McAfee Active Response

Umfassende Erkennungs- und Reaktionsmöglichkeiten für Endgeräte

Sicherheitsbewusste Unternehmen und Organisationen sehen sich heute mit Bedrohungen konfrontiert, die sich mit großem Tempo verändern. Angriffe werden immer schneller gestartet und verbreiten sich rasant. „Designer"-Angriffe nehmen einzelne Organisationen oder Unternehmen ins Visier und sind dank Spezialkenntnissen sehr effektiv, dabei aber nur schwer zu erkennen. Zudem überwinden die Angreifer häufig auch vorhandene Schutztechnologien. Vorausschauende Unternehmen fordern daher einfach bedienbare integrierte Tools, die Angreifer schneller erkennen sowie schnelle Untersuchungs- und Behebungsmöglichkeiten bieten. Die besten Erkennungs- und Reaktionslösungen verbessern die Effizienz bestehender Sicherheitsmaßnahmen auch dadurch, dass sie immer umfassendere Informationen von einer immer größeren Zahl von Systemen erfassen. Dank hervorragender standardmäßig enthaltener Funktionen, automatischer Interaktion mit vorhandenen Sicherheitsverwaltungslösungen sowie Anpassungsmöglichkeiten verringert McAfee® Active Response die Chance für Angreifer, Ihre IT-Ressourcen und Ihre Marke zu schädigen.

Hauptvorteile

- **Automatisiert:** Erfasst und überwacht den Kontext sowie den Systemstatus auf Änderungen, die auf Angriffsindikatoren hinweisen, findet „ruhende" Angriffskomponenten und sendet Erkenntnisse an Analyse-, Operations- und Forensik-Teams.
- **Anpassbar:** Sie können anpassen, wann Sie gewarnt werden und auf welche Angriffsmethoden geachtet werden soll. Zudem können Datenerfassung, Warnungen und Reaktionen bei wichtigen Elementen automatisiert sowie die Konfiguration an individuelle Workflows angepasst werden.
- **Kontinuierlich:** Persistente Kollektoren aktivieren bei Erkennung von Angriffsereignissen Auslöser und geben Warnungen über Angriffsaktivitäten an Sie und Ihre Systeme aus.

Wechselnde Bedrohungen

Unternehmen haben erkannt, dass ihnen jederzeit Kompromittierungen drohen und dass zur effektiven Abwehr gute Vorbereitung erforderlich ist, die eine frühzeitige Erkennung möglicher Angriffe sowie die Identifizierung laufender Aktivitäten oder vorhandener Angriffsindikatoren umfasst. Deshalb ist den Unternehmen auch bewusst, dass sie neue Technologien benötigen, die die derzeitigen Lücken in den Bereichen Transparenz, Erkennung und Reaktion schließen.

Grenzen aktueller Ansätze zur Reaktion auf Zwischenfälle

Wenn Verantwortliche für Reaktionen auf Zwischenfälle und Sicherheitsadministratoren die Aufgabe erhalten, verdächtige oder bekannt gefährliche Zwischenfälle im gesamten Unternehmen zu untersuchen, werden ihre Möglichkeiten meist von zwei Faktoren eingeschränkt: Zeit und Umfang. Während bestehende Systeme und Tools zahlreiche detaillierte Informationen sammeln, dauert die Erfassung und Analyse dieser Informationen sehr lange. Um die für die Datenerfassung so wichtige Geschwindigkeit zu gewährleisten, werden bei der Definition der zu erfassenden Daten sowie der Wahl der erfassten Systeme erhebliche Kompromisse eingegangen. Zudem wird es immer schwieriger, die schiere Menge der erfassten Daten überhaupt auf wichtige Informationen zu untersuchen.

Bei den meisten Tools zur Reaktion auf Zwischenfälle handelt es sich um Skripte, die von den Verantwortlichen selbst geschrieben wurden. Diese Tools erfassen die Daten, die für eine umfassendere Analyse berücksichtigt

intel Security

Systemanforderungen

Mindestanforderungen an die Hardware
Der Server kann bei Bedarf in einer virtuellen Maschine installiert werden. Für den McAfee Active Response-Server gelten folgende Hardware-Mindestanforderungen:

- 4 Intel® Xeon®-CPUs X5675, 3,07 GHz
- 8 GB Arbeitsspeicher
- SSD mit 120 GB

Anforderungen an die Dienstinfrastruktur
- McAfee® ePolicy Orchestrator® (McAfee ePO™) 5.1.1 oder höher
- McAfee Agent 5.0-Erweiterung oder höher
- McAfee Data Exchange Layer 2.0.0.405 Broker oder höher

Unterstützte Web-Browser
- Microsoft Internet Explorer ab Version 9
- Google Chrome ab Version 17
- Mozilla Firefox ab Version 10.0

Erforderliche Client-Infrastruktur
- McAfee Agent 5.0.0.2710 oder höher für Linux-Endgeräte
- McAfee Agent 5.0.0.2610 oder höher für Microsoft Windows-Endgeräte
- Clients mit McAfee Data Exchange Layer 2.0.0.405 oder höher auf allen verwalteten Endgeräten

werden sollen. Dieses Wissen sowie die zugehörigen Tools sind ziemlich ausgereift, doch die Möglichkeiten zur Skalierung und schnellen Bearbeitung sind beschränkt. Da die Verantwortlichen keine Live-Untersuchungen zu spezifischen Angriffsindikatoren für das gesamte Unternehmen durchführen können, bleiben die Bemühungen zur Erkennung und Reaktion meist kurzsichtig. Zudem werden diese Bemühungen häufig dadurch behindert, dass zeitliche Anforderungen eingehalten werden sollen, wodurch die Möglichkeiten zur Reaktion auf Zwischenfälle zusätzlich eingeschränkt werden. Und als wäre dies nicht genug, legen die begrenzten Möglichkeiten aktueller Tools den Sicherheitsverantwortlichen weitere Steine in den Weg.

Umfassende Erkennungs- und Reaktionsmöglichkeiten für Endgeräte

McAfee Active Response ermöglicht die kontinuierliche Erkennung und Reaktion auf hochentwickelte Sicherheitsbedrohungen, damit Sicherheitsverantwortliche die Sicherheitslage überwachen, die Bedrohungserkennung verbessern und die Möglichkeiten zur Reaktion auf Zwischenfälle erweitern können. Hierfür stehen vorausschauende Erkennung, detaillierte Analysen, forensische Untersuchungen, umfassende Berichterstellung sowie mit Prioritäten versehene Warnmeldungen und Aktionen zur Verfügung. McAfee Active Response wurde darauf optimiert, strenge Kriterien zur Endgeräteerkennung und Reaktion zu erfüllen.

Dazu nutzt die Lösung vordefinierte sowie anpassbare Kollektoren, die in allen Systemen intensiv nach Angriffsindikatoren suchen, wobei neben aktuell ausgeführten Prozessen auch ruhende oder gelöschte Prozesse berücksichtigt werden. Zudem ermöglicht McAfee Active Response nicht nur die Suche nach aktuell vorhandenen Angriffsindikatoren: Zur Einhaltung von Sicherheitszielen kann der Benutzer Auslöser definieren, damit bei zukünftigen Erkennungen eines bestimmten Angriffsindikators eine Warnung ausgegeben und eine Aktion vorgeschlagen wird.

McAfee Active Response ist der beste Beweis für die Effektivität der integrierten Intel Security-Sicherheitsarchitektur, die darauf ausgelegt ist, in einer immer komplexer werdenden Welt mehr Bedrohungen schneller und mit weniger Ressourcen abzuwehren. Dazu bietet die Lösung einen kontinuierlichen Überblick sowie äußerst nützliche Informationen zu Ihren Endgeräten, damit Sie Kompromittierungen schneller erkennen können. Zudem erhalten Sie die Tools, die Sie zur schnelleren und für Ihr Unternehmen sinnvollen Problembehebung benötigen. Alle diese Funktionen werden – mithilfe von McAfee Data Exchange Layer – über McAfee® ePolicy Orchestrator® (McAfee ePO™) verwaltet, sodass Sie Ihren Schutz einheitlich skalieren und erweitern können, ohne zusätzliche Mitarbeiter zur Produktverwaltung zu benötigen.

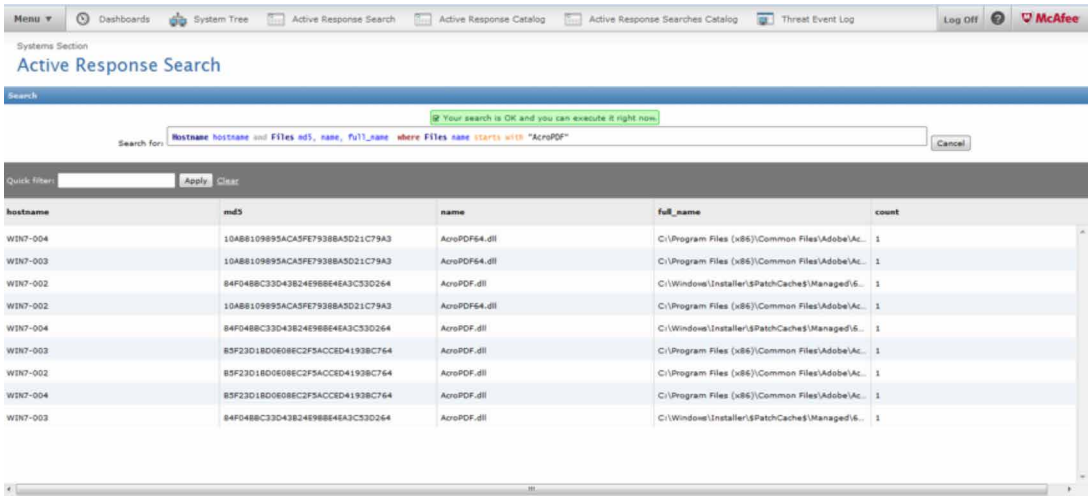

Abbildung 1. Suchfunktion der Benutzeroberfläche von McAfee Active Response

Unterstützte Client-Betriebssysteme

- Microsoft Windows
  - Windows 8.0 Standard (32-Bit- und 64-Bit-Version)
  - Windows 8.1 Standard, mit Update 1 (U1) (32-Bit- und 64-Bit-Version)
  - Windows Server 2012, Standard, R2, U1 (64-Bit-Version)
  - Windows Server 2008 R2 Enterprise, SP1 (64-Bit-Version)
  - Windows Server 2008 R2 Standard, SP1 (64-Bit-Version)
  - Windows 7 Enterprise bis SP1 (32-Bit- und 64-Bit-Version)
  - Windows 7 Professional bis SP1 (32-Bit- und 64-Bit-Version)
- CentOS 6.5 (32-Bit-Version)
- RedHat 6.5 (32 Bit-Version)

Komponente	Vorteil	Kundenvorteile	Differenzierung
Kollektoren	Kollektoren ermöglichen Benutzern die Suche in sowie Visualisierung von Daten, die sich auf ihren Systemen befinden.	Kollektoren bieten Suchfunktionen zur genauen Untersuchung der Systeme. Sie ermöglichen einen Überblick über kritische potenzielle Kompromittierungen und Angriffe, damit Sie die Daten von diesen Systemen erfassen und visualisieren können. Benutzer können eine von mehreren gebräuchlichen Skript-Sprachen wählen, um auf einfache Weise eigene Kollektoren und Reaktionen anzupassen. Das bedeutet optimale Konfigurier- und Anpassbarkeit.	McAfee Active Response untersucht nicht nur ausgeführte Prozesse oder Dateien, sondern auch ruhenden oder solchen Code, der beim Versuch, die Angriffsspuren zu verwischen, gelöscht wurde. Dabei kann McAfee Active Response nach Dateien, Netzwerkverkehr, Registrierungsdaten und Prozesszuordnungen suchen.
Auslöser	Auslöser erlauben Sicherheitsverantwortlichen die kontinuierliche Überwachung kritischer Ereignisse oder Zustands-änderungen anhand mehrerer Anweisungen. Dabei werden aktuelle und zukünftige Ereignisse oder Änderungen berücksichtigt.	Die Aktionen, bei denen es sich um Ereignisgenerierungen oder Reaktionen handeln kann, werden basierend auf zuvor definierten Auslösern ausgeführt. McAfee Active Response führt dabei nicht nur statische und kurzfristige Maßnahmen, sondern kontinuierliche Reaktionen durch.	McAfee Active Response kann heute Bedrohungen erkennen und Aktionen für Bedrohungen auslösen, die möglicherweise morgen eintreten.
Reaktionen	Reaktionen bieten vorkonfigurierte und anpassbare Aktionen, die ausgeführt werden, weil eine Auslöserbedingung erfüllt wird. Dadurch können Sie Bedrohungen erkennen und beheben.	Reaktionen ermöglichen Benutzern, Aktionen durchzuführen. Mögliche Suchen umfassen zum Beispiel Datei-Hashes (MD5 oder SHA1) gelöschter Dateien, Hosts mit aktiven oder nicht mehr aktiven Verbindungen zu einer IP-Adresse, nicht-PE-basierte böswillige Dateien, auf die nicht zugegriffen wurde oder die nicht auf dem System „ausgelöst“ wurden (z. B. böswillige PDF-Dateien auf einem System, die kopiert aber nicht geöffnet wurden).	McAfee Active Response ist so vorkonfiguriert, dass die Lösung basierend auf Suchergebnissen reagiert und benutzerdefinierte Aktionen ausführt, die der Benutzer zur Erfüllung individueller Anforderungen festgelegt hat.
Zentrale Verwaltung durch die Software McAfee ePO	Die Umgebung mit nur einer Konsole ermöglicht umfassende Verwaltung und Automatisierung.	Administratoren können die Software McAfee ePO als Teil der integrierten Intel Security-Sicherheitsarchitektur nutzen, um automatische Reaktionen zu Auslösern und Suchergebnissen zu unterstützen und auf Bedrohungen reagieren sowie diese beheben zu können. Die Verwaltung über eine einzige Oberfläche verbessert die Sicherheitstransparenz, ohne den Administrationsaufwand zu erhöhen. Dieser Ansatz vereinfacht Betriebsabläufe und verringert den Zeitaufwand für die Administratoren.	Die Verwaltung sowie Steuerung über eine zentrale Konsole ist ein deutliches Alleinstellungsmerkmal. Dank der zentralen Konsole können wir eine Vielzahl von Plattformen mit leistungsstarken Sicherheitskontrollen schützen, wozu auch McAfee Active Response gehört.
Integrierte Sicherheitsarchitektur	Das Framework nutzt den Data Exchange Layer, um die Kommunikation mit anderen Produkten von McAfee, einem Geschäftsbereich von Intel Security, zu optimieren.	Dank des innovativen Konzepts, der optimierten Prozesse sowie der praktischen Empfehlungen, durch die sich diese Plattform auszeichnet, können Unternehmen mit McAfee Active Response, das zur integrierten Intel Security-Sicherheitsarchitektur gehört, nicht nur die Risiken sowie den Zeitaufwand für Erkennung und Reaktion reduzieren, sondern gleichzeitig den Verwaltungsaufwand minimieren und die Betriebskosten senken.	

Weitere Informationen zu den Vorteilen von McAfee Active Response finden Sie unter **www.mcafee.com/de/products/active-response.aspx**.

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