Kurzvorstellung

Sicherheit durch Einheit

Anpassbare Sicherheitsdaten ermöglichen die sofortige Reaktion auf neue Bedrohungen.

Unternehmen sind gezwungen, effektive Schutzmaßnahmen gegen aktuelle und neue Bedrohungen zu implementieren. Dabei stehen sie vor zahlreichen Schwierigkeiten bei Sicherheit und Geschäftsabläufen. Zero-Day- sowie hochentwickelte gezielte Bedrohungen setzen Schaddaten ein, die noch nie zuvor beobachtet wurden. Polymorphe Malware-Bedrohungen stellen die Unternehmen vor ähnliche Probleme. Vorhandene herkömmliche und signaturbasierte Gegenmaßnahmen haben Schwierigkeiten, die Schaddaten hochentwickelter Malware zu erkennen.

Zur effektiven Abwehr neuer Bedrohungen benötigen Unternehmen ein Sicherheitssystem, das eine Kombination aus Verhaltens-, Reputations- sowie signaturbasierten Analysen für Netzwerk und Endgeräte bietet. Doch selbst wenn die einzelnen Technologieebenen jeweils gute Leistungen bei der Bedrohungserkennung bieten, ist es wichtig, dass sie eng verzahnt arbeiten, um Daten auszutauschen, Informationen zu erlangen und sich gemeinsam an neue Bedrohungen anzupassen. Die zeitaufwändige manuelle Kommunikation zwischen Netzwerk- und Endgerätelösungen ist nicht schnell genug, um heutige Gefahren abzuwehren.

McAfee® Threat Intelligence Exchange und McAfee Advanced Threat Defense arbeiten verzahnt, um gemeinsam automatisierten und adaptiven Schutz vor neuen Bedrohungen bereitzustellen. Unabhängig davon, wo der Erstkontakt durch eine unbekannte Malware-Datei stattfand, wird die gesamte verbundene Umgebung unmittelbar nach der Erkennung aktualisiert. Wenn eine Datei von McAfee Advanced Threat Defense überführt wurde, veröffentlicht McAfee Threat Intelligence Exchange diese Bedrohungsinformationen in einem Reputations-Update über den Data Exchange Layer an alle Gegenmaßnahmen im Unternehmen. Endgeräte mit McAfee Threat Intelligence Exchange besitzen also präventiven Schutz, wenn die Datei später erneut gefunden wird. Gateways mit McAfee Threat Intelligence Exchange verhindern, dass die Datei ins Unternehmen gelangt. Und wenn Endgeräte mit McAfee Threat Intelligence Exchange Dateien mit unbekannter Reputation erkennen, werden diese an McAfee Advanced Threat Defense weitergeleitet. Die Lösung überprüft dann, ob das Objekt böswillig ist, und schließt dadurch Erkennungslücken durch die Out-of-Band-Übertragung von Schaddaten.

Wichtige Vorteile

- Erhebliche Verkürzung der Zeitspanne bis zur Eindämmung durch automatisierte und adaptive Bedrohungsreaktion
- Bessere Übersicht, Flexibilität und Kontrolle durch Vernetzung des Netzwerk- und Endgeräteschutzes
- Intelligente Reaktion auf Zwischenfälle dank zuverlässiger Datei-Reputation und Informationen zur Ausführung
- Verbesserte Sicherheit bei optimierten Gesamtbetriebskosten durch vereinfachte Integration und Implementierung

intel Security

Schließen der Sicherheitslücke

Erkennung verborgener Malware-Schaddaten

McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense agieren gemeinsam, um verdächtige Objekte unabhängig vom Erstkontakt zu analysieren. Sobald der Versuch gestartet wird, neue Dateien auszuführen, werden sie in dieser kooperativen Lösung den gemeinsamen Endgeräte-regeln, Umgebungs- und weltweiten Reputationsinformationen sowie tiefgehenden statischen und dynamischen Analysen der verbundenen Komponenten unterzogen. Dieser vernetzte Ansatz zur Bedrohungsanalyse ermöglicht eine genauere Erkennung verborgener Malware, die andernfalls unentdeckt bleibt.

Verbesserung der Bedrohungserkennung durch verhaltensbasierte Bedrohungsanalyse

McAfee Advanced Threat Defense ermöglicht die Reputationsklassifizierung durch innovative Möglichkeiten zur Malware-Dekonstruktion, zu denen unter anderem leistungsstarke Entpack-funktionen gehören. Diese können Verschleierungstechniken aushebeln und den ursprünglichen ausführbaren Code offenlegen, was die Erkennung des beabsichtigten Verhaltens ermöglicht. Gemeinsam ermöglichen dynamische und statische Code-Analysen eine vollständige Bewertung und bieten die derzeit leistungsfähigste Technologie zur Erkennung hochentwickelter Bedrohungen auf dem Markt.

Übersicht und Kontrolle vom Endgerät bis zum Netzwerk

McAfee Advanced Threat Defense erfasst Malware-Exemplare, die von anderen Produkten in Ihrer Umgebung an Netzwerkeintrittspunkten gesammelt wurden. Diese Netzwerkkomponenten können wiederum die neuen Erkenntnisse aus diesen Exemplaren über McAfee Threat Intelligence Exchange teilen. Dieser Daten- und Reputationsaustausch verdeutlicht die Vorteile des Informationsaustauschs zwischen Endgeräten und Netzwerkkomponenten im Rahmen der McAfee Security Connected-Plattform. Zudem verwaltet McAfee Threat Intelligence Exchange eine KnowledgeBase mit Informationen dazu, wo die letzten Objekte in der Endgeräteumgebung ausgeführt wurden, um so eine umfassende Übersicht aller Zwischenfälle bereitzustellen.

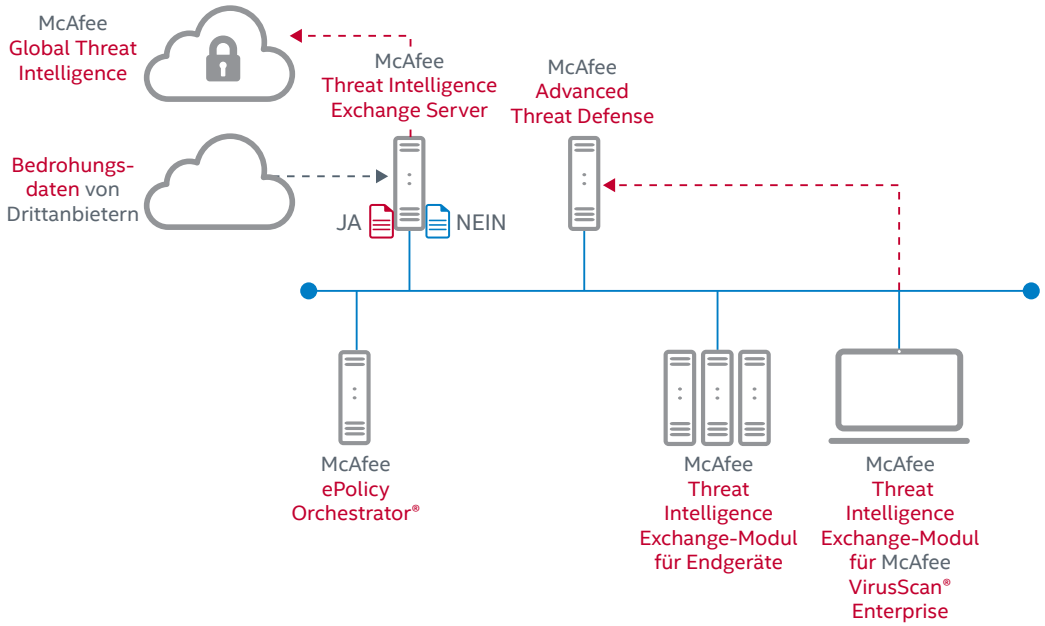

Abbildung 1. Daten- und Reputations-Synthese aus der Cloud, dem Netzwerk sowie von Endgeräten

Einbindung von Security Connected durch den McAfee Data Exchange Layer

McAfee Threat Intelligence Exchange ist die erste Lösung, die den McAfee Data Exchange Layer nutzt. Diese extrem schnelle und ressourcenschonende bidirektionale Kommunikationsstruktur erlaubt die Integration von Produkten sowie den Austausch von Kontext-informationen. Auf diese Weise kann sie Sicherheits-informationen und adaptiven Schutz bereitstellen. Produkte, die den McAfee Data Exchange Layer nutzen, melden sich einfach an der Struktur an und können ihrerseits Daten veröffentlichen. Dabei ist keine komplexe API-basierte Integration oder aufwändige Konfiguration notwendig. Das ist der Beginn einer neuen Sicherheitsära, in der alle Komponenten gemeinsam als zusammenhängendes System arbeiten.

Adaptive Reaktionen

Sobald McAfee Advanced Threat Defense eine Datei analysiert und klassifiziert hat, werden die Ergebnisse an McAfee Threat Intelligence Exchange gesendet. Die neue Datei-Reputation (ganz gleich, ob sie gut oder schlecht ist) wird sofort für alle Gegenmaßnahmen mit McAfee Threat Intelligence Exchange in der gesamten Umgebung veröffentlicht. Von da an wird jedes weitere Exemplar der Datei erkannt, sodass sie von allen Komponenten mit McAfee Threat Intelligence Exchange entsprechend ihren Richtlinien zugelassen, blockiert oder bereinigt wird. Diese adaptiven Reaktionen bieten sofortigen Schutz für die gesamte Umgebung, einschließlich Netzwerk, Gateway und Endgerätekomponenten. Die Reaktionsgeschwindigkeit wird beschleunigt und die Zeitspanne bis zur Eindämmung sowie Behebung erheblich verkürzt – und das alles ohne Netzwerkumbau.

Einfache Bereitstellung und Verwaltung

Die Verzahnung zwischen McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense erfolgt nahtlos über den Data Exchange Layer. Dieser wurde als offenes Framework konzipiert und erlaubt Sicherheitskomponenten die dynamische Einbindung in McAfee Threat Intelligence Exchange, ohne dass umfangreiche APIs oder komplexe Produktkonfigurationen erforderlich sind. Dies ermöglicht die Senkung der Fehlerhäufigkeit und vermeidet umfangreichen manuellen Aufwand.

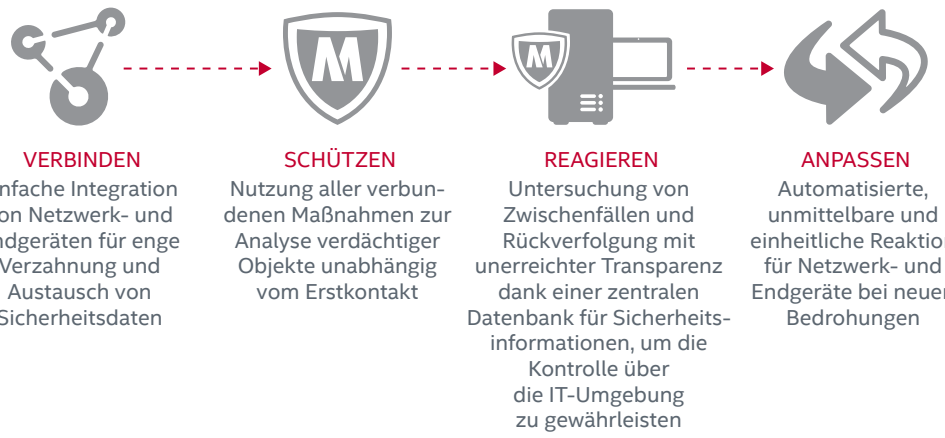

Abbildung 2. Dank Security Connected-Ansatz nahtlose Integration über den Data Exchange Layer

Weitere Informationen

McAfee Threat Intelligence Exchange und McAfee Advanced Threat Defense sind unverzichtbare Lösungen, die separate Sicherheitskomponenten verbinden, Ihre Umgebung schützen, auf Zwischenfälle reagieren und sich automatisch an neue Bedrohungen anpassen. Mit einem Sicherheits-Ökosystem, das modernste Bedrohungsanalyse, Netzwerkprodukte und Endgerätelösungen miteinander vernetzt, ermöglicht McAfee unternehmensweite Transparenz und Kontext für Bedrohungen bei gleichzeitiger Verkürzung der Reaktionszeit und Vereinfachung der Problembehebung.

- **www.mcafee.com/de/products/threat-intelligence-exchange.aspx**
- **www.mcafee.com/de/products/advanced-threat-defense.aspx**
- **www.mcafee.com/de/enterprise/security-connected/index.aspx**

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