Kurzvorstellung

Schutz von Gesundheitssystemen vor Ransomware

Ransomware ist Malware, die die Daten ihres Opfers meist mittels asymmetrischer Verschlüsselung als Geiseln nimmt. Asymmetrische (öffentlich-private) Verschlüsselung ist eine Form von Kryptografie, bei der ein Schlüsselpaar zum Ver- und Entschlüsseln einer Datei verwendet wird. Der Angreifer generiert das einmalige öffentlich-private Schlüsselpaar für das Opfer, wobei der private Schüssel für die Entschlüsselung der Dateien auf dem Server des Angreifers abgelegt wird. Der Angreifer verspricht dem Opfer, ihm den privaten Schlüssel nach Zahlung eines Lösegeldes auszuhändigen – ein Versprechen, das in der Vergangenheit nicht immer gehalten wurde. Ohne Zugang zu diesem privaten Schlüssel ist es praktisch unmöglich, die in Geiselhaft genommenen Dateien zu entschlüsseln.

Ransomware beschäftigt alle Sicherheitsexperten bereits seit mehreren Jahren sehr stark. Leider ist Ransomware ein einfaches und gleichzeitig effektives Tool für Cyber-Angriffe, mit dem sich leicht Geld verdienen lässt. Im vergangenen Jahr wurden statt Einzelpersonen immer häufiger Unternehmen angegriffen, da diese höhere Lösegelder zahlen. In letzter Zeit wurden Krankenhäuser zu beliebten Zielen für Ransomware-Autoren. Im *McAfee Labs Threat-Report vom September 2016* untersuchen wir Ransomware-Angriffe auf Krankenhäuser aus dem 1. und 2. Quartal. Wie sich zeigt, waren diese Angriffe erfolgreich, verwandt sowie gezielt und dennoch eher wenig raffiniert. Wir erläutern außerdem krankenhausspezifische Probleme in Bezug auf Ransomware, z. B. veraltete Systeme, medizinische Geräte mit schlechter Sicherheit sowie die Tatsache, dass der sofort verfügbare Zugriff auf Informationen über Leben und Tod entscheiden kann.

Richtlinien und Vorgehensweisen zum Schutz vor Ransomware

Der wichtigste Schritt zum Schutz der Systeme vor Ransomware besteht darin, sich des Problems bewusst zu sein und die Verbreitungswege zu kennen. Folgende Richtlinien und Verfahren sollten von Krankenhäusern befolgt werden, um die Aussicht auf Erfolg von Ransomware-Angriffen zu minimieren.

- Erstellen Sie einen Aktionsplan für den Fall eines Angriffs. Erfassen Sie, wo sich die wichtigen Daten befinden, und stellen Sie fest, ob diese infiltriert werden können. Führen Sie mit dem Notfall-Management-Team des Krankenhauses Übungen zur Sicherstellung des störungsfreien Geschäftsbetriebs und der Wiederherstellung nach einem Systemausfall

intel Security

durch, um den Wiederherstellungspunkt und die Zeitziele zu validieren. Bei diesen Übungen können verborgene Folgen für die Krankenhaus-Abläufe aufgedeckt werden, die bei normalen Backup-Tests nicht sichtbar werden. Die meisten Krankenhäuser zahlten das Lösegeld, weil ein Notfallplan fehlte!

- Halten Sie die Systeme auf dem neuesten Patch-Stand. Viele von Ransomware missbrauchte Schwachstellen können mit Patches geschlossen werden. Halten Sie Betriebssysteme, Java, Adobe Reader, Flash und Anwendungen mit Patches auf dem neuesten Stand. Sie sollten ein Verfahren zur Patch-Installation ausarbeiten und überprüfen, ob die Patches ordnungsgemäß installiert wurden.
- Minimieren Sie das Risiko für ältere Krankenhaus-Systeme und -Geräte, die nicht gepatcht werden können, mit Anwendungs-Whitelists, die Systeme abriegeln und die Ausführung nicht genehmigter Programme verhindern. Trennen Sie diese Systeme und Geräte mit einer Firewall und einem Eindringungsschutz-System vom restlichen Netzwerk. Deaktivieren Sie nicht benötigte Dienste und Ports auf diesen Systemen, um die Zahl der möglichen Infektionseintrittspunkte zu reduzieren.
- Schützen Sie Ihre Endgeräte. Nutzen Sie Endgeräteschutz und fortschrittliche Funktionen. In vielen Fällen wird der Client lediglich mit aktivierten Standardfunktionen installiert. Durch die Implementierung einiger hochentwickelter Funktionen (z. B. zum Verhindern, dass ausführbare Dateien aus einem Temp-Ordner ausgeführt werden) kann mehr Malware erkannt und blockiert werden.
- Wenn möglich, verhindern Sie die Speicherung sensibler Daten auf lokalen Laufwerken. Legen Sie fest, dass Daten in sicheren Netzwerkfreigaben gespeichert werden müssen. Dadurch reduziert sich die Ausfallzeit, da infizierte Systeme durch Aufspielen sauberer Images schnell wiederhergestellt werden können.
- Nutzen Sie Spam-Schutz. Am Anfang der meisten Ransomware-Kampagnen steht eine Phishing-E-Mail mit einem Link oder einem typischen Anhang. Bei Phishing-Kampagnen, die ihre Ransomware in eine SCR-Datei oder ein anderes ungewöhnliches Dateiformat packen, kann problemlos eine Spam-Regel zur Blockierung dieser Anhänge eingerichtet werden. Wenn ZIP-Dateien durchgelassen werden sollen, sollten sie mindestens zwei Ebenen tief auf mögliche böswillige Inhalte durchsucht werden.
- Blockieren Sie unerwünschte oder überflüssige Programme oder Datenverkehr. Wenn keine Notwendigkeit für die Nutzung von Tor besteht, sollten Sie die Anwendung und ihren Datenverkehr in Ihrem Netzwerk blockieren. Dadurch können Sie häufig verhindern, dass die Ransomware den öffentlichen RSA-Schlüssel vom Kontroll-Server abrufen kann, sodass die Verschlüsselung blockiert wird.
- Erstellen Sie Netzwerksegmente für Geräte, die für die Patientenversorgung dringend erforderlich sind.
- Bewahren Sie Sicherungen getrennt vom Netzwerk auf. Stellen Sie sicher, dass Systeme, Speicher und Bänder für Sicherungen an einem Ort aufbewahrt werden, auf den von Systemen in den Produktionsnetzwerken nicht zugegriffen werden kann. Wenn sich Schaddaten aus Ransomware-Angriffen innerhalb des Netzwerks bewegen, können sie andernfalls gesicherte Daten beschädigen.
- Nutzen Sie virtuelle Infrastrukturen für wichtige elektronische medizinische Datenverwaltungssysteme, die vom Rest des Produktionsnetzwerks getrennt sind.
- Führen Sie regelmäßig Benutzerschulungen zur Verbesserung des Sicherheitsbewusstseins durch. Die meisten Ransomware-Angriffe beginnen mit einer Phishing-E-Mail. Daher ist die Sensibilisierung der Benutzer absolut unverzichtbar. Statistiken zeigen, dass von zehn E-Mails, die von Angreifern gesendet wurden, mindestens eine erfolgreich ist. Öffnen Sie keine E-Mails oder Anhänge von unbekannten oder nicht überprüften Absendern.

So kann Intel Security-Technologie vor Ransomware schützen

McAfee VirusScan Enterprise und McAfee Endpoint Security 10

- McAfee VirusScan Enterprise (VSE) oder McAfee Endpoint Security (ENS) bieten folgende Vorteile:
  - Verwenden Sie McAfee ePolicy Orchestrator (ePO), um täglich die aktuellsten DAT-Dateien bereitzustellen.
  - Stellen Sie sicher, dass McAfee Global Threat Intelligence (McAfee GTI) aktiviert ist. McAfee GTI enthält mehr als 7 Millionen verschiedene Ransomware-Signaturen.
  - Entwickeln Sie Zugriffsschutzregeln, um die Installation und Ausführung von Ransomware-Schaddaten zu verhindern. Informationen dazu finden Sie in den Wissensdatenbank-Artikeln KB81095 und KB54812.
  - Verwenden Sie die dynamische Anwendungsprozess-Eindämmung, um zu verhindern, dass unbekannte Anwendungen böswillige Aktivitäten durchführen können.

McAfee Threat Intelligence Exchange

- Richten Sie in McAfee Threat Intelligence Exchange (TIE) folgende Richtlinien ein:
  - Starten Sie den Beobachtungsmodus.
  - Wenn Endgeräte als verdächtige Prozesse erkannt werden, verwenden Sie System-Tags zum Anwenden von McAfee TIE-Durchsetzungsrichtlinien.
  - „Säubern“ bei Reputation „bekannt böswillig“.
  - „Blockieren“ bei Reputation „höchstwahrscheinlich böswillig“ (die Blockierung bei Status „unbekannt“ würde besseren Schutz bieten, aber möglicherweise auch den Anfangsaufwand für Administratoren erhöhen).
  - Senden Sie Dateien an McAfee Advanced Threat Defense (ATD) ein, deren Reputation als „unbekannt“ und schlechter eingestuft ist.
  - TIE-Server-Richtlinie: McAfee ATD-Reputationen für Dateien akzeptieren, die noch nicht von McAfee TIE überprüft wurden.
- Manuelle Interventionen durch McAfee Threat Intelligence Exchange:
  - Durchsetzung der Datei-Reputation (je nach Betriebsmodus).
  - Höchstwahrscheinlich böswillig: Säubern/löschen.
  - Möglicherweise böswillig: Blockieren.
  - Die Reputation innerhalb des Unternehmens kann McAfee GTI außer Kraft setzen. Sie können optional festlegen, dass unerwünschte Prozesse blockiert werden (z. B. nicht unterstützte oder anfällige Anwendungen). Kennzeichnen Sie die entsprechende Datei als „Möglicherweise böswillig“.
  - Beziehen Sie Reputations-Daten von Drittanbietern als Kompromittierungs-indikatoren in McAfee TIE ein.

McAfee Advanced Threat Defense

- McAfee Advanced Threat Defense enthält standardmäßig folgende Erkennungsfunktionen:
  - Erkennung auf Signaturbasis: Signaturen, die von McAfee Labs gepflegt werden (umfassen mehr als 150 Millionen Signaturen, inklusive CTB-Locker, CryptoWall und den entsprechenden Varianten).
  - Erkennung auf Reputationsbasis: McAfee GTI.
  - Statische Analyse und Emulation in Echtzeit: Werden zur signaturlosen Erkennung verwendet.
  - Benutzerdefinierte YARA-Regeln.
  - Vollständige statische Code-Analyse: Führt ein Reverse Engineering des Datei-Codes durch, um Attribute und Befehle zu untersuchen und den Code vollständig zu analysieren, ohne ihn dabei auszuführen.
  - Dynamische Sandbox-Analyse.

- Erstellen Sie Analyseprofile für die Bereiche, unter denen Ransomware wahrscheinlich ausgeführt werden soll:
  - Verbreitete Betriebssysteme, Windows 7, Windows 8, Windows XP.
  - Installieren Sie Windows-Anwendungen (Word, Excel), und aktivieren Sie Makros.
- Legen Sie individuelle Analyseprofile für die einzelnen Betriebssysteme mit Internetzugriff fest:
  - Viele Malware-Varianten führen ein Skript aus einem Microsoft Office-Dokument aus, das eine ausgehende Verbindung herstellt und den Schadcode aktiviert. Mit einem Analyseprofil mit Internetverbindung wird die Erkennungsrate verbessert.

McAfee Application Control

- McAfee Application Control bietet Schutz durch eine Anwendungs-Whitelist. Damit können alle Gerätetypen ideal geschützt werden, insbesondere:
  - Statische Geräte wie medizinische Geräte.
  - Systeme mit älteren Betriebssystemen, die keine Aktualisierungen mehr erhalten.
  - Anwendungs-Server, die eine begrenzte Anzahl von Diensten zur Verfügung stellen.
  - Systeme, die selten geändert werden.
- Erstmalige Installation
  - McAfee Application Control scannt das System während der Installation vollständig und erstellt eine Whitelist des Endgeräte-Inventars und der Anwendungen.
- Beobachtungsmodus
  - Ermöglicht es Administratoren, neu installierte/gestartete Anwendungen nachzuverfolgen. Dabei besteht die Option, diese Anwendungen in die zentrale Whitelist aufzunehmen, wenn sie als autorisiert definiert werden.
  - Unterstützt die Whitelist-Pflege, indem neue vertrauenswürdige Aktualisierungsprogramme für Anwendungen in der Umgebung erkannt werden.
  - Erkennt Elemente, die neu in die Whitelist aufgenommen werden sollen, z. B. bestätigte Prozesse, Zertifikate, Verzeichnisse oder Benutzer.
- Selbstgenehmigungsmodus
  - Benutzer können in der Whitelist nicht enthaltene Anwendungen genehmigen. Diese Funktion erhöht die Flexibilität und verringert die Auswirkungen auf die geschäftlichen Abläufe.
  - Administratoren können von Benutzern bestätigte Inhalte zentral verfolgen und die Autorisierung der Anwendung basierend auf der Reputation und den Unternehmensrichtlinien akzeptieren oder widerrufen.
- Durchsetzung der Whitelist
  - Das System ist vollständig vor unbekannten Anwendungen wie böswilligen Anwendungen (z. B. Ransomware) geschützt.
  - Bietet die Möglichkeit, den Endbenutzer über die erforderliche Genehmigung neuer ausführbarer Dateien zu benachrichtigen.

Weitere Informationen

Intel Security Expert Center-Community

- McAfee VirusScan Enterprise
- McAfee Endpoint Security
- McAfee Threat Intelligence Exchange
- McAfee Advanced Threat Defense
- McAfee Application Control

916_0816_brf_protecting-health-care-systems-ransomware

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com