HealthManagement
Promoting Management and Leadership

Can Web Applications Be Used Securely In The Healthcare Sector?

Dr. Guenter Hellstern
******@***medavis.com

Chief Information Security Officer -
medavis GmbH

High protection goals such as confidentiality and integrity for medical data (including patient data) require the highest standards of information security not only since the GDPR came into force. While classic firewall technologies provide good protection at network level, a web application at a higher level must be able to withstand a whole bundle of attack scenarios. Furthermore, both users and manufacturers must be integrated into a comprehensive security concept.

Ensure High Standards of IT Security with OWASP

Similar standards and methods are applied to the IT security of web applications in the healthcare sector as they are used for web applications in the financial sector. Central tools for analysis and implementation in this industry are the security guidelines of the Open Web Application Security Project (OWASP) which covers the evaluation of the most common threats and offers effective measures for protection against these threats. The OWASP's design criteria for web applications provide a very comprehensive checklist of design and coding guidelines that should be consistently applied in the implementation of secure web applications.

Increased Security Through Penetration Tests

In a penetration test, IT systems or networks are subjected to a comprehensive examination to assess the vulnerability of the application. Penetration tests apply techniques and methods that would be used by real attackers.

Aims of a Penetration Test

A penetration test identifies weaknesses in the system, uncovers potential errors due to incorrect operation, and increases security at the technical and organisational level. Complementary to the OWASP design and coding guidelines, the goal of penetration tests is to reveal security gaps in the application. The penetration test is ideally carried out by an external information security specialist firm who certifies the proven IT security.

Information Security Management System According to ISO-27001

The information security management system ensures that the protection goals of confidentiality, integrity and availability of data are achieved and is thus a central pillar of effective data protection for IT vendors in the healthcare sector.

medavis, for instance, maintains an information security management system that was successfully audited in October 2020 in accordance with the leading standard ISO-27001:2013. The management system does not only cover the classic IT areas, but all processes of the value chain, in

particular software development, project implementation and support, which are of particular importance for customers. In the five-day ISO-27001 audit, medavis was not only able to prove the effective implementation of the standard in company processes, but also to demonstrate a high level of information security in the development of medavis software products and the operation of IT systems by means of automated test suites and penetration tests. medavis customers benefit highly from the fact that they can fully rely on a certified manufacturer to consistently implement the rules of a recognised standard. The ISO-27001 certification ideally complements the ISO-9001 (Quality Management System) and ISO-13485 (Quality Management System for Medical Devices) standards, to which medavis has been certified for many years.

Published on : Fri, 13 Nov 2020