

Faith Regional Health Services impft sich selbst gegen Schadsoftware

Gesundheitsdienstleister blockiert Schadsoftware und Exploits mit Malwarebytes Endpoint Security

BRANCHE

Gesundheitswesen

AUFGABE

Stoppen einer Schadsoftware-Epidemie, die die Techniker von der Durchführung von Projekten abhielt, die zur Verbesserung der Patientenpflege beitragen

IT-UMGEBUNG

Ein Data Center mit Microsoft Security Central und Check Point 4800 Appliance mit Firewall, Sophos AV, App-Control, Virtual Private Network (VPN) und Intrusion Prevention System (IPS)

LÖSUNG

Malwarebytes Endpoint Security einschließlich Anti-Malware, Anti-Exploit und der Management Console

ERGEBNISSE

- Verringerung der Bedrohung von mehreren Tausend auf Null
- Einsparung von Arbeitsstunden und -tagen für die Bereinigung der Geräte durch die Techniker
- Steigerung der Benutzerzufriedenheit mit der PC-Leistung
- Vereinfachung der Wahrung der HIPAA- und PCI DSS-Konformität

Profil

Faith Regional Health Services gewährleistet seit 1923 die Gesundheitsversorgung der Einwohnern des Nordostens von Nebraska. Derzeit versorgt das Unternehmen 156.000 Menschen in 13 Verwaltungsbezirken und bietet seine medizinischen Leistungen in einem Krankenhaus mit 200 Betten, in 20 Kliniken und an 12 dezentralen Standorten an. Als Faith Regional von einer Schadsoftware-Epidemie getroffen wurde, entschied sich das Unternehmen für eine Heilkur mittels Malwarebytes.

Es befand sich Schadsoftware in unserer Umgebung, und das bereitete uns im Hinblick auf die Wahrung der HIPAA- und PCI DSS-Konformität große Sorge. Jetzt sind wir sicher, dass Schadsoftware der Konformität nichts anhaben kann.

—Paul Feilmeier, IT Infrastructure Manager,
Faith Regional Health Services

Die Aufgabe

Beseitigen der frustrierenden, den Betrieb unterbrechenden Schadsoftware

Eine zunehmende Welle an Schadsoftware breitete sich im Help Desk von Faith Regional sowie unter den Servicetechnikern aus. Angesichts der Flut von 20 bis 30 PCs pro Woche, die aufgrund von Schadsoftware bereinigt werden mussten oder ein Reimaging erforderten, war die Situation für alle Beteiligten frustrierend — Techniker, Mitarbeiter der Geschäftsstellen und Mediziner.

Die Mitarbeiter verloren wertvolle Arbeitszeit, während die Geräte einer Heilkur unterzogen wurden. Für die Mediziner waren die Ausfallzeiten frustrierend, da sie auch zu einer Unterbrechung der Patientenpflegetätigkeiten führten. Selbst wenn die IT-Techniker ein Ersatzgerät bereitstellen konnten, mussten zunächst der neue Endpunkt konfiguriert und die grundlegenden Anwendungen und der Netzwerkzugang eingerichtet werden. Wenn infizierte PCs in einer Klinik erkannt wurden, musste ein Mitglied des IT-Teams zum entsprechenden Standort reisen, um die Infektion zu beheben. Das bedeutete manchmal den Verlust eines kompletten Arbeitstages für die Bereinigung von nur einem einzigen Gerät.



Schadsoftware wie etwa Bots und andere Command-and-Control-Bedrohungen konnten außerdem die Daten über die Endpunktgeräte gefährden und die HIPAA- und PCI DSS-Konformität aufs Spiel setzen. Bei mehreren Dutzend bestehenden Kontrollen, die die Einhaltung der Anforderungen dieser Standards für Faith Regional gewährleisten sollen, brauchte das IT-Team nicht noch mehr Kummer.

„Wir benötigten eine bessere Methode, die zunehmende Flut an Schadsoftware und Bots einzudämmen“, sagte Paul Feilmeier, IT Infrastructure Manager bei Faith Regional Health Services. „Unsere Sophos Antivirenlösung spürte Viren auf, erkannte jedoch Schadsoftware nicht effektiv.“ Das IT-Team begann die Auswertung seiner Möglichkeiten zur Bekämpfung von Schadsoftware und entschied sich dann für Malwarebytes Endpoint Security.

Die Lösung

Malwarebytes Endpoint Security

Malwarebytes Endpoint Security bietet eine leistungsfähige, mehrstufige Verteidigung zur Abwehr der neuesten und gefährlichsten Schadsoftware einschließlich Ransomware. Malwarebytes Endpoint Security umfasst Malwarebytes Anti-Malware, Anti-Exploit und die Management Console in einer einzigen, umfassenden Lösung. Der Systemadministrator von Faith Regional installierte Malwarebytes an den Endpunkten und auf den Servern und generierte die ersten Berichte in nur zwei Tagen.

Das Gegenmittel gegen Schadsoftware

„Nach der Implementierung von Malwarebytes erhielten wir erstaunliche Berichte“, sagte Feilmeier. „Tausende Dateien auf unseren Geräten waren infiziert. Unsere Anwender mussten angesichts der Auswirkungen von so viel Schadsoftware extrem frustriert gewesen sein.“

Malwarebytes deckte Duzende verschiedener potenziell unerwünschter Programme (PUPs) und potenziell unerwünschter Änderungen (PUMs) auf. Es blockierte den Zugriff auf zahlreiche schadhafte Websites. Und Malwarebytes Anti-Exploit schützte die Geräte erfolgreich gegen Exploits einschließlich Heap-Sprayings, schadhafte Inhalt-Downloads, Java-Exploits, ROP-Angriffe und ASLR-Umgehungsversuche.

Die tägliche Erkennung von Bedrohungen fiel von 1.800 auf Null.

„Die Management Console hat außerdem aufgezeigt, welche Benutzergruppen weiterhin Probleme mit Schadsoftware hatten“, berichtete er. „Dies hat uns ermöglicht, unsere Anwender besser über die Online-Bedrohungen aufzuklären und ihnen zu raten, was man besser nicht anklickt.“

Aufrechterhaltung einer robusten Gesundheit und der Normkonformität

Mit Malwarebytes war Faith Regional in der Lage, die Schadsoftware zu beseitigen und fernzuhalten. Die Software aktualisiert aktiv die Definitionen und überwacht die Endpunkte und Server bei einem äußerst geringen bis gar keinem Aufwand für die Techniker. Wenn der Netzwerktechniker verdächtige Netzwerkaktivitäten bemerkt, alarmiert er das Desktop-Team. Das Team kann dann das Gerät dezentral scannen und von Schadsoftware befreien. Der Benutzer merkt dies nicht einmal, und die Produktivität leidet hierunter nicht.

„Es befand sich Schadsoftware in unserer Umgebung, und das bereitete uns im Hinblick auf die Wahrung der HIPAA- und PCI DSS-Konformität große Sorge“, meinte Feilmeier. „Jetzt sind wir sicher, dass Schadsoftware der Konformität nichts anhaben kann.“

Neufokussierung auf Projekte, die die Patientenpflege verbessern

Die Techniker haben ausdrücklich betont, dass Malwarebytes eine großartige Investition sei - und sie erleben die Vorzüge jeden Tag. Sie haben Zeit gewonnen, um sich auf neue Projekte anstatt auf Problemfälle zu konzentrieren. Die Mitarbeiter des Help Desk und des Außendienstes verbringen jetzt mehr Zeit mit dem Pflegepersonal, um aktiv neue Anwendungen und Funktionen im Krankenhaus und in den Kliniken zu implementieren.


„Häufig realisieren unsere Anwender die Auswirkungen der Informationstechnologie auf die Patientenpflege nicht“, sagte Feilmeier. „Aber wenn die PCs stabil laufen, sind die Mediziner nicht frustriert. Alles läuft viel reibungsloser. Und dies alles trägt zu einer besseren Patientenerfahrung und -pflege bei.“




Malwarebytes stellt Antischadsoftware und Anti-Exploit-Software bereit, mit denen Unternehmen und Endanwender vor Zero-Day-Bedrohungen geschützt werden, die sich fortlaufend der Erkennung durch herkömmliche Antivirenlösungen entziehen. Malwarebytes Anti-Malware erhielt von den Redakteuren von CNET die Bewertung „Outstanding“ (Hervorragend), wurde von PCMag.com zur Editor's Choice auserkoren und erreichte bei einem Test von AV-TEST.org als einzige Sicherheitssoftware die Höchstpunktzahl für die Entfernung von Schadsoftware. Darum vertrauen mehr als 38.000 KMU und Großunternehmen weltweit in Bezug auf den Schutz ihrer Daten auf Malwarebytes. Das im Jahr 2008 gegründete Unternehmen Malwarebytes mit Hauptgeschäftssitz in Kalifornien verfügt über Standorte in ganz Europa und beschäftigt ein global agierendes Forschungs- und Expertenteam.

 Santa Clara, CA

 malwarebytes.com

 corporate-sales@malwarebytes.com

 1.800.520.2796