testing should be performed for Ethernet and Bluetooth connections? When is fuzzing necessary, and to what extent? In penetration testing, "ethical hackers" simulate an IT attack on a medical device or IVD and can thus detect vulnerabilities before they can be exploited by malicious actors. “Fuzzing” is a procedure in which testers input random and partly manipulated data to deliberately generate software errors. The white paper published by TÜV SÜD looks at concrete questions to address existing regulatory gaps from the perspective of manufacturers and companies, with the aim of using the answers to improve standards in future.

EU regulations, among them the Medical Device Regulation (MDR) and the In-Vitro Diagnostics Regulation (IVDR), contain specifications for cyber security. “However, the accompanying European guideline MDCG 2019-16, which is intended to clarify the process requirements, is lacking in crucial details. The same applies to the IEC 81001-5-1, the international standard addressing IT security across the software life cycle”, points out Dr Abtin Rad, cyber security and artificial intelligence (AI) expert at TÜV SÜD. “The harmonisation announced by the EU for the coming year offers the opportunity to bring various country-specific standards that are already in place into line with an EU-wide standard.”

Clarifying the scope of testing in dynamic threat situations

As IT tools develop and advance and new vulnerabilities can emerge from new software or updates, the threat situation is constantly changing. AI may thus support hackers and cyber-attackers, and not only medical professionals. Connectivity is essential for devices that have to perform rapid analysis of large volumes of medical data, like ultrasound devices or haemoglobin counters. This opens up more opportunities for cyber attacks.

Non-secure products pose risks for patient safety, data security and data protection. Manipulated data may further present the risk of errors in diagnosis and treatment, or even threaten public health in cases such as incorrect evaluation of infection events. Potential consequences could be refusal or delay of market approval, compensation payments and reputational damage.

TÜV SÜD’s experts perform activities including vulnerability analysis, penetration testing and “fuzzing campaigns”. To do so, they rely on a global network of penetration (pen) testing laboratories[1]. To keep the focus on patient risk at all times, TÜV SÜD’s pen test experts concentrate on medical devices and IVDs. areas in which classic cyber security methods do not always offer tailored solutions. Taking the risks evaluated by the testing as a basis, companies can then develop bespoke solutions for networks and mobile or web applications. The procedure used by the testing, inspection and certification company results in significantly shorter time-to-market for IVDs and medical devices. Dr Alexander Stock, Project Manager IVD Medical Device Testing at TÜV SÜD, explains, “We work within a network of colleagues spanning Singapore, Japan, India, China and the USA. TÜV SÜD also conducts cyber

[1] Munich, Singapore, Shanghai, Tokyo, Bangalore, Pune, Michigan, San Diego.

security training courses for external experts, with topics including determination of the purpose of medical devices and the various country-specific national regulatory requirements."

TÜV SÜD white paper;

Medical device cyber security – current European regulation and its gap: https://www.tuvsud.com/de-de/-/media/de/product-service/pdf/whitepaper/whitepaper-cybersecurity-en.pdf

More information: https://www.tuvsud.com/en/services/cyber-security/operational-technology-security

Note for editorial staff: The press release and high-resolution photos from Jan Küfner, Dr Abtin Rad and Dr. Alexander Stock are available on the Internet at www.tuvsud.com/pressreleases.

Media Relations:

Dirk Moser-Delarami	Tel.	+49 (0) 89 / 57 91 – 15 92
TÜV SÜD AG	Fax	+49 (0) 89 / 57 91 – 22 69
Corporate Communications	Email	dirk.moser-delarami@tuvsud.com
Westendstr. 199, 80686 Munich	Internet	www.tuvsud.com/de

Founded in 1866 as a steam boiler inspection association, the TÜV SÜD Group has evolved into a global enterprise. Over 26,000 employees continually improve technology, systems and expertise at more than 1,000 locations in around 50 countries. They contribute significantly to making technical innovations such as Industry 4.0, autonomous driving and renewable energy safe and reliable. www.tuvsud.com/en