BREAST IMAGING SOLUTIONS

Enterprise Cybersecurity Best Practices

MAN-00363 Revision 006

HOLOGIC®

Enterprise Cybersecurity Best Practices

Part Number MAN-00363

Revision 006

April 2013

HOLOGIC®

Corporate Headquarters

35 Crosby Drive,
Bedford, MA 01730-1401 USA
Tel: +1.781.999.7300
Sales: +1.781.999.7453
Fax: +1.781.280.0668
www.hologic.com

EC REP Europe
(EU Representative)

Hologic NV
Leuvensesteenweg 250A
1800 Vilvoorde, Belgium
Tel: +32.2.711.4680
Fax: +32.2.725.2087

Manufacturer

36-37 Apple Ridge Road
Danbury, CT 06810 USA

Refer to the corporate website for more facilities worldwide.

Table of Contents

1.0 Overview

Hologic® is a leading developer, manufacturer and supplier of premium diagnostics, medical imaging systems and surgical products dedicated to serving the healthcare needs of women. Ensuring the integrity of our systems and the business continuity of our customers is a top concern for Hologic. This document provides a "best practices" guide to assist an IT staff in securing their general network infrastructure where Hologic medical products are in use.

These recommendations intend to increase the overall security posture of the environment where Hologic medical products are installed and operated. Adherence to these security recommendations minimizes the overall risk of cybersecurity threats to your computer-based assets by reducing the number of possible exploitable avenues.

2.0 Introduction

Hologic regularly monitors the information security industry to assess new cybersecurity vulnerabilities, and offers solutions for increased product security. Hologic performs risk analysis to determine the potential consequences of any vulnerability. Hologic may offer solutions, such as:

- a software patch,
- a design change, or
- a suggested compensating control that is external to the product, such as configuring a network firewall device to block the malicious traffic.

Hologic validates product changes that mitigate a software vulnerability or exposure to ensure optimal patient care and the continual operation of our products.

Hologic also has an ongoing security maintenance program for the entire life cycle of our products. The ongoing maintenance program consists of:

- Regular software and OS vulnerability assessments
- Laboratory evaluation of anti-virus software or other products that may improve the security of our products
- Laboratory evaluation of OS security patches
- Ongoing monitoring of the industry for new vulnerabilities and exploits

Hologic is committed to the cybersecurity maintenance program for our products. We put forth some general cybersecurity best practices to assist our customers. We believe that when our customers incorporate these industry best practices, it increases the overall security posture of their organization.

3.0 Audience

The intended audience includes the systems administrator, network administrator, and/or security personnel. These practices intend to aid in securing the network infrastructure and network environments where Hologic products are deployed.

4.0 Remarks

At Hologic, we strive to make every Hologic medical system that we sell as secure and user-friendly as possible before it leaves our factory. However, these devices are for medical purposes and are not security devices by design.

We regularly validate OS security patches and publish the results as a product report. Any patches listed in the cybersecurity product report are safe to install on our systems to the best of our knowledge, based upon our testing.   Due to the regular pace of software vulnerabilities, speedy patching becomes impractical. Therefore, we assume our customers to take vigilant approaches to security in their day-to-day operations. We also assume our customers to have a resilient network environment with a security architecture design that incorporates proactive security mechanisms. These systems deal with emerging zero-day vulnerabilities and exploits.

A successful organizational IT security strategy consists of comprehensive security plan, policies, and best practices that utilize a combination of effective physical, administrative, and technical controls. A good security plan considers the following:

- Defense in Depth strategy that incorporates layered defenses
- Timed access control
- Centralized logging and auditing
- Disaster Recovery Plans / Business Continuity Plans
- Data backup and recovery strategy
- Authentication and password security
- Perimeter security (such as firewalls, IDS/IPS, proxy servers, anti-virus gateway)
- Internal security (such as network monitoring, intrusion detection, and extrusion detection, log review process, scan of network)
- Physical security (such as biometrics, locks, cameras)
- User Security Awareness Training focusing on safe computing practices
- Technical network defense design and control

5.0 Definitions, Terms, and Abbreviations

DHCP: Dynamic Host Configuration Protocol

IDS: Intrusion Detection System

IPS: Intrusion Prevention System

Malware: Malicious software such as computer viruses, worms, rootkits, Trojans, data stealing, or any other malicious intent

OS: Operating system

VLAN: Virtual Local Area Network

6.0 Defense in Depth Strategy

Defense in Depth is an Information Assurance strategy in which several layers of defense are placed to protect a computing resource such as an information system. It is designed to address security weaknesses in personnel, technology, and operations for the duration of the system life cycle. The idea behind this layered defense is to defend a system against any particular attack using several different methods. It is a layering tactic by the National Security Agency (NSA) as a comprehensive approach to information and electronic security.

The NSA provides a guide to "Defense in Depth" here: http://www.nsa.gov/ia/_files/support/defenseindepth.pdf.

7.0 Windows Domain & Active Directory

Many organizations have migrated to Windows® Active Directory® for the ease of centralized administration of their network resources. Some Hologic products support Active Directory functionality.

For more details, refer to the product-specific support information available at http://www.hologic.com/en/product-support-link/overview/.

8.0 Network Security

8.1 IP Address Assignment

Like most vendors, Hologic recommends that the IP addresses of Hologic devices be assigned statically, rather than dynamically via a DHCP server. This practice ensures the IP address records that our service technicians maintain are accurate, and can also prevent certain forms of denial-of-service attacks.

When possible, do not assign a publicly addressable IP address to Hologic devices. Instead, assign a private IP address space based on RFC 1918. Do not allow open internet access without strong technical safeguards in place.

8.2 Segmentation

Separating medical devices from the rest of your general network helps to increase the security of these devices. This step protects medical devices if a user accidentally downloads malware – such as viruses, worms, or Trojans - from the web or an email attachment. For security and privacy, have a separate physical network designed for the medical devices that does not connect directly or indirectly to the Internet. If a separate physical network is not feasible, then we recommend that you implement a logical or virtual separation using VLAN, a firewall, or a router. A medical network, whether partitioned off physically or logically, should not connect to the Internet without proper security protection to block malicious traffic.

8.3 Firewall

A firewall plays an integral role in any successful security architecture. A proper firewall provides protection from external threats originating from the Internet, as well as internal threats from viruses, worms, and malicious users.

Hologic recommends the use of hardware-based firewalls, rather than Windows software-based firewalls, which can often interfere with product operation.

8.4 Intrusion Detection Systems (IDS)

The installation of a host-based intrusion detection system solution on a Hologic medical device is not recommended. A host-based intrusion detection system solution can adversely impact the functionality and performance of the medical device. Network-based IDS may be supported. For more details, refer to the product-specific support information available at http://www.hologic.com/en/product-support-link/overview/.

9.0 Anti-virus

Running anti-virus software on endpoint devices such as workstations has become a necessity in most organizations to combat potential threats from malicious software. To support our customers, Hologic has validated several anti-virus products from Symantec, McAfee, Sophos, and Trend Micro with our products.

For more information concerning specific products, visit our product support website at http://www.hologic.com/en/product-support-link/overview/.

10.0 Physical Security

Good physical security is the foundation of any sound security plan, as it provides protection on the inside. Sound physical security helps to prevent the following from occurring:

- Theft, tampering, or destruction of equipment
- Theft, modification, or destruction of sensitive and confidential data
- Installation of a backdoor access program to compromise other devices on the network that may be more valuable

10.1 Medical device security

An easy way to protect your devices is to have a robust enterprise password policy. NIST provides a comprehensive guide that can be found here: http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf.

When determining policies for password length and complexity, organizations can consider maximum and likely actual key space. Since users are expected to memorize passwords, you can set policies that make them easier to remember, such as favoring longer passwords over more complex passwords. Another important consideration for password length and complexity policies is the rate at which cracking attacks are performed. Organizations must also consider how effectively their password strength requirements are enforced.

Some Hologic products have limitations on the password policy that they can support. For more details, refer to the product-specific support information available at http://www.hologic.com/en/product-support-link/overview/.