EINPRESSWIRE

Device management complexities could create cybersecurity gaps and leave NHS Trusts vulnerable

FOI request conducted by Armis shows 41% of NHS Trusts don't have a real-time risk register of all digital assets connected to their networks

LONDON, UK, November 18, 2021 /EINPresswire.com/ -- Armis, the leading unified asset visibility and security platform provider, today released figures from a Freedom of Information (FOI) request to over 80 NHS Trusts that highlighted compliance and device management complexities could be creating critical cybersecurity gaps. The study confirmed that while 85% had identified all devices, including medical devices, on the Trust's network, 41% had no real-time risk register of these assets and one in three did not identify and monitor all medical devices being used for remote patient management. With the Internet of Medical Things (IoMT) predicted to rise to $158.1bn next year, an explosion of devices could put Trusts on the back foot if these security blind spots are not addressed.

Main findings from the FOI request:
□□15% said "no" when asked if all devices including medical devices on the Trust's network have been identified
□41% do not have a real-time risk register of all assets connected to the network
□31% of those that use devices for remote patient management don't monitor them
□□14% have not met compliance with Data Security and Protection Toolkit (DSPT)
□46% don't comply with Cyber Essentials; 63% don't comply with Cyber Essentials Plus
□Of those that answered, 76% had less than ten percent of their medical device estate running on end of life or unsupported software; though 16% said more than 15% and almost one in ten didn't know how much of their medical device estate was running on EOL or unsupported software
□27% said none, 30% said all and 30% said 61-99% of medical device estate was segregated from the main network

A recent study by Obrela Security Industries confirmed that over 80% of healthcare organisations in the UK had been hit by ransomware last year, with a 30% rise in attacks from Q2 to Q3. And earlier this year, Ireland's Health Service was severely impacted by a ransomware attack, with the NCSC declaring the healthcare sector a top target for cybercrime.

"NHS Trusts are no doubt doing their best in the face of some extraordinary challenges, but unfortunately the list of challenges keeps getting longer," said Conor Coughlan, General Manager for EMEA at Armis. "The role of technology is obviously critical, yet its vulnerabilities have also been exposed by unscrupulous bad actors who, regrettably, believe that targeting healthcare services is acceptable. From WannaCry in 2017 to recent ransomware attacks in Ireland, the need to defend systems and devices in hospitals is self-evident. As IoMT proliferates, gaining visibility and understanding of these devices is paramount because without specialist technology, visibility into device estates can be as low as 60%."

The study also found that regulatory compliance remains a challenge, with 14% unable to yet meet their Data Security and Protection Toolkit (DSPT) requirements. Interestingly, one of the new DSPT non-mandatory requirements for '21-'22 is for Trusts to maintain a register of medical devices connected to its networks. Furthermore, the NCSC's Cyber Essentials is met by 54% of Trusts, though 63% have not yet met the controversial Cyber Essentials Plus recommendations; and 37% do not comply with the EU's Network & Information Security Directive (NIS). Over two-thirds (67%) of the NHS Trusts are not ISO27001 compliant.

When it comes to devices running outdated or unsupported software, it's clear that more security gaps appear. Of the Trusts that did not withhold their answers, only 37% said they had no medical device estate running on end of life or unsupported software, while 16% said they were running over one-tenth of their medical device estate on EOL or unsupported software. In terms of using segregation to keep potentially risky medical devices away from the main IT network, encouragingly, almost one in three (30%) recognise the importance and keep all their medical estate segregated form the main network, while the same amount keeps the majority (61-99%) of it segregated. Nearly the same amount (27%) said none of the medical device estate is segregated from the main network.

"Device management can be a complex task and therefore it becomes a matter of context and the ability to confidently accept some risk. The key here is for systems administrators to have all the information about devices, known threats and where they are on their support lifecycles to be able to make these quick judgements and remediate issues swiftly," said Sumit Sehgal, Armis Strategic Product Marketing Director. "Having this level of knowledge, mapped to their compliance requirements, will help put NHS Trusts in the best position to defend themselves against a backdrop of increasing medical devices and attackers waiting to exploit them."

Implementing a successful medical device security strategy requires a multi-faceted approach that accounts for the entire healthcare device ecosystem in addition to connected medical devices. Mapping this data to clinical workflows and creating a holistic visual of prioritised risk transforms security operations and allows information security strategy to be aligned with resilience and continuity of operations.

For further information on securing healthcare environments, Armis has also produced a whitepaper entitled Security and Operational Efficiency which can be accessed here: https://www.armis.com/analyst-reports/security-operational-nhs-research-healthcare.

Methodology
FOI request information gathered from over 80 NHS Trusts from July to October 2021

About Armis
Armis is the leading unified asset visibility and security platform designed to address the new threat landscape that connected devices create. Fortune 1000 companies trust our real-time and continuous protection to see with full context all managed, unmanaged, and IoT devices, including medical devices (IoMT), operational technology (OT) and industrial control systems (ICS). Armis provides passive and unparalleled cybersecurity asset management, risk management, and automated enforcement. Armis is a privately held company and headquartered in Palo Alto, California.

Armis
beth@smileonfridays.com
Beth Smith
Visit us on social media:
Facebook
Twitter
LinkedIn
Other
