HealthManagement
Promoting Management and Leadership

Medical Device Security Health Check from EU

Digital healthcare aims to improve delivery of care and outcomes for patients. However, an upward trend in healthcare cyber attacks has raised concerns about the use of IoT medical devices and patient safety. The technologically fragmented IoT infrastructure, as noted by infosec experts, is a major factor behind the increasing number of attacks.

It is against this backdrop that the European Union has moved to put the medtech industry – with nearly €110 billion in annual sales regionwide – under closer scrutiny as regards security of their products.

You might also like: **Ten Ways to Keep Your Networks Hacker Proof**

The European Commission is all set to implement the updated EU Medical Device Regulation (MDR). Thus, effective on 26 May 2020, manufacturers of medical devices and products, from contact lenses to pacemakers, must adhere to stricter standards throughout a product's lifecycle.

IoT medical devices bound for the EU market must undergo approval through a risk classification system that puts onus of cybersecurity mainly on the manufacturer. The new MDR requires vendors to obtain certification approval of their device through an accredited "Notifying Body."

These Notifying Bodies are also responsible for issuing fines or requesting product recalls. The General Data Protection Regulation (GDPR), the NIS Directive, and the Cybersecurity Act all work in conjunction with the MDR in the corresponding EU member state.

This shift towards manufacturer accountability, according to tech expert Rusty Carter, has been driven by consumers (who are normally held responsible for implementing device security patches).

"Clinicians are a critical component in building awareness, as they are the least likely to understand the security aspects of manufacturers, clinicians, and patients, and needs to maintain patient safety," said Carter, vice president of product management at Arxan Technologies. "They [clinicians] are typically prescribing, recommending, selecting, or installing devices."

Crafted to lessen the onus on medical practitioners, the revised MDR will require device manufacturers to develop software with appropriate access controls and protection of data, both stored and in transit.

"Weak access control may allow malicious modification of the operation of an implanted cardiac device," according to a document published by the Medical Device Coordination Group (MDCG) , which issues cybersecurity guidance to device manufacturers under the new MDR.

It will be recalled that, in 2017, the U.S. Federal Drug and Administration ordered the removal of six types of Abbott pacemakers, totalling nearly half a million devices, over cybersecurity risk.

The MDCG document further states, "During an emergency, the medical personnel must be able to access an implanted cardiac device without restrictions, but strong security measures need to be in place under normal operating conditions."

The more stringent rules set out by the EU have drawn criticism from industry players. In a survey of 230 medical device manufacturers last September, for instance, only 27% of respondents reported they were ready to comply with the new MDR come the May deadline.

"Considering the significance of these changes and the operational issues they raise, there is widespread concern in the industry that many actors will be unable to fully comply with the MDR by the general date of application," said Oliver Bisazza, director for regulations and industrial policy at MedTech, a European trade association representing the medical device industry.

"This could negatively affect the availability and safety of medical devices in the European Union."

Source: The Daily Swig

Image credit: Pixabay

Published on : Tue, 17 Mar 2020