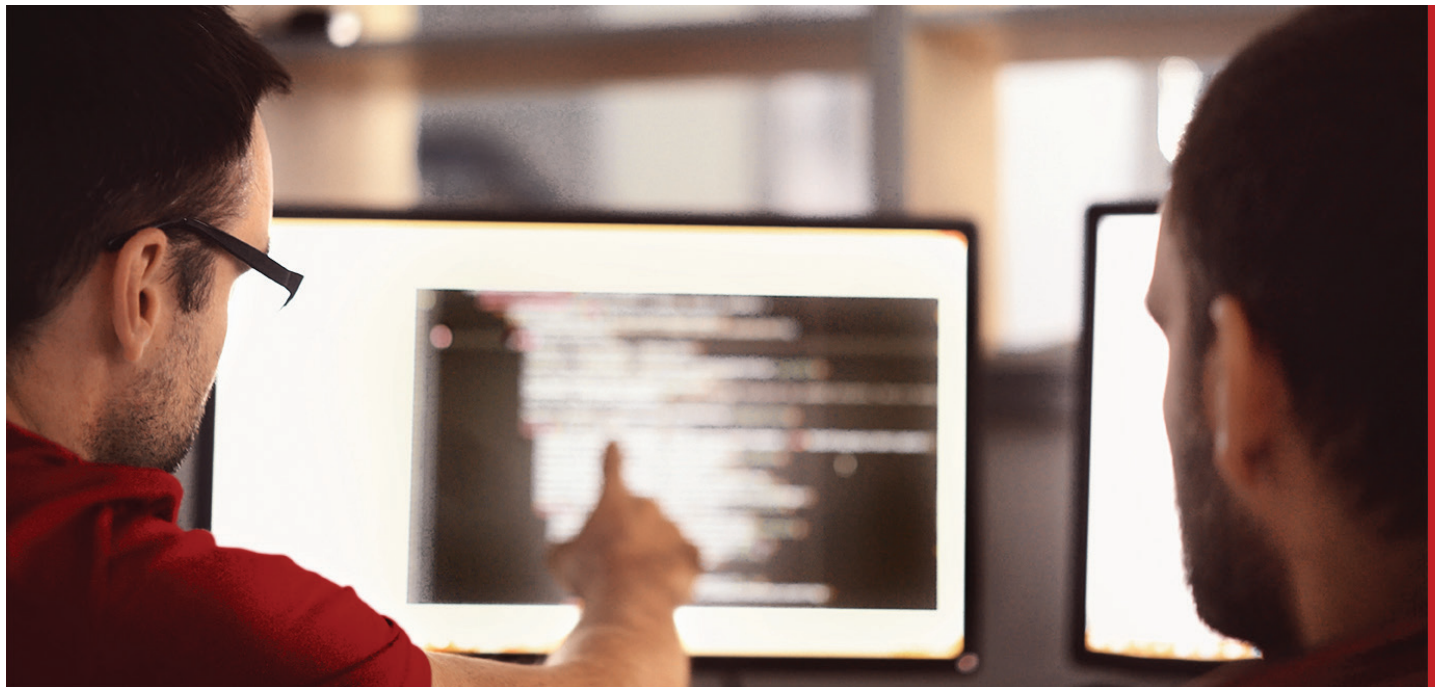
ANWENDERBERICHT

Mehrstufiger Schutz stärkt Sicherheitslage einer Bundesbehörde

Die Bundesagentur für Arbeit vereinfacht die Sicherheitsverwaltung und stärkt den Schutz dank der integrierten Sicherheitsplattform von McAfee



Bundesagentur für Arbeit, Deutschland

Kundenprofil
Bundesbehörde, die für Entgeltersatzleistungen, Arbeitsvermittlung und andere arbeitsmarktbezogene Aufgaben verantwortlich ist

Branche
Behörde

IT-Umgebung
160.000 Endgeräte in ganz Deutschland

Die Bundesagentur für Arbeit ist kompetenter Ansprechpartner für die Arbeits- und Ausbildungsvermittlung. Jeden Tag berät sie Menschen zu Themen rund um den Beruf und unterstützt Millionen Bürgerinnen und Bürger mit finanziellen Leistungen wie Arbeitslosen- und Kindergeld. Durch die Einführung einer integrierten Sicherheitsinfrastruktur, die McAfee Endpoint Security, McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense sowie McAfee SIEM-Lösungen umfasst, konnte die Bundesagentur für Arbeit einen mehrstufigen Schutz einrichten, der die Zeitspanne bis zur Bedrohungseindämmung verkürzt und die allgemeine Sicherheitslage verbessert.

Folgen Sie uns

Schutz für 160.000 Endgeräte vor hochentwickelten Malware-Angriffen

Zu Beginn ihres Arbeitstages wissen die Mitarbeiter des Computer Emergency Response Teams (CERT) der Bundesagentur für Arbeit nicht, was der neue Tag bringen wird. Ihre Aufgabe besteht darin, 160.000 Endgeräte und mehr als 100.000 interne Benutzer innerhalb des Netzwerks sowie die vertraulichen Daten ihrer Mitbürger zu schützen. Dabei sind sie sich der zentralen Bedeutung dieser Aufgabe bewusst und können bestätigen, dass die Cyber-Bedrohungen an Zahl und Raffinesse zunehmen.

„In den vergangenen Jahren verzeichneten wir eine deutliche Steigerung der bei uns eingehenden Bedrohungen wie Ransomware und Distributed-Denial-of-Service-Attacken“, berichtet Peter Neuhauser, Leiter des CERT. „Unsere Behörde verzeichnet pro Tag 300 Millionen Sicherheitszwischenfälle. Die Suche nach schwerwiegenden Zwischenfällen und den besten Möglichkeiten zum Schutz unseres großen Netzwerks ist sehr aufwändig und nervenaufreibend. Wir müssen jederzeit aufmerksam sein, ganz besonders in Bezug auf hochentwickelte Zero-Day-Bedrohungen.“

Schutz vor WannaCry-Ransomware weckt Aufmerksamkeit der Behördenleitung

Die Bundesagentur für Arbeit verwendet seit mehr als 20 Jahren McAfee-Lösungen, angefangen mit McAfee-Virenschutz. Die Lösungen bieten kontinuierlich zuverlässigen Schutz und halten mit der sich ändernden Bedrohungslandschaft sowie der zunehmenden Zahl und Raffinesse Schritt.

„Auch wir wurden von WannaCry angegriffen, doch im Gegensatz zu vielen anderen großen US-amerikanischen und europäischen Organisationen wurden unsere Netzwerke nicht infiziert“, erinnert sich Peter Neuhauser. „Dass unsere Abläufe von dieser Bedrohung nicht betroffen waren, war für unsere Sicherheitsabteilung sehr gut, da diese Tatsache vom Vorstand registriert wurde und die Bedeutung der Cyber-Sicherheit für die Bundesagentur hervorhob.“

Vereinfachte Sicherheitsverwaltung bei weniger Aufwand

Die zentrale Verwaltungskonsole McAfee ePolicy Orchestrator (McAfee ePO) hat sich bei der Verwaltung und dem Schutz der zahlreichen Endgeräte als unverzichtbar erwiesen. Das Team verwendet die McAfee ePO-Software zur Verwaltung verschiedenster Sicherheitsprodukte für die gesamte physische und virtuelle Infrastruktur der Behörde. Diese Produkte reichen von Viren- und Host-Eindringungsschutz bis zu Verschlüsselung und Schwachstellenverwaltung.

„McAfee ePO erleichtert unser Leben, weil wir mehrere Sicherheitsprodukte über eine einzige Plattform und eine Benutzeroberfläche verwalten können“, erklärt Peter Neuhauser. „Durch das anpassbare Dashboard und die Berichte kann mein operatives Team eine enorme Anzahl an Endgeräten schützen. Fast jeder Server-Task läuft automatisiert und geplant ab. Die Aufgabe des Teams beschränkt sich darauf, die Automatisierung zu verbessern und in solchen Fällen manuell einzugreifen, in denen die Automatisierung aus irgendeinem Grund nicht greift.“

Herausforderungen

- Zuverlässiger Schutz vor raffinierten Angriffen, einschließlich Ransomware und hochentwickelter Malware
- Verringerung des Verwaltungsaufwands für den Schutz der Infrastruktur und der 160.000 Endgeräte
- Einhaltung des ISO 27001-Standards und der gesetzlichen Vorschriften für kritische Infrastrukturen

McAfee-Lösungen

- McAfee® Advanced Threat Defense
- McAfee® Endpoint Security
- McAfee® ePolicy Orchestrator® (McAfee ePO™)
- McAfee® Threat Intelligence Exchange
- McAfee SIEM-Lösungen: McAfee® Enterprise Security Manager, McAfee® Log Manager, McAfee® Advanced Correlation, McAfee® Event Receiver, McAfee® Global Threat Intelligence for McAfee Enterprise Security Manager
- McAfee® Network Security Platform

Das CERT-Team der Bundesagentur für Arbeit setzt mehrere McAfee ePO-Berichte regelmäßig ein, zum Beispiel um die Software-Aktualisierungsrate des Virenschutzes nach der Push-Bereitstellung in der gesamten Behörde darzustellen. Mit einem anderen Bericht werden alle verdächtigen oder böswilligen Aktivitäten aufgelistet, damit das Team die Sicherheitslage überwachen sowie genau ermitteln kann, welche Zwischenfälle ihre Aufmerksamkeit benötigen bzw. behoben werden müssen. Typische Zwischenfallzahlen pro Monat:

- 2.000 Viren/Malware-Varianten auf Endgeräten
- 5.000 Erkennungen im Netzwerk
- 30 Millionen verdächtige E-Mails
- 1.000 Spyware-Instanzen

Hochentwickelter Endgeräteschutz steigert Sicherheit und sorgt für zufriedenere Benutzer

Um die neuen Technologien im Bereich Endgeräteschutz nutzen zu können, entschied sich die Bundesagentur für Arbeit für ein Upgrade auf McAfee Endpoint Security. Nach einer gründlichen Test- und Staging-Phase, die über mehrere Monate lief, migrierte das CERT-Team die meisten der 160.000 Endgeräte der Behörde von McAfee® VirusScan® Enterprise auf McAfee Endpoint Security. Dank Unterstützung der McAfee® Professional Services konnte dieser Schritt an einem Wochenende umgesetzt werden.

Nach der Implementierung von McAfee Endpoint Security standen zur Bedrohungserkennung nicht mehr nur signaturbasierte Scans zur Verfügung. Die modernen Machine Learning-Techniken der Lösung erkennen böswilligen Code basierend auf Erscheinungsbild und Verhalten. Herrn Neuhauser war besonders die Einführung des adaptiven Bedrohungsschutzes in der gesamten Behörde wichtig. Dieses Modul umfasst die Real Protect-Technologie, die Cloud-basierte Echtzeitinformationen auswertet. Die Daten stammen von Millionen böswilligen Schadcode-Einsendungen sowie statischen und dynamischen Verhaltens-analysen und werden dazu genutzt, Attribute und Verhaltensweisen unbekannter Dateien automatisch mit Bedrohungsmodellen abzugleichen, um so effektiv Zero-Day-Malware zu erkennen.

Ein weiteres Ergebnis des Wechsels zu McAfee Endpoint Security war nicht nur zuverlässigerer Schutz, sondern auch zufriedenere Kunden, da die Malware-Scans viel schneller und vorrangig im Hintergrund ablaufen, wenn sich die Systeme im Leerlauf befinden. Die deutliche Reduzierung der Prozessorbelastung ist ein wichtiger Pluspunkt für die Benutzer und führte zu einer Steigerung der Produktivität.

Ergebnisse

- Einfachere Verwaltung der Sicherheitsmaßnahmen dank einer zentralen Konsole für unterschiedlichste Lösungen
- Hervorragender Schutz, schnellere Workstations und zufriedenere Benutzer durch hochentwickelten Endgeräteschutz
- Kürzere Reaktionszeiten bei Zwischenfällen durch bidirektionalen Austausch von Bedrohungsdaten
- Umsetzbare Informationen und Überblick über Sicherheitszwischenfälle

Integration von Sicherheits-Tools über DXL beschleunigt Malware-Blockierung und verringert Zeitspanne bis zur Eindämmung

Parallel zu McAfee Endpoint Security implementierte die Bundesagentur für Arbeit die Lösung McAfee Threat Intelligence Exchange, die den Data Exchange Layer (DXL) nutzt. Diese Open-Source-Plattform verbindet Sicherheitskomponenten und ermöglicht den bidirektionalen Austausch lokaler sowie globaler Bedrohungsinformationen zwischen allen Systemen, die innerhalb der Umgebung per DXL vernetzt sind. Das bedeutet: Wird auf einem Endgerät der Behörde eine verdächtige oder böswillige Datei erkannt, dann geht diese Information sofort an McAfee Threat Intelligence Exchange und wird dort mit der integrierten Reputationsdatenbank verglichen. Wenn die Datei als böswillig eingestuft wird, wird sie sofort blockiert – nicht nur auf dem „Patienten Null", sondern auf allen Endgeräten. Alle neu erkannten Bedrohungen – ganz gleich, ob in der lokalen Umgebung oder in externen Quellen – werden zur McAfee Threat Intelligence Exchange-Datenbank hinzugefügt.

Wenn McAfee Threat Intelligence Exchange keine Informationen zu einer unbekannten Datei besitzt, wird diese Datei automatisch zu einer der McAfee Advanced Threat Defense-Appliances weitergeleitet und dort einer gründlichen statischen und dynamischen Analyse (Malware-Sandbox-Analyse) unterzogen. Falls McAfee Advanced Threat Defense die Datei als böswillig einstuft, geht diese Information sofort an alle Systeme in der Umgebung, die über DXL verbunden sind.

„Durch die Vernetzung von McAfee Endpoint Security, McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense erhalten wir unverzichtbaren, mehrstufigen Schutz vor Zero-Day-Angriffen", fasst Peter Neuhauser zusammen. „Dank der Echtzeit-Informationen aus der Cloud in Kombination mit dem bidirektionalen Bedrohungsdatenaustausch über DXL können wir Malware bereits bei ‚Patient Null' stoppen."

Innovatives Postfach für Sicherheitsprüfungen testet verdächtige E-Mails an Benutzer

Das CERT-Team profitierte von einem weiteren Vorteil von McAfee Advanced Threat Defense: Die Appliance kann nicht nur eingehende Dateien per DXL analysieren, sondern bietet zusätzlich die XMODE-Funktion, mit der sich ein „Postfach für Sicherheitsprüfungen" erstellen lässt. Mit diesem Postfach können die Mitarbeiter der Bundesagentur für Arbeit aktiv zur Sicherheit beitragen. „Die XMODE-Funktion von McAfee Advanced Threat Defense ist einzigartig. Ich habe sie in noch keiner anderen Sandbox gesehen", sagt der Verantwortliche für Endgerätesicherheitsprodukte der Behörde. „Mit ihr können wir verdächtige Dateien bei Bedarf unkompliziert in einer sicheren Umgebung manuell analysieren."

Wenn Behördenmitarbeiter eine E-Mail erhalten und sich über die Echtheit nicht sicher sind (z. B. wenn sie nicht in deutscher Sprache verfasst ist oder einen unbekannten Link bzw. einen unerwarteten Anhang enthält), können sie sie an eine spezielle E-Mail-Adresse, das so genannte „Postfach für Sicherheitsprüfungen", weiterleiten. Ein CERT-Analyst erhält die E-Mail und kann verdächtige

Anhänge über die intuitive Benutzeroberfläche der McAfee Advanced Threat Defense-Appliance analysieren lassen. Die Analyse erfolgt in einer sicheren Umgebung, und die Appliance stellt die Ergebnisse anschließend dem CERT-Analyst zur Verfügung.

McAfee SIEM bietet umsetzbare Informationen und vereinfacht die Einhaltung gesetzlicher Bestimmungen

Die Bundesagentur für Arbeit setzt darüber hinaus die McAfee SIEM-Lösung, bestehend aus McAfee Enterprise Security Manager, McAfee Log Manager, McAfee Advanced Correlation Engine und anderen verwandten Produkten, ein – sie erfüllt weitgehendst die Anforderungen der Behörde und integriert sich nahtlos in die McAfee ePO-Software sowie Network Security Platform.

„Durch die McAfee SIEM-Lösung erhalten wir einen Überblick über jeden der 300 Millionen Sicherheitszwischenfälle, die wir jeden Tag erfassen“, sagt Peter Neuhauser. „Wir können umsetzbare, nützliche Berichte zentral abrufen. Die Dashboards und Berichte machen unsere Sicherheitsmaßnahmen sichtbar, und sie helfen uns dabei, die Compliance-Anforderungen einzuhalten.“

Eine strategische Sicherheitspartnerschaft

Herr Neuhauser sieht in McAfee einen wichtigen Partner im IT-Sicherheitsumfeld. Die Bundesagentur für Arbeit verwendet zahlreiche McAfee-Produkte und nutzt bei Bedarf McAfee Professional Services, zum Beispiel zur Migration zu McAfee Endpoint Security und zur Unterstützung bei der Erstellung von Zwischenfall-reaktionsplänen. „Kriminelle arbeiten äußerst professionell zusammen. Ich denke, dass das McAfee-Motto "Together is Power – Gemeinsam sind wir stark" der richtige Ansatz für unsere Seite ist“, schlussfolgert Peter Neuhauser.

> „Durch die Vernetzung von McAfee Endpoint Security, McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense erhalten wir unverzichtbaren, mehrstufigen Schutz vor Zero-Day-Angriffen. Dank der Echtzeit-Informationen aus der Cloud in Kombination mit dem bidirektionalen Bedrohungsdaten-austausch über DXL können wir Malware bereits bei ‚Patient Null‘ stoppen.“
>
> – Peter Neuhauser, Leiter des CERT, Bundesagentur für Arbeit, Deutschland

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
www.mcafee.com/de