McAfee Threat Intelligence Exchange

Gemeinsame Bedrohungsdaten zum Schutz vor gezielten Angriffen

McAfee® Threat Intelligence Exchange ermöglicht dank übergreifender Datennutzung in Sicherheitslösungen für Endgeräte, Gateways, Netzwerke sowie Rechenzentren adaptive Bedrohungserkennung und -abwehr in Echtzeit. Durch die Kombination und sofortige Freigabe globaler Bedrohungsinformationen sowie lokal erfasster Daten können Ihre Sicherheitslösungen als Einheit fungieren, die nicht nur Informationen austauscht, sondern auch auf Basis gemeinsamer Informationen agiert. McAfee Threat Intelligence Exchange verringert die Schutzlücke zwischen Entdeckung und Eindämmung von Tagen, Wochen oder Monaten auf wenige Millisekunden.

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.
- Zeigt sofort eine Übersicht aller hochentwickelten gezielten Angriffe in Ihrem Unternehmen an.
- Der Austausch relevanter Sicherheitsinformationen erfolgt in Echtzeit zwischen Sicherheitslösungen für Endgeräte, Gateways, Netzwerke sowie Rechenzentren.

Aufbau eines gemeinschaftlich agierenden Ökosystems für Bedrohungsdaten

McAfee Threat Intelligence Exchange nutzt für den Informationsaustausch und die daraus resultierende integrierte Sicherheit den McAfee Data Exchange Layer. Die aus zahlreichen Quellen gesammelten Bedrohungsinformationen werden zusammengefasst und unverzüglich an alle verbundenen Sicherheitslösungen – einschließlich Lösungen von Drittanbietern – weitergegeben.

Da die Sicherheitskomponenten als Einheit agieren, werden alle für die Bedrohungserkennung und -abwehr relevanten Informationen sofort zwischen Endgeräten, Gateways, Rechenzentren, Cloud sowie anderen Sicherheitskontrollpunkten in Ihrer Umgebung ausgetauscht. Dank der einfachen Integration durch den McAfee Data Exchange Layer werden die Implementierungs- und Betriebskosten erheblich gesenkt, sodass unerreichte Sicherheit, betriebliche Effizienz sowie Effektivität ermöglicht werden.

McAfee Data Exchange Layer wurde als offenes Framework konzipiert, sodass alle Sicherheitslösungen – auch Sicherheitsprodukte von Drittanbietern – dynamisch in das McAfee Threat Intelligence Exchange-Ökosystem eingebunden werden können. Dadurch reduzieren sich nicht nur Ihre Gesamtbetriebskosten, sondern Sie können dank Sicherheitskomponenten, die jetzt vollständig miteinander kommunizieren, den Wert Ihrer Investitionen in vorhandene Sicherheitsprodukte und -lösungen besser nutzen.

Die gemeinsame und anpassbare Bedrohungsabwehr stellt einen völlig neuen Ansatz bei der IT-Sicherheit von Unternehmen dar, bei dem getrennte Systeme für echte Sicherheitsverzahnung zusammengeführt werden. Sicherheitsteams, die organisatorische und Budget-bedingte Hindernisse überwinden sollen, müssen den Austausch von Sicherheitsbedrohungsdaten automatisieren und Schutzrichtlinien sowie -maßnahmen präventiv überall im Netzwerk anwenden können.

intel Security

Hauptvorteile (Fortsetzung)

- Bietet Unterstützung mit Endgerätekontext (Datei, Prozess und Umgebungsattributen) sowie kollektiven Bedrohungsdaten die Entscheidungen bei völlig unbekannten Dateien.
- Die Integration wird durch den McAfee Data Exchange Layer vereinfacht. Durch die Vernetzung von Sicherheitslösungen von Intel Security und Drittanbietern zur Verarbeitung von Bedrohungsdaten in Echtzeit sinken die Implementierungs- und Betriebskosten.

Durch die Umwandlung der Sicherheitsinfrastruktur in ein Kooperationssystem können Sicherheitsadministratoren Bedrohungen erkennen, melden und ihre Umgebungen immunisieren. McAfee Threat Intelligence Exchange verbessert die Ausfallsicherheit erheblich und bietet mehr Kontrollmöglichkeiten im Kampf gegen neu aufkommende und gezielte Bedrohungen.

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 Lenkwaffen handelt, benötigen Unternehmen ein lokales Überwachungssystem, das die Bedrohungstrends sowie alle einmaligen Angriffe erfasst. Dank der Kombination dieser lokal aus Zwischenfällen erfassten Kontextdaten mit globalen Bedrohungsdaten können bessere Entscheidungen bei völlig unbekannten Dateien getroffen sowie Schutz und Erkennung erheblich beschleunigt werden.

Wenn eine nicht identifizierte Datei in Ihrem Netzwerk auftaucht, wird sie lokal durch McAfee Threat Intelligence Exchange bewertet. Sollte sich während dieser Bewertung herausstellen, dass die Datei böswillig ist, werden alle Ihre Systeme in Echtzeit geschützt. 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.

Zum Beispiel werden Informationen zu einer böswilligen Datei, die an Ihrem Gateway erkannt wurde, über den McAfee Data Exchange Layer an McAfee Threat Intelligence Exchange gesendet und erreichen innerhalb von Millisekunden Ihre Endgeräte und Rechenzentren. Diese haben dann die notwendigen Informationen, um sich proaktiv vor dieser Bedrohung zu schützen. Ein blockierter Kompromittierungsversuch auf einem Endgerät, bei dem Malware entdeckt wird, kann sofort weitergemeldet werden und erreicht darüber das Gateway sowie weitere Sicherheitskomponenten, die anschließend alle Grenzen auf diese Bedrohung überwachen.

Nutzung von Bedrohungsdaten in Echtzeit

Sie haben jetzt die Möglichkeit, Bedrohungsdaten aus importierten weltweiten Quellen wie McAfee Global Threat Intelligence (McAfee GTI) sowie Bedrohungsinformationen von Drittanbietern und gemeinsame Kompromittierungsindikatoren wie STIX-Dateien (Structured Threat Information eXpression) zu kombinieren. McAfee Global Threat Intelligence erfasst lokale Daten aus Echtzeit- und Verlaufsereignissen von Endgeräten, Rechenzentren, Gateways, Ihrem Netzwerk und der Sandbox-Lösung McAfee Advanced Threat Defense. Diese kombinierten globalen und lokalen Bedrohungsdaten können dann in Ihrem gesamten Sicherheitsökosystem in Echtzeit genutzt und ausgetauscht werden.

Dank McAfee Threat Intelligence Exchange erhalten Administratoren die Möglichkeit, umfassende Bedrohungsdaten aus globalen Datenquellen wie McAfee GTI, Daten von Drittanbietern und importierten STIX-Dateien abzurufen. Diese Daten werden mit lokalen Bedrohungsdaten aus Echtzeit- und Verlaufsereignissen kombiniert, die von Endgeräten, Gateways, Sandbox-Lösungen und anderen Sicherheitskomponenten weitergegeben wurden. Sicherheitsadministratoren können die umfassenden Informationen zusammenstellen, außer Kraft setzen, erweitern und sie an die eigene Umgebung sowie das Unternehmen anpassen (z. B. Black- und Whitelists für Dateien sowie Zertifikate, die vom Unternehmen genutzt werden).

Hochentwickelte gezielte Bedrohungen – eine echte Herausforderung

Hochentwickelte gezielte Bedrohungen wurden entwickelt, um die Erkennung zu erschweren und einen dauerhaften Brückenkopf im Unternehmen zu bilden, über den wertvolle Daten exfiltriert werden. Daher ist diese Bedrohung unvermindert aktuell. Laut den Daten im „*Verizon 2015 Data Breach and Investigations Report*“ *(Verizon-Bericht zu Daten-kompromittierungen 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 **http://www.mcafee.com/de/products/threat-intelligence-exchange.aspx**.

Dank dieser lokal priorisierten und angepassten Bedrohungsinformationen kann auf künftige Zwischenfälle sofort reagiert werden. Die kollektiv erfassten Bedrohungsdaten enthalten beschreibende Metadaten zu wichtigen Objekten. Administratoren sowie SIEM-Produkte (Sicherheitsinformations- und Ereignis-Management) können anhand der erfassten Informationen sofort gemeinsam Systeme identifizieren, die aufgrund früherer böswilliger Aktivitäten sehr wahrscheinlich kompromittiert sind.

Hochmoderner Endgeräteschutz

Durch den Einsatz des VirusScan® Enterprise-Moduls bietet McAfee Threat Intelligence Exchange innovativen Endgeräteschutz. Dank konfigurierbarer Regeln trifft das Modul korrekte Entscheidungen zur Dateiausführung. Dabei nutzt es die kombinierten Daten aus lokalen Endgerätekontexten (Datei-, Prozess- und Umgebungsattribute) sowie die aktuell verfügbaren gesammelten Bedrohungsdaten (z. B. Verbreitung im Unternehmen, Alter und Reputation).

Wenn Sie als Administrator das VirusScan Enterprise-Modul von McAfee Threat Intelligence Exchange an die Risikotoleranz Ihres Unternehmens bei Endgeräten anpassen, können Sie die Ausführungsbedingungen entsprechend den jeweiligen spezifischen Anforderungen flexibel festlegen. Diese können so rigide ausgelegt sein, dass eine Nulltoleranz-Richtlinie für unbekannte sowie „graue“ Dateien durchgesetzt wird oder basierend auf entsprechenden Regeln nur dann Zugriff auf Dateien gewährt wird, wenn diese bekannt sind und eine akzeptable Reputation aufweisen.

Endgeräteverwaltung – jederzeit und überall

McAfee Threat Intelligence Exchange bietet adaptiven Bedrohungsschutz und Sicherheits-verwaltung mit weltweiter Reichweite – das heißt die Lösung greift auf Endgeräte unabhängig von ihrem Standort zu und stellt die Mittel bereit, um Bedrohungsrichtlinien und Erkennungen sowie Sicherheitsaktualisierungen und Remote-Untersuchungen zu verwalten. Die Sicherheits-komponenten agieren unabhängig von physischen Grenzen als Einheit. Sie geben sofort relevante Sicherheitsdaten an Endgeräte, Gateways und andere Sicherheitsprodukte weiter, wobei der Standort keine Rolle spielt, und ermöglichen adaptiven Bedrohungsschutz.

Andere Sicherheitsverwaltungs-Lösungen sind nicht imstande, Richtlinienänderungen, Inhalte und Programmaktualisierungen sofort an die Endgeräte auszubringen. Das öffnet ein Bedrohungsfenster, in dem Unternehmen einem höheren Risiko ausgesetzt sind. Durch den Einsatz des McAfee Data Exchange Layer kann McAfee Threat Intelligence Exchange auch bei Netzwerkhindernissen eine dauerhafte Verbindung aufrechterhalten. Die Lösung schließt diese Risikolücke effektiv und gewährleistet, dass kein Endgerät ungeschützt bleibt.

Vorteile durch Zusammenarbeit

Reputationsabfrage mit einem Klick

Nach der Erkennung einer unbekannten Datei durch eine der Sicherheitskomponenten in Ihrem Unternehmen (Gateway, Endgerät oder Netzwerk) kann die Reputation basierend auf Attributen und den in Ihrem Unternehmen zusammengestellten Bedrohungsdaten auf einfache Weise ermittelt werden.

Hochentwickelte Bedrohungsanalysen
Wenn weitere Informationen über eine Datei benötigt werden, kann sie automatisch von McAfee Threat Intelligence Exchange an McAfee Advanced Threat Defense gesendet werden, um sofort zusätzliche Informationen über potenzielle neue Bedrohungen zu erhalten. Sie greifen gemeinsam auf Bedrohungsdaten aus statischen und dynamischen Code-Analysen zu, um die Reputation der fraglichen Datei zu ermitteln. Diese Vorgänge laufen automatisiert ab, werden vollständig dokumentiert und über den McAfee Data Exchange Layer 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.

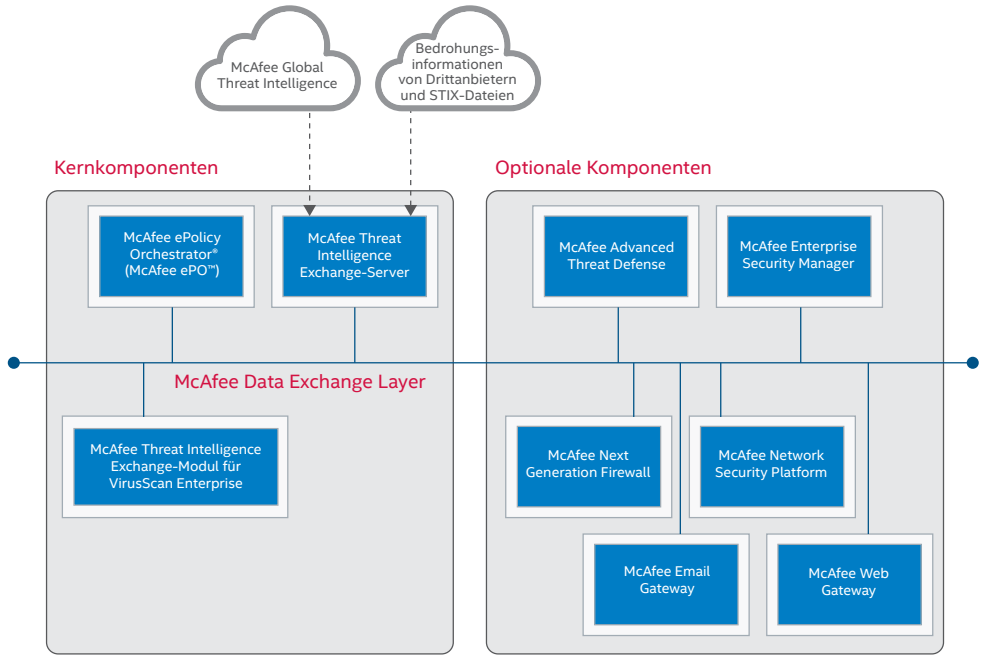

Abbildung 1. Die einfache Vernetzung über den McAfee Data Exchange Layer senkt Implementierungs- sowie Betriebskosten und ermöglicht unerreichte Effizienz von Abläufen – ein neuer Entwicklungsschritt für die McAfee Security Connected-Plattform.

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

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

62120ds_threat-intelligence-exchange_0915