McAfee Threat Intelligence Exchange

Gemeinsam genutzte Bedrohungsdaten für mehrere Sicherheitslösungen

McAfee® Threat Intelligence Exchange agiert als Reputations-Broker, um adaptive Bedrohungserkennung und Reaktionen zu ermöglichen. Dabei kombiniert die Lösung lokale Daten aus den Sicherheitslösungen Ihres Unternehmens mit externen globalen Bedrohungsdaten und gibt diese Erkenntnisse sofort an die kollektive Intelligenz weiter, damit Ihre Lösungen Informationen austauschen und basierend darauf agieren können.

Aufbau eines gemeinschaftlich agierenden Ökosystems für Bedrohungsdaten

Der Reputations-Broker McAfee Threat Intelligence Exchange kombiniert Bedrohungsdaten aus importierten globalen Quellen, wie McAfee Global Threat Intelligence (McAfee GTI) und Drittanbieter-Bedrohungsdaten (z. B. VirusTotal), mit lokalen Quellen, einschließlich Endgeräte, Gateways und hochentwickelte Analyselösungen. Über den Data Exchange Layer (DXL) werden diese kollektiven Informationen sofort über Ihr Sicherheits-Ökosystem geteilt, damit die Sicherheitslösungen als Einheit agieren und so den Schutz im gesamten Unternehmen verbessern können.

Aufgrund der einfachen Integration über den DXL werden die Implementierungs- und Betriebskosten der zahlreichen direkten API-Integrationen (Application Programming Interface) gesenkt und einzigartige Sicherheit, operative Effizienz sowie Effektivität erreicht.

Der DXL wurde als offenes Framework konzipiert, sodass alle Sicherheitslösungen – auch Sicherheitsprodukte von Drittanbietern – dynamisch in das McAfee Threat Intelligence Exchange-Ökosystem eingebunden werden können.

Anpassung und Immunisierung gegen Bedrohungen

Jede geteilte Information, die im gesamten Netzwerk erkannt wird, stärkt die Position des Unternehmens im Kampf gegen gezielte Bedrohungen. Da es sich bei diesen Bedrohungen um präzise gesteuerte Attacken handelt, benötigen Unternehmen ein lokales Überwachungssystem, das die Bedrohungstrends sowie alle einmaligen Angriffe erfasst. Dank der Kombination dieser aus Zwischenfällen erfassten lokalen Kontextdaten mit globalen Bedrohungsdaten können bei völlig unbekannten Dateien bessere Entscheidungen getroffen sowie Schutz und Erkennung erheblich beschleunigt werden.

Hauptvorteile

- Adaptiver Bedrohungsschutz verringert die Schutzlücke zwischen Entdeckung und Eindämmung hochentwickelter gezielter Angriffe von Tagen, Wochen oder Monaten auf wenige Millisekunden.
- Stellt kollektive Bedrohungsdaten bereit, die aus weltweiten Quellen gewonnen und mit lokalen Bedrohungsdaten kombiniert wurden.
- Der Austausch relevanter Sicherheitsinformationen erfolgt in Echtzeit zwischen Sicherheitslösungen für Endgeräte, Gateways, Netzwerke sowie Rechenzentren.
- Bietet Unterstützung mit Endgerätekontext (Datei, Prozess und Umgebungsattributen) sowie kollektiven Bedrohungsdaten für Entscheidungen bei völlig unbekannten Dateien.

Wenn an einem beliebigen Punkt in Ihrem Netzwerk eine unbekannte Datei gefunden wird, erfolgt eine Abfrage bei McAfee Threat Intelligence Exchange, ob bereits Reputationsdaten zu dieser Datei vorliegen. Außerdem werden beschreibende Metadaten (z. B. Verbreitung im Unternehmen und Alter) gepflegt, die die kollektiven Erkenntnisse ergänzen. Die verbundenen Sicherheitslösungen können nicht nur Reputationsdaten abrufen, sondern auch selbst basierend auf lokalen Erkenntnissen Aktualisierungen an McAfee Threat Intelligence Exchange senden. Diese Aktualisierungen werden daraufhin in Echtzeit an Ihre Systeme verteilt. Anschließend werden die lokal erfassten Bedrohungsinformationen für künftige Zwischenfälle gespeichert. Sollte diese Datei also noch einmal auf einem anderen Gerät oder Server auftauchen, gilt sie nicht mehr als unbekannt, sondern wird sofort entdeckt.

Mit McAfee Threat Intelligence Exchange können Administratoren Bedrohungsdaten problemlos anpassen, und Sicherheitsadministratoren erhalten die Möglichkeit, die umfangreichen Informationen zu sammeln, zu überschreiben, zu erweitern und zu verbessern, damit Ihre Umgebung und Ihr Unternehmen optimal geschützt werden. Dank dieser lokal priorisierten und angepassten Bedrohungsinformationen kann auf künftige Zwischenfälle sofort reagiert werden.

Durchsetzungspunkte verbessern den Schutz

Die im gesamten Netzwerk verbundenen Lösungen – von Endgeräten bis zur Netzwerkperipherie – wenden die Richtlinien basierend auf verfügbaren Reputationsdaten, Metadaten oder einer Kombination von Datenpunkten an.

Die stark vernetzte Lösung McAfee Endpoint Security nutzt die kombinierten lokalen Daten (einschließlich Datei-Metadaten wie Verbreitung im Unternehmen und Alter sowie lokale Reputationsdaten aus anderen Sicherheitskomponenten) zusätzlich zu aktuell verfügbaren globalen Bedrohungsdaten, um zuverlässige Entscheidungen zu ermöglichen. Wenn zum Beispiel eine benutzerdefinierte Anwendung ohne globale Reputation im Unternehmen stark verbreitet ist, wird diese nicht als böswillig eingestuft und darf wahrscheinlich ausgeführt werden. Wenn jedoch eine verdächtig gepackte Datei noch nicht im Unternehmen gesehen wurde und keine globalen oder lokalen Reputationswerte vorliegen, wird sie wahrscheinlich als wenig vertrauenswürdig eingestuft. Das würde bedeuten, dass sie anfangs blockiert oder zusätzlich von den McAfee Endpoint Security-Zusatzmodulen sowie McAfee Advanced Threat Defense- bzw. McAfee Cloud Threat Detection-Sandboxes untersucht wird.

Real Protect, die Machine Learning-Funktion von McAfee Endpoint Security, sowie die Funktion zur dynamischen Eindämmung von Anwendungsprozessen verbessern die Möglichkeiten zur Erkennung und Absicherung von Endgeräten noch weiter. Real Protect führt basierend auf aktuellsten Bedrohungsdaten Cloud-Suchen sowie Analysen vor und nach der Ausführung durch, während die dynamische Eindämmung von Anwendungsprozessen böswillige Aktivitäten auf Endgeräten verhindert und so gewährleistet, dass „Patient Null“ noch während der Ausführung zusätzlicher Analysen vor neuen Bedrohungen geschützt ist.

Hauptvorteile (Fortsetzung)

- Die Integration wird durch den DXL vereinfacht. Durch die Vernetzung von Sicherheitslösungen von McAfee und Drittanbietern zur Verarbeitung von Bedrohungsdaten in Echtzeit sinken die Implementierungs- und Betriebskosten.

Hochentwickelte gezielte Bedrohungen – eine echte Herausforderung

Da hochentwickelte gezielte Angriffe darauf abzielen, die Erkennung zu vermeiden und sich langfristig in Unternehmen festzusetzen, werden sie Unternehmen noch lange beschäftigen und hochwertige Daten exfiltrieren. Laut den Daten im *„Verizon 2015 Data Breach and Investigations Report“* (Verizon-Bericht zu Datenkompromittierungen und Untersuchungen für 2015) wurden 70 bis 90 Prozent aller Malware-Varianten speziell für ein Unternehmen konzipiert, was die Erkennung individueller Bedrohungsindikatoren zur derzeit größten Herausforderung macht.[1]

Weitere Informationen finden Sie unter **www.mcafee.com/de/products/threat-intelligence-exchange.aspx**.

Vorteile durch Zusammenarbeit

Hochentwickelte Bedrohungsanalysen

Wenn weitere Informationen über eine Datei benötigt werden, kann diese automatisch von McAfee Threat Intelligence Exchange an McAfee-Lösungen für erweiterte Analysen (z. B. McAfee Advanced Threat Defense und McAfee Cloud Threat Detection) gesendet werden, um sofort zusätzliche Informationen über potenzielle neue Bedrohungen zu erhalten und die Reputation der jeweiligen Datei zu bestimmen. Diese Vorgänge laufen automatisiert ab, werden vollständig dokumentiert und über den DXL weitergegeben, um Ihr gesamtes Sicherheitsökosystem zu schützen.

Verwaltung von Sicherheitsvorfällen

McAfee Enterprise Security Manager ermöglicht die tiefgehendere Untersuchung der Kompromittierungsindikatoren, die von McAfee Threat Intelligence Exchange entdeckt wurden. Die Sicherheitseffizienz des Unternehmens wird durch den Zugang zu Sicherheitsverlaufsdaten sowie die Möglichkeit zur Erstellung automatisierter Whitelists verbessert.

1. http://www.verizonenterprise.com/DBIR/2015/

McAfee
Together is power.

Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 3707 0
www.mcafee.com/de