Data Security

MR

How effectively are you protecting your imaging equipment from patient data breaches?

Like every industry that relies on increasingly connected computer networks, the global healthcare industry is faced with a growing number of security breaches.

WannaCry ransomware attack impact on the UK's National Health Service considerably larger than previously suggested

The National Audit Office's (NAO) report into the WannaCry ransomware attack, exploiting a flaw in Microsoft Windows server message block (SMB), functionality that was present in every Windows operating system from XP to Server 2008 R2, that infected services across the UK's National Health Service (NHS) has found that its impact was considerably larger than previous reports suggested[1].

The ransomware attack caused widespread disruption to global IT systems in May 2017. According to the NAO's published report, WannaCry affected at least 81 of the 236 trusts across England, either directly or indirectly.

Thirty-seven trusts, of which 27 were acute care trusts, were locked out of devices after being infected with the WannaCry ransomware – leading to the cancellation of thousands of patient appointments and operations.

In addition to preventing access to computers, the cyber-attack also locked out important medical equipment such as MRI scanners and devices for testing blood and tissue samples.

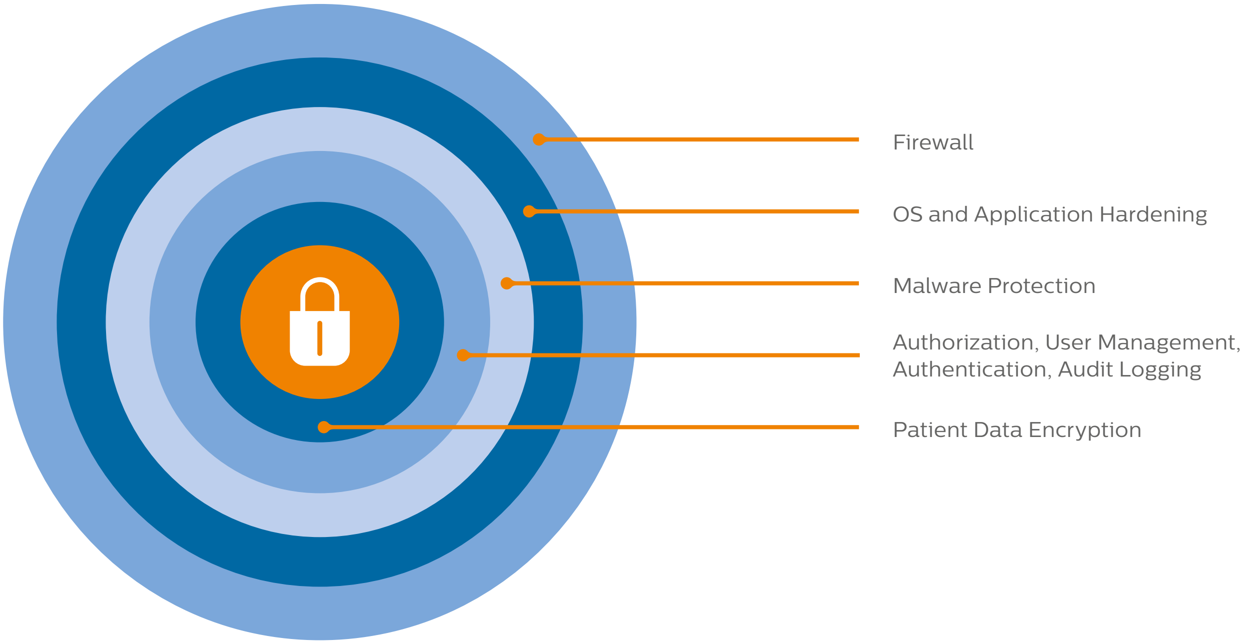
The NAO's report concluded that the NHS could have prevented the WannaCry cyber-attack had it followed basic IT security practices, including migrating computer systems to newer software versions.

The challenge for imaging devices

Imaging devices are not immune to these types of cyber attacks. Most were developed with a focus on clinical utility, with little regard to the fact they are also computers on a network that can be exploited for illegal purposes. This leaves medical devices vulnerable, and attackers are able to use these closed medical devices as pivot points within the healthcare system. A cohesive defense-in-depth security strategy can help healthcare providers avoid security breaches in the future.

Defense-in-depth security strategy

Defense-in-depth security strategy, the idea that a multi-layered defense is more difficult to penetrate than a single barrier, is the basis for best practices in medical device security. The layers can include security policies, procedures, access controls, technical measures, training, and risk assessments.


Firewall
OS and Application Hardening
Malware Protection
Authorization, User Management, Authentication, Audit Logging
Patient Data Encryption

Each of these defensive layers plays an important role in helping obstruct hackers, defend against malware, and prevent unauthorized access to imaging systems and devices.

> “ **Common best practices should always be followed when dealing with software updates and suspicious e-mails containing links and attachments, as the first line of defense against any ransomware or other malware. Continuing education should also be provided frequently to all levels of staff to promote awareness of and compliance with these best practices.”**

source: ECRI Institute:
https://www.ecri.org/components/HDJournal/Pages/Ransomware-Attacks-How-to-Protect-Your-Systems.aspx

Addressing security in Philips Magnetic Resonance (MR) Release 5 imaging systems

Philips has applied the principle of the defense-in-depth strategy to its MR Release 5 systems, implementing a security strategy that comprises multiple layers:

- Firewall
- Operating System (OS) and Application Hardening
- Malware Protection
- Authorization, User Management and Authentication
- Audit Logging
- Patient data encryption

Firewall to protect from network attacks

Strict firewall policies that block all unnecessary ports help inhibit communication with unauthorized computers, limiting the attack profile that a malicious hacker may try to exploit.

Operating system hardening to limit the attack surface

Similar in principle to firewalls, operating system hardening involves identifying all unnecessary services and functions that are included within the operating system and disabling those not required by MR Release 5 systems. OS hardening reduces the attack surface by eliminating those services that may become vulnerable over time. Philips MR follows the guidance provided by the Center of Internet Security (CIS) as a baseline for the OS hardening.

Malware protection via whitelisting provides protection against unknown threats

To mitigate the risk of unknown threats, Philips has implemented policies which allow only trusted code to run on the system. This solution, known as whitelisting, helps protect MR systems from malware.

Malware protection via conventional anti-malware provides additional protection against known threats

To mitigate the risk of infections during service activities, Philips has additionally implemented conventional anti-malware which protects your MR systems from malware during service activities. To keep the anti-malware up to date, Philips maintains the anti-malware signatures via an on-line service as part of a Philips MR service agreement.

Authorization to protect your assets

To help control access to data on your Philips MR Release 5 system, users have access restricted to need:

- **A clinical user** may perform exams and access any previously completed exams stored on the system. The system requires a login before the operator can access the data. When configured, clinical users can install released updates.
- **Hospital Administration**: can perform simple administration tasks, lock/unlock clinical accounts, and create new accounts for clinical users. Administrators can install released updates, but do not have access to patient data.
- **Service Engineers:** can perform system maintenance tasks, perform the initial installation and fault finding activities.

User management to improve access control and audit trail

With MR Release 5 you have the ability to create multiple clinical user accounts and multiple hospital administrator accounts. With both systems, hospital administrators have the option of specifying password policies in accordance with local information security requirements and policies.

MR Release 5 systems can interface with your LDAP environment to authenticate users and groups using your standard network accounts (i.e., Active Directory). Service Engineers can access the system using 2-factor authentication. Dongles can be activated and/or revoked by Philips.

Audit logging provides data for analysis

Philips has enhanced MR Release 5 systems' audit logging capabilities. Users can configure the system to send the logs to a local system log (syslog) server for retention, accessibility, and further analysis. To aid forensic analysis, users can ensure consistent time stamps by synchronizing the time on the MR systems with your network time server.

Patient data encryption at rest and in-transit to protect patient data

All patient data stored on Philips MR Release 5 system hard drives can be encrypted according to your institution's specific requirements. In addition, you can choose DICOM with TLS for node authentication without encryption, DICOM utilizing TLS encryption, or a combination of the two to encrypt patient data in-transit. (Note: This requires corresponding functionality on your PACS system.)

Philips MR Release 5 Features Summary

- Firewall policy blocks all unnecessary ports
- Microsoft Windows 7 OS hardening (note: the next Philips MR release will be based on Microsoft Windows 10)
  - OS settings utilizing the CIS benchmarks as baseline
  - Default having disabled unnecessary services
  - Disabled auto-run for removable media, and configurable access
- Media export security
  - Provides the ability to disable export of patient data to removable media (configurable)
  - Provides the ability to encrypt removable media
- Malware protection utilizing the McAfee Anti-Malware solution combined with whitelisting policies
- User management policy
  - User management using local accounts
  - Support for multiple unique user accounts
  - Support for multiple unique administrator accounts
  - User management LDAP
  - Supports Active Directory authentication utilizing LDAP (system will be joined to the domain)
  - Support for individual accounts or Active Directory groups for users and administrators
- Configurable password policies
  - Provides the ability to specify password policies for local accounts and LDAP
  - Password history (0-24)
  - Minimum password length (0-14)

  - Maximum password length (14 (local authentication), 63 (LDAP))
  - Minimum password age (0-998 days)
  - Maximum password age (1-999 days)
  - Complex password required (yes/no)
  - Account lockout policies
  - Lockout threshold (0- 999 attempts)
  - Lockout duration (1-99999 minutes)
  - Lockout counter reset (1-99999 minutes)
- Screensaver with password protection – locks the screen after the specified period of inactivity. Screensaver will not interfere during scan. (enabled/disabled, 1-999 minutes, password protected yes/no)
- Patient Data encryption
  - 128 bit AES Bitlocker(can be enabled during installation)
  - DICOM (Secure DICOM managed by certificates)
- Audit log export
  - Audit logs may be continuously exported utilizing syslog

Philips recognizes the importance of securing your medical devices and protecting your patient data. Together we can maintain a secure environment by remaining vigilant and identifying the ever-changing cybersecurity threat landscape. We are committed to meeting the needs and requirements of our customers.

To illustrate the security posture on the Philips Ingenia MR system, it received an Authority to Operate (ATO) from the U.S. Defense Health Agency (DHA) based on the compliance requirements and risk assessments as required through the Risk Management Framework (RMF) process. The risk-based approach was created by the National Institute for Standards and Technology (NIST) to create a strict security method including continuous monitoring of all information assurance controls.

[1] From Digitalhealth 27 October 2017 (www.digitalhealth.net/2017/10/wannacry-impact-on-nhs-considerably-larger-than-previously-suggested)

[2] From BankInfo Security (www.bankinfosecurity.com/wannacry-healthcare-reax-a-9921)

www.philips.com

4522 991 34081 * FEB 2018