PHILIPS

Datensicherheit

MR

Wie wirksam schützen Sie Ihre Bildgebungssysteme vor Verletzungen des Patientendatenschutzes?

Wie jede Branche, die sich auf zunehmend miteinander verbundene Computer-Netzwerke stützt, sieht sich das globale Gesundheitswesen einer steigenden Anzahl von Sicherheitsverletzungen gegenüber.

Auswirkungen des WannaCry Ransomware-Angriffs auf den britischen National Health Service bedeutend größer als zuvor angenommen

Einem Bericht des National Audit Office (NAO) über den WannaCry Ransomware-Angriff zufolge, der eine Schwachstelle des auf allen Microsoft Windows Betriebssystemen von XP bis Server 2008 R2 vorhandenen Protokolls Server Message Block (SMB) ausnutzte und Dienste im gesamten britischen National Health Service (NHS) infizierte, waren die Auswirkungen des Angriffs bedeutend größer als in vorherigen Berichten zunächst angenommen[1].

Der Ransomware-Angriff verursachte im Mai 2017 eine weitreichende Störung in globalen IT-Systemen. Laut dem vom NAO veröffentlichten Bericht befiel WannaCry mindestens 81 von 236 Trusts in ganz England, entweder direkt oder indirekt.

Siebenunddreißig Gesundheitseinrichtungen, darunter 27 in der Akutversorgung, wurden von ihren Geräten ausgesperrt, nachdem diese mit der WannaCry Ransomware infiziert wurden. Dies hatte zur Folge, dass Tausende von Patiententerminen und Operationen abgesagt bzw. verschoben werden mussten.

Zusätzlich zur Sperrung des Rechnerzugriffs verhinderte der Cyber-Angriff auch die Nutzung von wichtigen medizinischen Geräten wie MR-Scannern und Geräten zur Blut- und Gewebeanalyse.

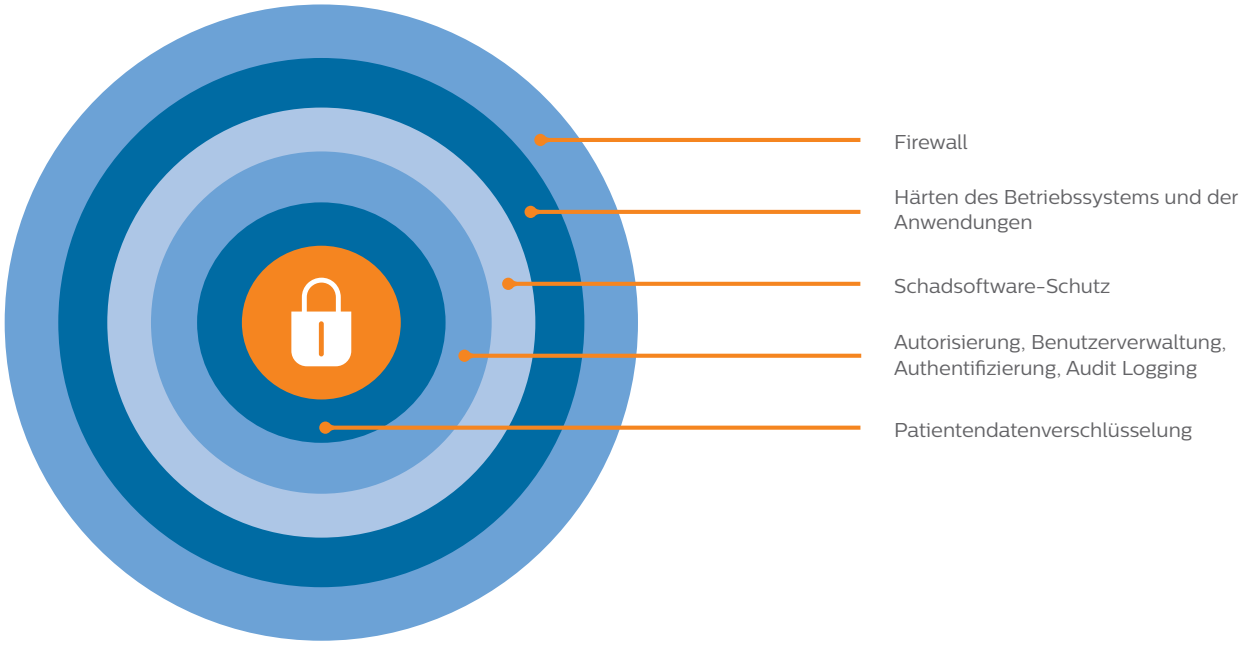
Der NAO-Bericht kam zu dem Schluss, dass der NHS den WannaCry Angriff hätte verhindern können, wenn grundlegende IT-Sicherheitsmaßnahmen ergriffen worden wären, z.B. das Migrieren von Computersystemen auf neuere Software-Versionen.

Eine Herausforderung für Bildgebungssysteme

Bildgebungssysteme sind nicht immun gegen diese Art von Cyber-Angriffen. Die meisten Bildgebungssysteme werden unter dem Gesichtspunkt des klinischen Nutzens entwickelt, unter Vernachlässigung der Tatsache, dass es sich auch um vernetzte Computersysteme handelt, die zu unlauteren Zwecken missbraucht werden können. Dadurch sind medizinische Geräte anfällig und können Angreifern als Eintrittspunkt zum gesamten Versorgungssystem dienen. Eine solide Defense-in-Depth-Sicherheitsstrategie kann Gesundheitseinrichtungen helfen, zukünftigen Sicherheitsverletzungen entgegenzuwirken.

Defense-in-Depth-Sicherheitsstrategie

Die Defense-in-Depth-Sicherheitsstrategie basiert auf der Idee, dass eine mehrschichtige Verteidigung schwerer zu durchbrechen ist als eine einzelne Barriere und bildet die Grundlage für bewährte Abläufe (Best Practices) im Bereich der Sicherheit von medizinischen Geräten. Geeignete Maßnahmen sind beispielsweise Sicherheitsrichtlinien, Prozessvorgaben, Zugriffskontrollen, technische und organisatorische Maßnahmen, Schulungen und Risikobewertungen.



Jede dieser Schutzfunktionen spielt eine wichtige Rolle dabei, Hacker zu behindern, das System vor Malware zu schützen und den unbefugten Zugriff auf Bildgebungssysteme und -geräte zu verhindern.

„Für Software-Updates und verdächtige E-Mails, die Links und Anhänge enthalten, sollten stets die allgemein bekannten und bewährten Abläufe (Best Practices) befolgt werden, die als erste Verteidigungslinie gegen jegliche Ransomware oder sonstige Malware gelten. Zudem sollte das Personal auf allen Ebenen regelmäßig und systematisch geschult werden, um Kenntnis und Umsetzung dieser Best Practices bestmöglich zu fördern.“

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

Adressierung der Sicherheit der Philips MR Release 5 Systeme

Philips hat das Prinzip der „tief gestaffelten Verteidigung“ auf die MR Release 5 Systeme angewendet und eine mehrschichtige Sicherheitsstrategie implementiert, die die folgenden Aspekte umfasst:

- Firewall
- Härten des Betriebssystems und der Anwendungen
- Schutz vor Malware
- Autorisierung, Benutzerverwaltung und Authentifizierung
- Audit Logging
- Patientendatenverschlüsselung

Firewall zum Schutz vor Netzwerkangriffen

Strenge Firewall-Richtlinien, die alle unnötigen Ports blockieren, tragen dazu bei, die Kommunikation mit unbefugten Computern zu unterbinden. Das Angriffspotential wird so reduziert.

Härten des Betriebssystems zur Reduzierung des Angriffspotentials

Ähnlich wie bei den Firewalls werden beim Härten des Betriebssystems alle nicht erforderlichen Services und Funktionen, die im Betriebssystem enthalten sind, identifiziert und solche deaktiviert, die für die MR Release 5 Systeme nicht erforderlich sind. Durch das Härten des Betriebssystems wird das Angriffspotential reduziert, indem Services beseitigt werden, die mit der Zeit angreifbar werden können. Philips MR befolgt die vom Center of Internet Security (CIS) bereitgestellten Vorgaben als Grundlage zum Härten des Betriebssystems.

Schadsoftware-Schutz per Whitelisting bietet Schutz vor unbekannten Bedrohungen

Um das Risiko unbekannter Bedrohungen zu reduzieren, hat Philips Richtlinien eingeführt, die nur die Ausführung von vertrauenswürdigem Code auf dem System erlauben. Diese Lösung, die als Whitelisting bekannt ist, trägt zum Schutz der MR-Systeme vor Schadsoftware bei.

Schadsoftware-Schutz durch herkömmliche Anti-Malware-Lösungen bietet zusätzlichen Schutz vor bekannten Bedrohungen

Um das Risiko von Infektionen während Serviceleistungen zu senken, hat Philips zusätzlich Anti-Malware-Lösungen implementiert, die Ihre MR-Systeme während Serviceleistungen vor Schadsoftware schützen. Zur regelmäßigen Aktualisierung der Anti-Malware verwaltet Philips die Anti-Malware-Signaturen über einen Online-Dienst im Rahmen eines Philips MR Dienstleistungsvertrags.

Autorisierung zum Schutz Ihrer Daten

Um die Zugriffe auf die Daten des Philips MR Release 5 Systems zu kontrollieren, sind die Benutzerrechte entsprechend dem jeweiligen Bedarf eingeschränkt:

- **Ein klinischer Anwender** kann Untersuchungen durchführen und auf alle zuvor durchgeführten Untersuchungen zugreifen, die auf dem System gespeichert sind. Das System verlangt eine Anmeldung, bevor der Anwender auf die Daten zugreifen kann. Bei entsprechender Konfiguration können klinische Anwender veröffentlichte Updates installieren.
- **Mitarbeiter der Krankenhausverwaltung**: kann einfache Verwaltungsaufgaben durchführen, klinische Konten sperren/entsperren und neue Konten für klinische Anwender einrichten. Administratoren können veröffentlichte Updates installieren, haben jedoch keinen Zugriff auf Patientendaten.
- **Kundendiensttechniker**: können die Erstinstallation, Wartungs- und Instandhaltungsaktivitäten durchführen.

Benutzerverwaltung zur verbesserten Zugriffskontrolle und Prozessprotokollierung

MR Version 5 bietet Ihnen die Möglichkeit, mehrere Konten für Anwender und Krankenhausverwaltung einzurichten. Bei beiden Systemen haben Mitarbeiter der Krankenhausverwaltung die Möglichkeit, Kennwortrichtlinien entsprechend den lokalen Sicherheitsanforderungen und -richtlinien festzulegen.

Systeme mit MR Version 5 lassen sich in Ihre LDAP-Umgebung einbinden, so dass Anwender und Gruppen mittels Standard-Netzwerkkonten (d.h. Active Directory) authentifiziert werden können. Kundendiensttechniker können über Zwei-Faktor-Authentifizierung auf das System zugreifen. Dongles können von Philips aktiviert und/oder ihre Aktivierung zurückgezogen werden.

Audit Logging liefert Daten zur Analyse

Philips hat die Audit-Protokollierungsfähigkeiten der MR Release 5 Systeme erweitert. Benutzer können das System so konfigurieren, dass die Protokolle an einen lokalen Systemprotokoll-Server (Syslog-Server) zur Aufbewahrung, Abrufbarkeit und weiteren Analyse gesendet werden. Zur Unterstützung der forensischen Analyse können Benutzer die Einheitlichkeit der Zeitstempel sicherstellen, indem sie die Zeit auf den MR-Systemen mit Ihrem Netzwerk-Zeitserver synchronisieren.

Datenschutz durch Verschlüsselung gespeicherter Patientendaten und während der Datenübertragung

Alle Patientendaten, die auf den Festplattenlaufwerken von Philips MR Release 5 Systemen gespeichert sind, können gemäß den individuellen Anforderungen Ihrer Einrichtung verschlüsselt werden. Darüber hinaus können Sie zur Verschlüsselung von Patientendaten während der Übertragung DICOM mit TLS zur Knotenauthentifizierung ohne Verschlüsselung, DICOM mit Verwendung der TLS-Verschlüsselung oder eine Kombination aus beidem wählen. (Hinweis: Dies erfordert die entsprechende Funktionalität auf Ihrem PACS-System).

Überblick über die Funktionen von Philips MR Version 5

- Firewall-Richtlinie zur Blockierung nicht benötigter Ports
- Härtung des Betriebssystems Microsoft Windows 7 (Hinweis: Die nächste Philips MR Version basiert auf Microsoft Windows 10.)
  - OS-Einstellungen mit CIS-Benchmarks als Grundlage
  - Standardmäßige Deaktivierung nicht erforderlicher Services
  - Deaktivierung der automatischen Ausführung von Wechselmedien und konfigurierbarer Zugriff
- Sicherheitsfunktionen für den Export auf Wechselmedien
  - Bietet die Möglichkeit, den Export von Patientendaten auf Wechselmedien zu deaktivieren (konfigurierbar)
  - Bietet die Möglichkeit, Wechselmedien zu verschlüsseln
- Malware-Schutz mit McAfee Anti-Malware-Lösung in Kombination mit Whitelisting-Richtlinien
- Richtlinie zur Benutzerverwaltung
  - Benutzerverwaltung mit lokalen Konten
  - Unterstützung von mehreren eindeutig zugeordneten Benutzerkonten
  - Unterstützung von mehreren eindeutig zugeordneten Administratorkonten
  - Benutzerverwaltung mit LDAP
  - Unterstützt Active-Directory-Authentifizierung mit LDAP (System gehört der Domäne an)
  - Unterstützt einzelne Konten oder Active-Directory-Gruppen für Benutzer und Administratoren
- Konfigurierbare Kennwortrichtlinien
  - Bietet die Möglichkeit, Kennwortrichtlinien für lokale Konten und LDAP festzulegen
  - Kennwortverlauf (0 bis 24)
  - Minimale Kennwortlänge (0 bis 14)
  - Maximale Kennwortlänge (14 (lokale Authentifizierung), 63 (LDAP))
  - Minimale Kennwortgültigkeit (0 bis 998 Tage)
  - Maximale Kennwortgültigkeit (1 bis 999 Tage)
  - Komplexes Kennwort erforderlich (ja/nein)
  - Richtlinien für Kontosperrung
  - Sperrschwellenwert (0 bis 999 Versuche)
  - Sperrdauer (1 bis 99999 Minuten)
  - Zurücksetzen der Kontosperrung (1 bis 99999 Minuten)
- Bildschirmschoner mit Kennwortschutz – sperrt den Bildschirm nach der festgelegten Inaktivitätsdauer. Der Bildschirmschoner behindert nicht den Scanvorgang (aktiviert/deaktiviert, 1 bis 999 Minuten, Kennwortschutz ja/nein).
- Patientendatenverschlüsselung
  - Bitlocker mit 128-Bit-AES (kann bei der Installation aktiviert werden)
  - DICOM (sichere DICOM-Übertragung durch Zertifikate verwaltet)
- Export von Audit-Log
  - Kontinuierlicher Export von Audit-Logs mittels Syslog möglich

Für Philips hat der Schutz von medizinischen Geräten und der Patientendaten besonders hohe Priorität. Gemeinsam können wir eine sichere Umgebung aufrechterhalten, indem wir wachsam bleiben und die sich ständig verändernden Bedrohungen der Internetsicherheit erkennen. Es ist unser erklärtes Ziel, die spezifischen Bedürfnisse und Anforderungen unserer Kunden zu erfüllen.

Das Sicherheitskonzept des Philips Ingenia MR-Systems wurde von der US Defense Health Agency (DHA) mit dem Zertifikat „Authority to Operate“ (ATO) ausgezeichnet, das auf den Regularien und Risikobewertungen des Risk Management Framework (RMF) basiert. Der risikobasierte Ansatz wurde vom National Institute for Standards and Technology (NIST) für eine strikte Sicherheitsmethode mit kontinuierlicher Überwachung aller die Informationssicherheit betreffenden Kontrollmechanismen erarbeitet.

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

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

www.philips.de/healthcare

4522 991 34083 * SEP 2020