Schutz eines Klinikbetriebs gegen Cyber-Angriffe

Das Klinikum Arnsberg bildet einen Klinikverbund, der aus dem Marienhospital in Arnsberg, dem Karolinen-Hospital in Hüsten und dem St. Johannes-Hospital in Neheim besteht. Die Organisation, die auch als Lehrkrankenhaus der Universität Münster fungiert, umfasst 25 Kliniken und 4 Institute bei insgesamt 728 Planbetten. Es werden Akut- und Notfallpatienten versorgt, angeschlossen ist außerdem eine Pflegeeinrichtung mit 90 Plätzen.

Die Herausforderung

Lebenswichtige Technik schützen

IT im Krankenhaus hat eine besonders kritische Bedeutung. Sie muss zuverlässig funktionieren, damit ihr Betreiber Leben retten kann. Im Februar 2016 verzeichnete das Klinikum Arnsberg einen Vorfall, bei dem Angreifer die bereits vorhandenen Sicherheitssysteme überwinden konnten: Malware hatte sich ihren Weg über Links in Social-Engineering-Mails in die IT-Landschaft des Klinikverbunds gebahnt.

Da die wesentlichen medizinischen Geräte auch ohne Anbindung ans Netz funktionieren, war die Versorgung der Patienten jederzeit uneingeschränkt sichergestellt. Die Klinik-internen Kommunikationsprozesse allerdings mussten fast zwei Tage lang mit erhöhtem Aufwand manuell abgewickelt werden. „In unserem Fall haben es die Mitarbeiter mit gewaltigem Engagement geschafft, den Betrieb mittels ‚Zettelwirtschaft' über die Ausfallzeit zu retten", erinnert sich Stefan Peters, Leitung Geschäftsbereich IT beim Klinikum Arnsberg, „aber über einen längeren Zeitraum hinweg hätten wir unsere Arbeit so nicht bewältigen können." Neue Patienten etwa konnten nur noch in dringenden Fällen aufgenommen werden. Am Ende verzeichnete das Klinikum einen Schaden in siebenstelliger Höhe.

Klinikum Arnsberg
Akademisches Lehrkrankenhaus
Westfälische Wilhelms-Universität Münster

Organization
Klinikum Arnsberg

Branche
Gesundheitswesen, Kliniken

Umfang
Echtzeit-Loganalyse über mehrere Standorte

Projektziele
- Erkennung laufender Angriffe
- Aufbau eines Frühwarn-Systems
- Höhere IT-Verfügbarkeit auch im Angriffsfall

„Man hört immer, SIEM-Einführungen seien endlos und hoch komplex", erinnert er sich, „aber in unserem Fall konnten wir innerhalb kürzester Zeit Resultate vorweisen."

- Stefan Peters, Leitung Geschäftsbereich IT beim Klinikum Arnsberg

Die Lösung

Früh gewarnt vor Cyber-Angriffen

Um weiteren Attacken dieser Art künftig besser begegnen zu können, entschied sich das Klinikum unter anderem dafür, in ein Frühwarn-System gegen Cyber-Angriffe zu investieren. Ziel war es, Attacken schneller aufdecken und eingrenzen zu können, etwa um Bereiche der Technik in Zukunft auch sektorenweise außer Betrieb nehmen zu können. Die Aktions- und Kommunikationsfähigkeit sollte in zukünftigen schwierigen Situationen so weit wie möglich erhalten bleiben. Als mögliche Lösung prüfte man früh die Implementierung eines Security-Information-und-Event-Management-Systems (SIEM).

Da bereits eine Geschäftsbeziehung zwischen dem Dienstleistungspartner DTS und dem Klinikum Arnsberg bestand und man sich häufiger über Security-Themen ausgetauscht hatte, nahm die IT des Krankenhaus-Verbunds Kontakt mit DTS auf. Man vereinbarte die Evaluation eines SIEM-Systems von LogRhythm.

„Man hört immer, SIEM-Einführungen seien endlos und hoch komplex", erinnert sich Peters, „aber in unserem Fall konnten wir innerhalb kürzester Zeit Resultate vorweisen." Das LogRhythm-System selbst etwa ließ sich von vier Stunden in Betrieb nehmen, anschließend begann sofort die Anbindung der zuvor ausgewählten Logquellen. Bereits am zweiten Tag war es möglich, die ersten Korrelationsregeln einzuschalten. Bereits in dieser Phase erkennt LogRhythm beispielsweise Ransomware, alarmiert die Security-Teams und ermöglich es ihnen, die Attacke innerhalb von wenigen Sekunden weitgehend automatisiert zu stoppen.

Flexibilität bewies das LogRhythm-System, als es darum ging, auf das Golden-Image-Verfahren der Server im Klinikum zu reagieren. Die Images werden wöchentlich mehrfach kopiert und die Systeme anschließend gestartet, was die Log-Auswertung nicht stören darf. Hier machte es die Agentenfunktionalität von LogRhythm möglich, einmalig einen Log Collection Agent per Server zu installieren und zu konfigurieren. Anschließend wurde die Agenten-/Logquellen-Konfiguration jeder Server-Kopie automatisiert zentral gespeichert und bei jedem Neustart neu auf das Zielsystem gepusht. Damit entfällt im Klinikum eine komplizierte manuelle wöchentliche Neuinstallation und Konfiguration der Logquellen der Image-Server.

Schon im Juni 2016 fiel schließlich die Entscheidung, LogRhythm produktiv einzusetzen.

Erfolgreicher Übergang in den Betrieb

Ein Immun-System gegen Cyber-Angriffe

Bereits mit dem ersten Alarm erhalten die Security-Analysten im Klinikum nun genaue und übersichtlich aufbereitete Informationen über die festgestellten schädlichen Vorgänge – dazu gehören der Name des bösartigen Prozesses sowie die Namen bereits infizierter Dateien. Auf Knopfdruck sind weitere Informationen abrufbar, darunter Hinweise auf mögliche andere infizierte Hosts. „Solche Informationen sind es, die es uns bei der ursprünglichen Attacke erlaubt hätten, gezielter zu reagieren und der Malware entweder komplett einen Riegel vorzuschieben oder beispielsweise Systeme in Betrieb zu halten, die mit Sicherheit noch nicht betroffen waren", beschreibt Stefan Peters den Vorteil der schnellen Bereitstellung von Angriffsdetails. Das System lässt sich problemlos vom vorhandenen IT-Security-Stab betreiben. „Die Investition lohnt sich – sie erhöht die Schlagkraft unseres Security-Teams zu vertretbaren Kosten ungemein", zieht Peters Resümee.