Case Study

Wie der internationale Verpackungsmittelhersteller MAUSER ein vernetztes und anpassungsfähiges IT-Sicherheitssystem verwirklicht

Die MAUSER Gruppe

Kundenprofil
Internationaler Verpackungsmittelhersteller

Gewerbe
Produktionstechnik

IT-Umfeld
1.200 Endpunkte in 80 Produktionsstätten in 16 Ländern, vier regionale Rechenzentren

Aufgaben und Herausforderungen
- Schnellere Erkennung von Malware
- Zunehmende Häufung von Malware-Angriffen durch das MPLS-Netzwerk
- Lösung, die alle rechtlichen Anforderungen erfüllt, konform mit staatlichen Regulierungen ist und ISO-Zertifizierungen vorweist
- Druck internationaler Kunden und Aktionäre, sich gegen Datenpannen abzusichern

Intel Security-Lösungen
McAfee® Enterprise Security Manager, McAfee Advanced Threat Defense, McAfee Threat Intelligence Exchange, McAfee Global Threat Intelligence, McAfee Application Data Monitor, McAfee Complete Endpoint Protection Enterprise-Advanced

Ergebnisse
- Bereits 12 Stunden nach der Inbetriebnahme wurde mindestens ein Angriff verhindert
- Zeitspannen, um Schadprogramme zu erkennen, einzudämmen und die verursachten Probleme zu beheben, wurden stark reduziert
- Reduzierte Anzahl an Vorfällen, in denen die Sicherheit gefährdet war
- Erhöhte Effizienz im Tagesgeschäft

Das in Deutschland ansässige Unternehmen ist auf dem richtigen Weg, ein flexibles Abwehrsystem gegen IT-Sicherheitsgefahren zu realisieren. Im Gegensatz zu zahlreichen Einzellösungen, gelingt es dem neu eingeführten Sicherheitsmodell, sowohl Daten und Arbeitsabläufe, als auch Management-Dashboards in eine zentral zu verwaltende und erweiterbare Umgebung zu integrieren, was Arbeitsprozesse vereinfacht und beschleunigt.

Thomas Langer, Leiter der Abteilung für Netzwerk- und IT-Sicherheit des europäischen Zweiges des internationalen Verpackungsmittelherstellers MAUSER, beschäftigte sich schon länger damit, ein optimales Sicherheitssystem in seinem Unternehmen zu integrieren. Das System sollte in der Lage sein, Daten der Gefahrenanalyse und den damit zusammenhängenden Informationen mit allen Endpunkten, Netzwerken und Schnittstellen in allen 80 Produktionsstätten und vier Rechenzentren zu teilen, um dann unverzüglich und ohne zusätzliches menschliches Eingreifen auf aktuelle Geschehnisse angemessen reagieren zu können. Darüber hinaus sollte die Lösung aus vergangenen Vorfällen lernen können, um sich so eigenständig zu verbessern und sich zu einer intelligenten und anpassungsfähigen Abwehr gegen zukünftige Cyber-Bedrohungen zu formieren.

Warum Intel Security? Der einzige Anbieter mit einer langfristigen Vision

Tatsächlich entschied sich MAUSER im Jahre 2013, seine einzelnen Sicherheitsanbieter zu konsolidieren und eine integrierte Lösung für alle Aspekte der IT-Sicherheit zu finden. Langer begann, gemeinsam mit Mitarbeitern aus dem Netzwerk- und Sicherheitsteam, nach einem Anbieter zu suchen, der MAUSER bei der Implementierung eines offenen, miteinander vernetzten Sicherheitssystems unterstützen kann.

„Intel Security war das einzige Unternehmen das uns helfen konnte, unsere mittel- bis langfristige Strategie zu optimieren", erklärt Langer. „Dass Intel zudem McAfee übernahm, hat unsere Entscheidung noch gefestigt. Der Umfang der McAfee-Lösungen und die Marktstärke von Intel gab uns die Gewissheit, dass Intel Security seinen Ansprüchen bezüglich ganzheitlichen Sicherheitssystemen gerecht werden würde und Sicherheitsstandards sogar neu definieren könnte. Kein anderer Anbieter ist in der Lage, dies zu leisten." Langer weist zudem darauf hin, dass große Datenpannen seit der Implementierung der Lösungen deutlich seltener vorfallen. Dies bestätigt ihn darin, dass sich MAUSER mit seiner IT-Sicherheitsstrategie auf dem richtigen Weg befindet: „Selbst die leistungsfähigsten Einzellösungen sind in ihrer Effektivität eingeschränkt, solange sie nicht die relevanten Informationen miteinander austauschen und so voneinander lernen."

Vernetzte Lösungen und der Austausch von Bedrohungsinformationen

Um seine neue, umfassende Strategie zu verfolgen, erwarb und implementierte MAUSER den McAfee Enterprise Security Manager als SIEM, zusammen mit der McAfee Advanced Threat Defense Appliance – welche dynamische und statische Code-Analysen nach der Sandbox-Technik durchführt – sowie McAfee Threat Intelligence Exchange und Application Data Monitoring. McAfee Threat Intelligence Exchange sorgt dafür, dass sämtliche globale, lokale sowie Daten bezüglich Gefahrenaufklärung die von Dritten und dem eigenen Unternehmen stammen, zwischen allen Sicherheitslösungen die mit McAfee Threat Intelligence Exchange verbunden sind, geteilt werden. Dieses System läuft über den McAfee Data Exchange Layer, eine bidirektionale Schnittstelle, die dazu dient, Daten und Prozessinformationen auszutauschen. McAfee Application Data Monitoring überwacht dazu wichtige Netzwerkdienste, wie z.B. DNS.

Das Sicherheitskonzept von Intel Security, das bisher für den Schutz von MAUSER's Endgeräten zuständig war, sah immer

schon die Möglichkeit der Automatisierung und Integration weiterer Einzelsysteme vor. Doch durch die Ergänzung der McAfee Advanced Threat Defense Appliance, dem McAfee Enterprise Security Manager sowie McAfee Threat Intelligence Exchange hebt die MAUSER Gruppe ihre Gefahrenprävention auf ein höheres, bisher unerreichtes Niveau. So vereinfacht McAfee Advanced Threat Defense Appliance die Entdeckung von besonders hartnäckigen und zielgerichteten Angriffen. Zeitgleich macht McAfee Enterprise Security Manager Bedrohungen und Risiken schneller sichtbar, die mithilfe von McAfee Threat Intelligence Exchange gemeinsam mit vielen anderen relevanten Daten mit dem gesamten Unternehmensnetzwerk geteilt werden. Darüber hinaus lernen alle Systeme, die mit McAfee Threat Intelligence Exchange verbunden sind, auf Basis jener Informationen voneinander und können ihren Schutz sowie Ihre Erkennungsfunktionen im Laufe der Zeit anpassen und verbessern.

Durch die Verbindung von McAfee Threat Intelligence Exchange mit dem McAfee Enterprise Security Manager, der McAfee Advanced Threat Defense Appliance und dem McAfee ePolicy Orchestrator® (ePO™) – die Konsole, mit der MAUSER bisher seine Endpunkte verwaltete – ist das Unternehmen auf einem guten Weg all seine Ziele bezüglich IT-Sicherheit zu erreichen.

Die Rechtfertigung gegenüber dem CIO und CFO

Langer zufolge war es nicht allzu schwierig, den Chief Financial Officer (CFO) von dem Vorhaben zu überzeugen, das neue Intel Security-System zu erwerben. „Wir legten dar, wie wichtig diese Lösungen für unsere langfristige IT-Sicherheitsstrategie sind, aber auch, dass sie notwendig sein würden, um den aktuellen Rechts- sowie Compliance-Anforderungen zu genügen“, so Langer. „Wir erklärten die Vorteile des McAfee Enterprise Security Managers gegenüber der Einstellung von neuen Mitarbeitern, die die Belegschaft weiter vergrößern würden, nicht abgeschrieben werden könnten und nicht ansatzweise so effektiv arbeiten könnten, wie ein System, dass über 24 Millionen Eingänge pro Tag analysiert. Er hat verstanden, worauf wir hinauswollten.“

Um auch dem CIO das neue Sicherheitskonzept sowie die Rolle von Intel Security darin näherzubringen, lud das Sicherheitsteam ihn in das Intel Security Executive Briefing Center (EBC) in Amsterdam ein. Im dort stattfindenden Meeting wurde ihm von Vorstandsmitgliedern von Intel Security das vernetzte Sicherheitskonzept demonstriert. Nachdem auf seine Fragen und Bedenken durch Sicherheitsexperten eingegangen wurde, war er vom neuen, integrierten Sicherheitssystem überzeugt.

Automatisierung als Grundlage für eine nachhaltige Bedrohungsbekämpfung

Einer der Aspekte, die Langer am vernetzten Intel Security-System am meisten begeistert, sind die Antworten, die es automatisch auf jede Art von Störfällen parat hat. In Zukunft soll beispielsweise ein infizierter Computer automatisch vom Netz getrennt und unter Quarantäne gestellt werden, wenn er versucht Schadsoftware zu verbreiten. Gleichzeitig soll automatisch eine Firewall-Regel erstellt werden, die ihn daran hindert, weiter auf das Netzwerk oder Internet zuzugreifen.

„Unsere Computer sind über die ganze Welt verteilt und ich kann nicht rund um die Uhr arbeiten. Wenn aber das Intel Security-System etwas Verdächtiges entdeckt, kann ich darauf vertrauen, dass es die entsprechenden Gegenmaßnahmen ergreift und mir die Details in einem Bericht zukommen lässt, den ich lesen kann, sobald ich wieder im Büro bin“, erklärt Langer.

Langer sieht auch einer zukünftigen Automatisierung von Arbeitsabläufen mit Hilfe von Intel Security gelassen entgegen – zum Beispiel, wenn es darum geht, die Windows-Geräte mit neuen Service Packs zu aktualisieren. Zieht man in Betracht, dass die MAUSER Gruppe nur über eine begrenzte Anzahl an Mitarbeitern verfügt, die sich speziell um das Thema Sicherheit kümmern, erscheint es selbstverständlich, dass eine Automatisierung der Bedrohungsbekämpfung eine essentielle Rolle in ihrem Sicherheitskonzept spielt.

„Intel Security war das einzige Unternehmen, das uns helfen konnte unsere mittel- bis langfristige Strategie zu optimieren. Dass Intel McAfee übernahm, hat unsere Entscheidung noch gefestigt. Der Umfang der McAfee-Lösungen und die Marktstärke von Intel gab uns die Gewissheit, dass Intel Security seinen Ansprüchen bezüglich ganzheitlichen Sicherheitssystemen gerecht werden wird und sogar Sicherheitsstandards neu definieren kann. Kein anderer Anbieter kann dies leisten."

— Thomas Langer, Leiter Netzwerk- und IT-Sicherheit , Europa
MAUSER Gruppe

Verkürzte Zeitspannen zur Unterbindung von böswilligen Angriffen

„Seit das Intel Security-System mit McAfee Enterprise Security Manager, McAfee Advanced Threat Defense Appliance sowie McAfee Threat Intelligence Exchange aktiv ist, ist die benötigte Dauer, um jegliche Art von Bedrohungen zu finden und zu analysieren, erheblich gesunken", resümiert Langer. „Schnellere Erkennung und Analyse ist dabei gleichbedeutend mit einer schnelleren Reaktion."

Tatsächlich hat es nur zwölf Stunden gedauert, bis das Intel Security-System seinen Wert zum ersten Mal unter Beweis stellen konnte, indem es einen Angriff abwehren musste. „Als wir am Morgen zur Arbeit kamen, zeigte die Protokolldatei, dass unsere Systeme versucht hatten schädliche Software aus dem Internet abzurufen. In unserem Standort in China hatte sich ein externer Mitarbeiter unerlaubt mit dem MAUSER-Netzwerk verbunden. Der Laptop war mit Schadsoftware verseucht, welche gleich mit einem C&C-Server Kontakt aufnehmen wollte. Unsere Firewall hat dies bemerkt und geblockt. Der McAfee Enterprise Security Manager hat den Log-Eintrag der Firewall als gefährlich erkannt und sofort als Alarm ausgegeben, sodass wir zeitnah mit der Analyse beginnen konnten. Bei der Menge an Protokolldateien hätten wir diese Malware ohne das Intel Security-System niemals so schnell entdecken können."

Neben dem McAfee Enterprise Security Manager hat sich auch die McAfee Advanced Threat Defense Appliance als äußerst effektiv erwiesen. So hat McAfee Advanced Threat Defense Appliance eine ausgesprochen fortschrittliche und zielgerichtete Malware erkannt, bevor sie einen verheerenden Schaden anrichten konnte. „Diese Malware war so fortschrittlich, dass die Analyse mehrere Minuten dauerte und der PDF-Report mehr als 35 Seiten Information enthielt", so Langer. „Auch dieser Vorfall hat uns gezeigt, wie leistungsfähig das Intel Security-System ist. Wir wollen uns gar nicht vorstellen, was ansonsten passiert wäre."

Zentrales Management und weniger Vorfälle sparen auch Zeit

Ein weiterer Aspekt der Intel Security-Lösungen ist die Fähigkeit, die Relevanz der einzelnen Vorfälle intelligent einzuschätzen. MAUSER muss nun weniger Störungen im eigenen Netzwerk untersuchen und laut Langer können die einzelnen Störfälle jetzt im Nachhinein erklärt werden, was zuvor nicht immer möglich war. Das ganze Netzwerk läuft darüber hinaus viel reibungsloser, und aufgrund weniger Störungen und Netzwerkprobleme sparen wir Zeit und Energie.

Auch die Möglichkeit, alle wichtigen Informationen auf einem zentralen Dashboard verfolgen zu können, spart dem Sicherheitsteam Zeit und steigert seine Effizienz. Von seinem Desktop kann Langer sowohl auf das SIEM-Dashboard, als auch auf die ePO-Konsole zugreifen, mit deren Hilfe er die Netzwerksicherheit sowie zusammen mit einem weiteren Kollegen die Endgerätesicherheit gewährleistet. Mit Hilfe des maßgefertigten Dashboards, das er selbst einrichten konnte und mehrfach am Tag konsultiert, ist es ihm außerdem möglich, vergangene Vorfälle auf eine Weise zu analysieren, die bisher extrem zeitaufwändig oder überhaupt nicht möglich war. Dazu gehört zum Beispiel die Untersuchung historischer Daten, die Rückschlüsse auf Muster zulassen und somit dabei helfen, das System oder einzelne Prozesse zu optimieren.

Threat Intelligence Exchange und Data Exchange Layer – der neue Standard

Der nächste Schritt für MAUSER ist es nun, weitere Sicherheitslösungen zum bestehenden Sicherheits-Framework hinzuzufügen. Dafür kommen in erster Linie die McAfee Web Gateway Appliance in Frage. „Wir werden auf alle Fälle nach Produkten Ausschau halten, die mit McAfee Threat Intelligence Exchange und McAfee Data Exchange Layer zusammenarbeiten“, sagt Langer. „Nach unserer Auffassung sind sie bereits jetzt der Standard und eine Grundvoraussetzung – neue Produkte zu erwerben, die nicht mit der Intel Security-Plattform im Austausch stehen, würde keinen Sinn ergeben.“

„Der integrierte Sicherheitsansatz ist zu 100 Prozent mit unserer Strategie konform – einer Strategie, von der wir überzeugt sind, dass sie die Sicherheit unseres gesamten Unternehmens so effektiv wie möglich gewährleistet“, schließt Langer.

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

Intel und die Intel- und McAfee-Logos sind Marken der Intel Corporation oder von McAfee, Inc. in den USA und/oder anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. Die in diesem Dokument enthaltenen Produktpläne, Spezifikationen und Beschreibungen dienen lediglich Informationszwecken, können sich jederzeit ohne vorherige Ankündigung ändern und schließen alle ausdrücklichen oder stillschweigenden Garantien aus. Copyright © 2016 McAfee, Inc. 62441cs_mauser_0516