MEDTECH INSIGHT
CITELINE COMMERCIAL

10 Aug 2023 | **News**

Vulnerabilities Up 59%: The State Of Healthcare Cybersecurity In 2023

by Hannah Daniel

A report from the Health-ISAC, Finite State and Securin found a large increase in vulnerabilities in healthcare devices since 2022.

The *2023 State of Cybersecurity for Medical Devices and Healthcare Systems* found that there was a 59% increase in vulnerabilities in healthcare devices since 2022.

Health-ISAC, Finite State and Securin Inc conducted a survey of 966 products from 117 medical device manufacturers and healthcare application venders. 993 vulnerabilities were found within the products.

Devices were put into four categories. Three were risk-based levels of class I, II or III. According to the report, class I devices, like bandages, have “minimum potential to cause patient harm” and least regulatory control; class II devices, like infusion pumps, are considered “moderate risk” and usually require special regulatory controls; class III devices, like implantable devices, are high-risk devices “intended to sustain or support life.”

The fourth category was Healthcare Information Technology, which included software and applications that support healthcare delivery operations. The category had 741 vulnerabilities, the highest number among the four.

Click here to explore this interactive content online

The results aren’t too surprising, considering results from the Medical Device Innovation Consortium’s October 2022 *Cybersecurity Maturity Industry Benchmark* report.

“While cybersecurity maturity varies significantly between [medical device manufacturers], the industry as a whole has a low level of cybersecurity maturity,” the report concluded. (Also see "*MDIC Cybersecurity Benchmarking Maturity Report: An ‘Honest Reflection’ Of The Industry*" -

Medtech Insight, 24 Jan, 2023.)

In a recent example, HCA Healthcare was breached in a ransomware attack on 5 July. As many as 11 million patients may have been affected by the breach, in which an external server was accessed by an unauthorized party and 27 million rows of data were stolen. (Also see "*HCA Healthcare Data Breach Crosses State Lines*" - Medtech Insight, 14 Jul, 2023.)

SBOMs, Penetration Testing Among Recommendations

The report recommends regular penetration testing as a way to detect vulnerabilities in devices, especially in large healthcare settings. Penetration testing often includes hiring a third party to test a system's vulnerabilities by trying to exploit the system as much as possible. After the tests are finished, the vulnerabilities are reported back to the organization for fixing.

Keeping up to date with updates, especially ones that patch high-risk vulnerabilities, is not only good practice but critical for keeping devices and IT safe.

Additionally, report authors recommend developing software bills of material (SBOMs) for any device with software. And SBOM is an itemized list of all software components in a system that can be critical when searching for vulnerabilities.

Congress recently gave the US Food and Drug Administration the authority to require SBOMs for all new medical device applications that contain software. (Also see "*Expert: Cybersecurity Requirements In Omnibus Bill Will Provide Visibility For Industry*" - Medtech Insight, 10 Jan, 2023.)

In April, the International Medical Device Regulation Forum published a guidance for SBOM use, the *Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity*. (Also see "*Latest Cybersecurity Guidance From IMDRF Highlights Software Bills Of Materials*" - Medtech Insight, 18 Apr, 2023.)

The report also urges companies to implement a security-by-design process when creating and manufacturing healthcare products which considers the total lifecycle of a product.