NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

HEALTH CARE

Securing Wireless Infusion Pumps

The National Cybersecurity Center of Excellence (NCCoE) addressed the challenge of securing wireless infusion pumps through collaborative efforts with members of the healthcare sector and vendors of cybersecurity solutions. The example solution is detailed in NIST Cybersecurity Practice Guide, SP 1800-8, *Securing Wireless Infusion Pumps in Healthcare Delivery Organizations*. The NCCoE solution may not be the only one available in this fast-moving cybersecurity technology market. Please contact us at hit_nccoe@nist.gov with suggestions and comments.

CHALLENGE

Technology improvements happen rapidly across all sectors. For organizations focused on delivering high-quality patient care, it can be difficult to take advantage of the latest technological advances, while also ensuring new medical devices or applications are secure. For many Healthcare Delivery Organizations (HDOs), this can result in improperly configured networks and components that increase cybersecurity risks.

Unlike prior medical devices that were once standalone instruments, today's wireless infusion pumps connect to a variety of healthcare systems, networks, and other devices. Although connecting infusion pumps to point-of-care medication systems and electronic health records can improve healthcare delivery processes, this can also increase cybersecurity risk, which could lead to operational or safety risks. Tampering, intentional or otherwise, with the wireless infusion pump ecosystem can expose an HDO enterprise to serious risk factors, such as: access by malicious actors; a breach of protected health information; loss or disruption of healthcare services; and damage to an organization's reputation, productivity, and bottom-line revenue.

With an increasing number of infusion pumps connecting to networks, the vulnerabilities and risk factors become more critical as they can expose the pump ecosystem to external attacks, compromises, or interference.

SOLUTION

The NCCoE has developed cybersecurity guidance, NIST Special Publication 1800-8 *Securing Wireless Infusion Pumps*, using standards-based commercially available technologies and industry best practices to help HDOs strengthen the security of the wireless infusion pump ecosystem within healthcare facilities.

This NIST cybersecurity publication provides best practices and detailed guidance on how to manage assets, protect against threats, and mitigate vulnerabilities by performing a questionnaire-based risk assessment. In addition, the security characteristics of wireless infusion pump ecosystem are mapped to currently available cybersecurity standards and the Health Insurance Portability and Accountability Act (HIPAA) Security Rule. Based on our risk assessment findings, we apply security controls to the pump's ecosystem to create a 'defense-in-depth' solution for protecting infusion pumps and their surrounding systems against various risk factors. Ultimately, we show how biomedical, networking, and cybersecurity engineers and IT professionals can securely configure and deploy wireless infusion pumps to reduce cybersecurity risk.

BENEFITS

The potential business benefits of the example implementation developed in this project include:

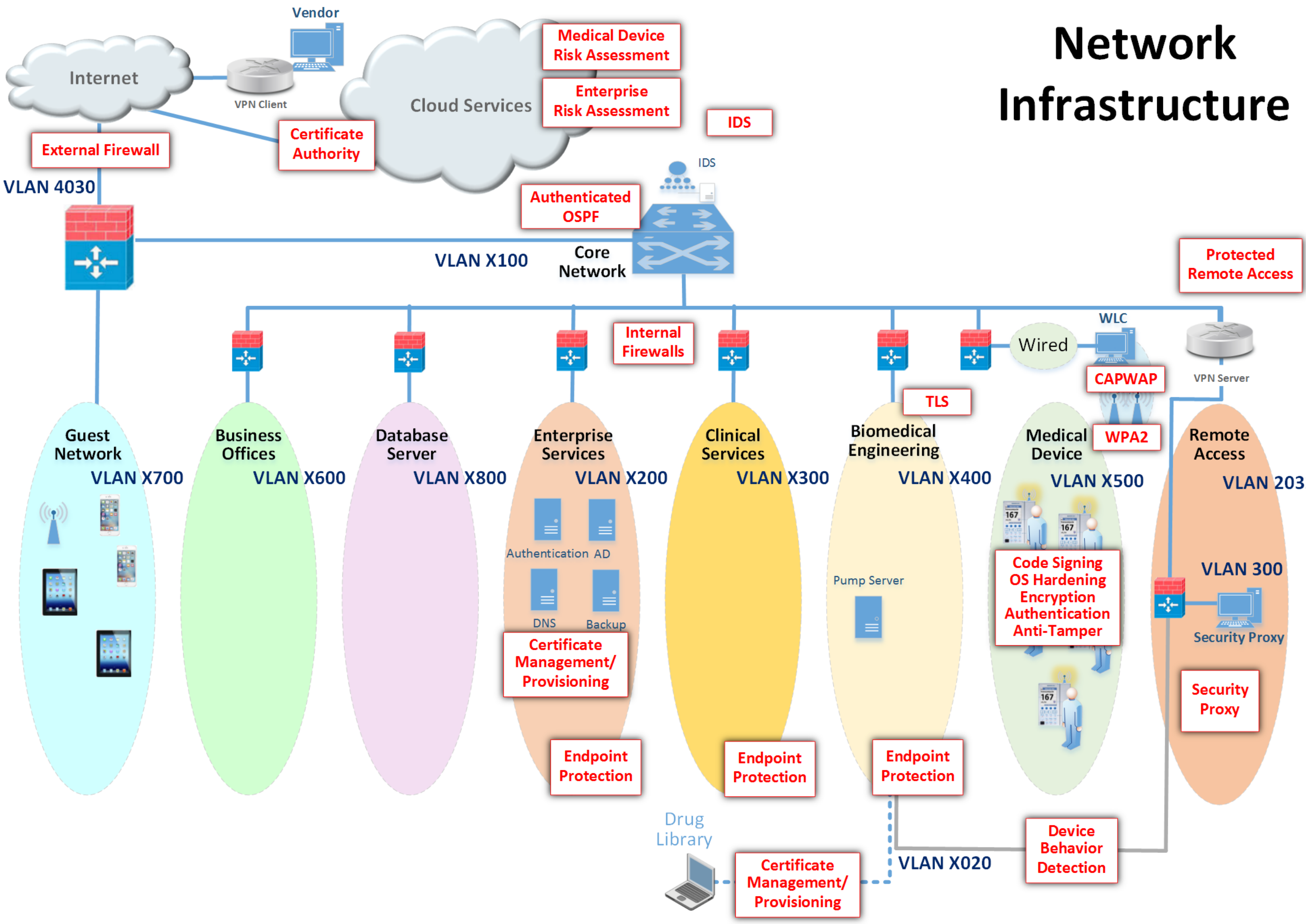
- reduces cybersecurity risk, and potentially reduces impact to safety and operational risk, such as the loss of patient information or interference with the standard operation of a medical device
- develops and executes a defense-in-depth strategy that protects the enterprise with layers of security to avoid a single point of failure and provide strong support for availability
- implements current cybersecurity standards and best practices, while maintaining the performance and usability of wireless infusion pumps

The National Cybersecurity Center of Excellence (NCCoE), a part of the National Institute of Standards and Technology (NIST), is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions demonstrating how to apply standards and best practices using commercially available technology.

LEARN MORE ABOUT NCCOE
Visit https://nccoe.nist.gov

CONTACT US
hit_nccoe@nist.gov
301-975-0200

HIGH-LEVEL ARCHITECTURE



TECHNOLOGY PARTNERS/COLLABORATORS

The technology vendors who participated in this project submitted their capabilities in response to a call in the Federal Register. Companies with relevant products were invited to sign a Cooperative Research and Development Agreement with NIST, allowing them to participate in a consortium to build this example solution. Technology collaborators on this project include:

B|BRAUN   Baxter   BD   CISCO   CLEARWATER COMPLIANCE   digicert   Hospira   intercede

MDISS   PFP CYBERSECURITY   RAMPARTS   smiths medical bringing technology to life   Symantec   tdi technologies

Certain commercial entities, equipment, products, or materials may be identified in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST or NCCoE, nor is it intended to imply that the entities, equipment, products, or materials are necessarily the best available for the purpose.

DOWNLOAD THE PRACTICE GUIDE

For more information about this project, visit:
https://nccoe.nist.gov/projects/use_cases/medical_devices

HOW TO PARTICIPATE

As a private-public partnership, we are always seeking insights and expertise from businesses, the public, and technology vendors. If you have feedback on the architecture or the relevance and usefulness of this Practice Guide, or would like to schedule a demonstration, please email hit_nccoe@nist.gov.

June 2017