



McAfee Artemis Technology: Ständig aktiver Echtzeitschutz

Die Geschwindigkeit, mit der Malware heute verbreitet wird, erschwert Sicherheitsanbietern die ständige Aktualisierung ihrer herkömmlichen Sicherheitsverfahren (Signaturen). Aus diesem Grund ist eine Korrelation von Signaturen und Verhaltensweisen erforderlich, die eine Analyse der Bedrohungen in Echtzeit anhand der Daten der gesamten Benutzergemeinde ermöglicht. Die McAfee® Artemis Technology ist der erste Echtzeitschutz, der „ständig aktiv“ ist und Unternehmen sowie Privatbenutzer vor Bedrohungen schützt, sobald diese auftreten. McAfee-Kunden können sich nun das Wissen der Internetgemeinde zunutze machen und sich vor Schäden schützen, noch bevor eine aktualisierte Signatur verfügbar ist - und so ihre Endgeräte ohne Mehrkosten intelligenter und sicherer machen.

WICHTIGE FUNKTIONEN UND VORTEILE

- **Echtzeitschutz gegen Malware verringert die Sicherheitslücke und die Anfälligkeit für auftretende Bedrohungen beträchtlich**
- **Veränderliche Empfindlichkeitsniveaus für „verdächtige“ Dateien ermöglichen Unternehmen die Anpassung ihrer Risikotoleranz**
- **Nahtlose Bereitstellung über McAfee ePO™ implementiert kostenlosen Echtzeitschutz ohne Installations- und Verwaltungsaufwand**

Die Bedrohungslage im Internet

Die beispiellose Zunahme an Malware erschwert Sicherheitsanbietern die ständige Anpassung ihrer Sicherheitslösungen an die aktuelle Sicherheitslage im Internet. Die Anzahl der Malware-Programme, die im Jahr 2008 im Internet verbreitet wurden, überschreitet bereits jetzt die Zahlen aus 2006 und 2007 zusammen. Dies ist in erster Linie auf die veränderte Motivation der Cyberkriminellen zurückzuführen. Denn die sind jetzt hinter richtigem Geld her und nicht mehr nur an der Pflege ihrer Egos interessiert. Dem Unternehmensberater Gartner zufolge sind derzeit über 80 Prozent aller Angriffe finanziell motiviert. Der Verkauf der von Malware-Schreibern gesammelten personenbezogenen und vertraulichen Daten hat eine Cybercrime-Wirtschaft geschaffen, deren Umfang bereits mehrere Milliarden US-Dollar erreicht hat. Ein Großteil dieser Bedrohungen wird normalerweise versteckt verbreitet, sie sind entweder verschlüsselt oder in andere Dateien gepackt, um ihren wahren Inhalt zu verschleiern, ihre Größe zu verringern und den Sicherheitsanbietern die Analyse und die Bereitstellung eines geeigneten Schutzes zu erschweren.

Viele dieser Bedrohungen werden über die Sicherheitslücken häufig besuchter Webseiten sowie mithilfe von E-Mail-Nachrichten, Multimedia-Dateien oder Microsoft Office- und PDF-Dokumenten verbreitet. Der zunehmende Einsatz von Instant Messaging- und Social Networking-Webseiten hat der Malware-Verteilung zusätzliche Türen geöffnet. Dabei nutzen Cyberkriminelle häufig Social Engineering-Tricks, um sicherzustellen, dass Benutzer auch auf die Links zu den böswilligen Inhalten klicken oder bestimmte Dateien herunterladen. Über 82 Prozent der Social Networking-Benutzer laden unbekannte Dateien herunter. Aber auch die Ergebnisse bestimmter in Suchmaschinen eingegebener Schlüsselbegriffe enthalten eine Reihe von infizierten Webseiten.

Die „Sicherheitslücke“ in aktuellen Lösungen



Aktuelle Lösungen, die zum Schutz vor Bedrohungen einzig auf Signaturenverfahren basieren, weisen unter Umständen als Folge eine Sicherheitslücke auf. Diese ergibt sich aus dem Zeitraum zwischen der ersten Verbreitung einer Malware (zum Zeitpunkt t0) und der endgültigen Bereitstellung des Schutzes bei der Mehrheit der Benutzer (in unserer Grafik zum Zeitpunkt t4). Während dieser Zeit muss eine Bedrohung erkannt und analysiert, eine entsprechende Signatur entwickelt sowie an den Endgeräten bereitgestellt werden. Dies kann zwischen 24 und 72 Stunden dauern, in denen Benutzer vor dieser Bedrohung nicht geschützt sind. Daher setzen Sicherheitsanbieter an den Endgeräten häufig auch Lösungen mit verhaltensgesteuerten Verfahren ein (wie die Host Intrusion Protection-Systeme). Aber diese Systeme arbeiten voneinander getrennt, so dass keine Kommunikation zwischen ihnen stattfindet. Da es sich bei vielen Bedrohungen um versteckte und komplexe Angriffe handelt, die zur Infizierung der Systeme und ihrer eigenen Verbreitung mehrere Kanäle nutzen, wie E-Mails und Webseiten, kommt einer zentralen und kombinierten Analyse der von den Sicherheitslösungen der Benutzergemeinschaft gesammelten Daten eine entscheidende Bedeutung zu.

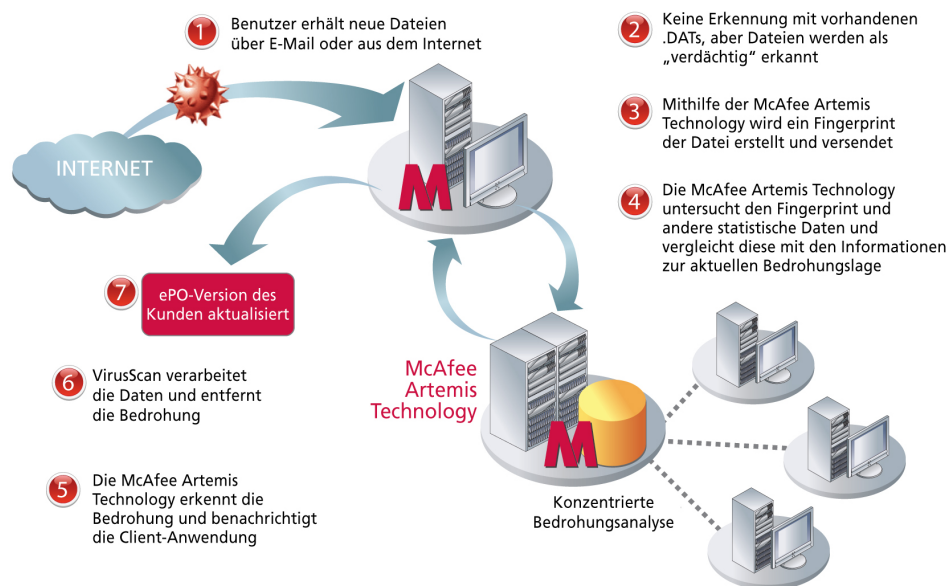
Kundenprobleme

Wer gegenüber solchen Bedrohungen ungeschützt bleibt, riskiert den Diebstahl vertraulicher und personenbezogener Daten, Einschnitte bei der Produktivität sowie Einkommens-, Image- und Vertrauensverluste. Schätzungen zufolge lassen sich die Schäden durch Angriffe bei Verbrauchern auf 1.200 US-Dollar und bei Unternehmen auf ca. 350.000 US-Dollar beziffern, so das Internet Crime Complaint Center des FBI und des National White Collar Crime Center. Zudem erhöhen solche Bedrohungen auch das Risiko einer Nichteinhaltung gesetzlicher Bestimmungen.

Um mit der Zunahme und der Heimtücke dieser Bedrohungen Schritt zu halten, müssen Sicherheitslösungen kreativere Ansätze und schnellere Reaktionen bieten. Außerdem müssen die Erkennung und die Bereitstellung des endgültigen Schutzes anstatt nach Stunden oder Tagen innerhalb weniger Minuten erfolgen und exakt genug sein, um dem Ausmaß und der Bedeutung der Internetnutzung im heutigen Wirtschaftsleben gerecht zu werden.

McAfee Artemis Technology

Bei der McAfee Artemis Technology handelt es sich um den ersten Echtzeitschutz, mit dem die Anfälligkeit für bekannte und neue Bedrohungen signifikant reduziert werden kann. Durch die Nutzung einer konzentrierten Bedrohungsanalyse aus den Daten der Benutzergemeinschaft reduziert die McAfee Artemis Technology den Bereitstellungszeitraum und schließt auf diese Weise die Sicherheitslücke. Dieser Schutz steht bei allen McAfee-Sicherheitsprodukten für Endgeräte ohne Zusatzkosten zur Verfügung. Er ist ständig aktiv und auf allen Systeme verfügbar, die mit dem Internet verbunden sind, ohne dass sich auf Benutzerseite ein Schulungs- oder Einarbeitungsaufwand ergibt.

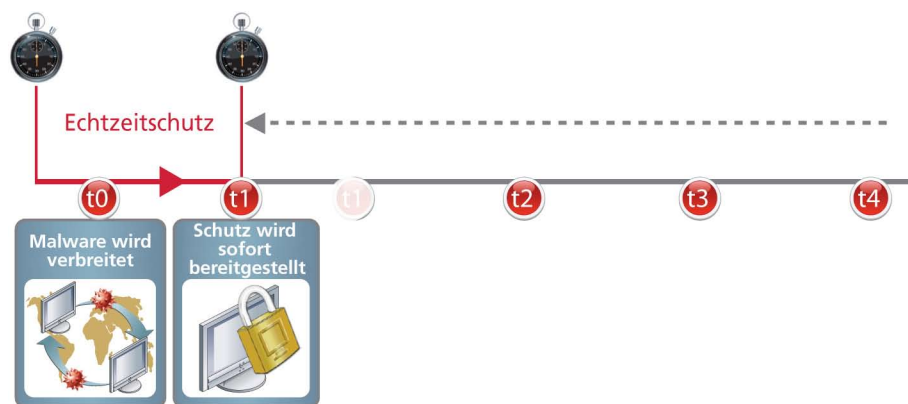


Die McAfee Artemis Technology bietet ein neuartiges, ständig aktives Bereitstellungsmodell für relevante und aktuelle Forschungs- und Reaktionsleistungen zum Schließen der Sicherheitslücke. Anhand der Kombination von Signatur- und Verhaltensanalyse sowie der Nutzung einer konzentrierten Bedrohungsanalyse aus den Daten der gesamten Benutzergemeinschaft ermöglicht das „Pull“-Modell einen bedarfsgerechten Echtzeitschutz der Systeme. Dabei handelt es sich

um eine zusätzliche Funktion, durch welche die bereits vorhandene signaturbasierte Erkennung erweitert wird. Sobald der Benutzer eine Datei erhält, die dem Scan-Agent „verdächtig“ erscheint (beispielsweise eine verschlüsselte oder gepackte Datei) und für die in der lokalen .DAT-Datenbank noch keine Signatur vorliegt, sendet der Agent mithilfe der Artemis Technology einen Fingerprint der Datei zur sofortigen Überprüfung an die umfassende Datenbank der McAfee Avert® Labs. Wird der Fingerprint als bekannte Malware identifiziert, sendet das Labor innerhalb weniger Millisekunden eine entsprechende Information an den Computer des Endbenutzers zurück, verbunden mit dem Hinweis, die fragliche Datei zu blockieren oder zu isolieren.

Schließen der Sicherheitslücke

Über die McAfee Artemis Technology steht den Endgeräten der Benutzer die gesamte Datenbank von Avert Labs mit ihren Bedrohungsanalysen zur Verfügung. Wann immer Malware auftritt, bleiben die Geräte auf diese Weise geschützt. Die Nutzung der Artemis Technology ist vergleichbar mit einem Avert Labs-Forscher, der neben Ihrem System steht und jede „verdächtige“ Datei auf eine ggf. vorhandene lokale Signatur überprüft. Da die zur Analyse herangezogenen Daten aus mehreren Quellen einschließlich der gesamten McAfee-Benutzergemeinschaft stammen, stehen Erkennung und Verfügbarkeit des Schutzes jetzt früher zur Verfügung als je zuvor. Diese Reduzierung der Sicherheitslücke verringert die Anfälligkeit für Bedrohungen erheblich.



Unternehmen haben auch die Möglichkeit, Ihre Risikotoleranz zu bewerten. Sie können hierzu das Empfindlichkeitsniveau von McAfee ePolicy Orchestrator® (ePO™) für die Erkennung „verdächtiger“ Dateien einstellen.

Kostenlose, optimierte Bereitstellung ohne Bedienungsaufwand

Die McAfee Artemis Technology ist ohne Zusatzkosten in die McAfee-Endgeräteprodukte integriert. In einer Unternehmensumgebung kann die Artemis Technology nahtlos über McAfee ePO genutzt werden, ohne dass hierzu auf dem Endgerät weitere Software oder eine zusätzliche Management-Komponente installiert werden muss. Die einfache Aktivierung einer Steuerungsoption reicht aus, um diesen bedarfsgerechten Echtzeitschutz auf allen Clients bereitzustellen. Dabei entstehen bei der Nutzung dieser zusätzlichen Schutzebene weder Schulungsaufwand noch Betriebs- oder Verwaltungskosten.

Verbrauchern wird die McAfee Artemis Technology über die Aktualisierung der .DATs bereitgestellt. Eine Aktualisierung der vorhandenen Software bzw. die Installation einer neuen Programmversion ist hierbei nicht erforderlich.

Wegen der schnellen und rein im Hintergrund ausgeführten Funktion der Artemis Technology ergeben sich für Benutzer keine Änderungen.

McAfee GmbH, Ohmstraße 1, 85716 Unterschleißheim, Deutschland, Telefon: +49 (0)89 3707 0, www.mcafee.com/de

McAfee, ePolicy Orchestrator, ePO, Avert und/oder andere genannte McAfee-Produkte in diesem Dokument sind eingetragene Marken oder Marken von McAfee, Inc. und/oder seinen Niederlassungen in den USA und/oder anderen Ländern. Die Farbe Rot in Verbindung mit Sicherheit ist ein Merkmal der McAfee-Produkte. Alle anderen nicht zu McAfee gehörenden Produkte sowie eingetragene und/oder nicht eingetragene Marken in diesem Dokument werden nur als Referenz genannt und sind Eigentum ihrer jeweiligen Rechtsinhaber. © 2008 McAfee, Inc. Alle Rechte vorbehalten.

1-na-cor-aptb-001-0808