McAfee Application Data Monitor

Erkennung verborgener Bedrohungen durch Überprüfung der Anwendungsschicht

Die McAfee® Application Data Monitor-Appliance überwacht den gesamten Pfad bis zur Anwendungsschicht und löst Sicherheit sowie Compliance damit von den Beschränkungen der Protokollverwaltung. Sie können die Anwendungsinhalte vollständig untersuchen, um einen umfassenden Überblick über die Nutzung Ihres Netzwerks zu erhalten.

Die McAfee Application Data Monitor-Appliance dekodiert die gesamte Anwendungssitzung bis zur Schicht 7 und ermöglicht die vollständige Analyse des gesamten verwendeten Protokolls sowie der Sitzungsintegrität, aber auch der eigentlichen Anwendungsinhalte (z. B. den Text oder die Anlage einer E-Mail). Diese Detailtiefe bildet die Grundlage für die genaue Analyse der tatsächlichen Anwendungsnutzung und bietet gleichzeitig die Möglichkeit, die Nutzungsrichtlinien für die Anwendung zu erzwingen sowie verborgenen böswilligen Datenverkehr zu erkennen.

Diese tiefgründige Untersuchung unterstützt Ihre Compliance-Maßnahmen, da jegliche Nutzung vertraulicher Daten im Netzwerk überwacht wird. Wenn die McAfee Application Data Monitor-Appliance eine Richtlinienverletzung erkennt, werden alle Details über diese Anwendungssitzung zwecks Gegenmaßnahmen, Forensik oder aufgrund von Compliance-Audit-Anforderungen gespeichert.

Gleichzeitig bietet die McAfee Application Data Monitor-Appliance einen Überblick über Bedrohungen, die sich möglicherweise als legitime Anwendungen tarnen:

- Hochentwickelte Bedrohungen der Anwendungsschicht
- Unberechtigte Verwendung oder Diebstahl vertraulicher Daten
- Angriff auf oder aus „blinden Punkten“ der Sicherheitsmaßnahmen heraus
- Verwendung von gefährlichem, älterem Code
- Diebstahl oder Missbrauch von Benutzeranmeldedaten
- Übertragung sensibler Daten über eine Anwendung
- Fehlerhafte Geschäftsabläufe

Hauptvorteile

- Dekodierung der gesamten Anwendungssitzung bis zur Schicht 7 für hunderte Anwendungen
- Inklusive vorinstallierter Erkennungsregeln für regulierte und vertrauliche Daten
- Unterstützung benutzerdefinierter Wörterbücher und Regeln
- Generierung vollständiger Audit-Protokolle zu Anwendungsereignissen zum Nachweis der Compliance
- Passiver Betrieb im Hintergrund, um eine Beeinträchtigung der Anwendung zu vermeiden
- Integration in McAfee Enterprise Security Manager, um Korrelation von Anwendungsinhalten mit Ereignissen und anderen Datenquellen zu ermöglichen
- Flexible Hybrid-Bereitstellungsoptionen mit physischen und virtuellen Appliances

Datenverlust und Verstöße gegen Compliance-Richtlinien

Die McAfee Application Data Monitor-Appliance erkennt die Übertragung sensibler Informationen innerhalb von E-Mail-Anlagen, Sofortnachrichten, Dateiübertragungen, HTTP-Posts oder anderen Anwendungen und benachrichtigt Sie sofort darüber, damit die Kompromittierung verhindert werden kann.

Sie können sofort nach der Installation sensible Informationen wie Kreditkartendaten und Steueridentifikationsnummern erkennen oder die Erkennungsfunktionen der McAfee Application Data Monitor-Appliance anpassen, indem Sie eigene Wörterbücher für Ihre sensiblen und vertraulichen Informationen definieren. Die Appliance erkennt diese Datentypen, benachrichtigt die verantwortlichen Mitarbeiter und protokolliert den Sicherheitsverstoß für das Audit-Protokoll.

Dokumenterkennung

Die McAfee Application Data Monitor-Appliance erkennt mehr als 500 Dokumenttypen, die per E-Mail, Chat, P2P, Dateifreigaben und andere Kommunikationsmittel über das Netzwerk übertragen werden – unabhängig davon, ob sie sich als anderer Dateityp ausgeben, um E-Mail-Gateways und Geräte für Eindringungserkennung (IDS) bzw. Eindringungsschutz (IPS) zu umgehen. Selbst Dokumente, die in andere Dokumente eingebettet sind, sowie archivierte, komprimierte und verschlüsselte Dokumente werden anhand abrufbarer Rahmendaten wie Dateiname und durchgeführter Vorgänge erkannt.

Bedrohungen der Anwendungsschicht

Die neuen ausgeklügelten Bedrohungen nutzen Schwachstellen in verbreiteten Geschäftsanwendungen aus, um in Ihr Netzwerk zu gelangen und vertrauliche Daten auszuspähen. Während diese Bedrohungen der Anwendungsschicht mithilfe herkömmlicher Firewalls und IDS- sowie IPS-Systeme nur schwer zu erkennen sind, kann die McAfee Application Data Monitor-Appliance den gesamten Inhalt der Anwendung (einschließlich der verwendeten Protokolle) analysieren, um verborgene Schaddaten, Malware und verborgene Kommunikationskanäle zu erkennen. Dabei kann es sich beispielsweise um eine ausführbare Datei handeln, die in ein PDF-Dokument eingebettet wurde.

Protokollanomalien

Die Anomalieerkennung kann proaktiv zur Identifizierung bevorstehender Bedrohungen sowie zur Risiko- und Verlustminimierung eingesetzt werden. Während einige herkömmliche Sicherheitslösungen nur den Netzwerkdatenfluss analysieren können, geht die McAfee Application Data Monitor-Appliance einen Schritt weiter: Sie erkennt nicht nur Anomalien im Netzwerkverhalten, sondern auch innerhalb von Anwendungen und Protokollen, sodass Risiken zuverlässiger und vorausschauender identifiziert werden.

Keine Beeinträchtigungen für Anwendungen

Da die McAfee Application Data Monitor-Appliance einen SPAN-Port nutzt, beeinträchtigt sie weder die Anwendungsleistung noch deren Zuverlässigkeit und verursacht keine Latenzen.

Mehr als 500 unterstützte Anwendungen und Protokolle

- **Netzwerkprotokoll auf niedriger Ebene:** TCP/IP, UDP, RTP, RPC, SOCKS, DNS usw.
- **E-Mail:** MAPI, NNTP, POP3, SMTP, Microsoft Exchange
- **Web-Mail:** AOL Webmail, Hotmail, Yahoo! Mail, Google Mail, Facebook und MySpace-E-Mail
- **Instant Messaging:** AOL, ICQ, Jabber, MSN, SIP und Yahoo!
- **Dateiübertragungsprotokolle:** FTP, HTTP, SMB und SSL
- **Protokolle zum Komprimieren und Entpacken von Daten:** BASE64, GZIP, MIME, TAR, ZIP usw.
- **Archivdateien:** RAR, ZIP, BZIP, GZIP, Bin-hex und per UU-codierte Archive
- **Installationspakete:** Linux-Pakete, InstallShield-CAB-Dateien, Microsoft-CAB-Dateien
- **Bilddateien:** GIF, JPEG, PNG, TIFF, AutoCAD, Photoshop, Bitmap, Visio, Digital RAW und Windows-Symbole
- **Audiodateien:** WAV, MIDI, RealAudio, Dolby Digital AC-3, MP3, MP4, MOD, RealAudio, SHOUTCast usw.
- **Videodateien:** AVI, Flash, QuickTime, Real Media, MPEG-4, Vivo, Digital Video (DV), Motion JPEG usw.
- **Weitere Anwendungen und Dateien:** Datenbanken, Tabellenblätter, Faxe, Web-Anwendungen, Schriftarten, ausführbare Dateien, Microsoft Office-Anwendungen, Spiele sowie Software-Entwicklungs-Tools
- **Weitere Protokolle:** Netzwerkdrucker, Shell-Zugriff, VoIP und Peer-to-Peer

Integration in Ihre Infrastruktur

Im Gegensatz zu den meisten Netzwerküberwachungslösungen arbeitet die McAfee Application Data Monitor-Appliance nicht isoliert, sondern zusammen mit anderen Informationssicherheitssystemen. Über McAfee Enterprise Security Manager verbindet sich die Lösung mit Ihrer übrigen Sicherheitsinfrastruktur und vereinfacht so die Sicherheitsabläufe, verbessert die Gesamteffizienz und senkt Kosten. Sie können die Kompromittierungs- und Betrugserkennung mit leistungsstarken Analysen, Netzwerkuntersuchungen, Datenbank-Ereignisüberwachung und anderen Funktionen verzahnen.

Anwendungsfälle

Die McAfee Application Data Monitor-Appliance erkennt eine Vielzahl unberechtigter Aktivitäten, Richtlinienverletzungen sowie Diebstahl und Betrugsversuche. Im Folgenden werden einige Beispiele genannt.

Diebstahl vertraulicher Informationen

Ein als mmustermann@unternehmen.com angemeldeter Mitarbeiter sendet eine E-Mail an komplize@gmail.com. An die E-Mail ist eine Datei mit dem Namen „shoo.doc“ angehängt, die die Wörter „geheime Formel“ enthält. Die E-Mail wurde um 12:20 Uhr vom Host-Desktop 0232 (192.168.0.36) über den SMTP-Server (10.0.2.13) gesendet. Der Betreff: „Ich hab's.“

Verwendung unzulässiger Anwendungen

Ein Mitarbeiter verstößt gegen die Richtlinie, indem er über eine von ihm installierte Anwendung für den Peer-to-Peer-Dateiaustausch eine Musikdatei freigibt. Während seiner Arbeitszeit wurden über diese Anwendung große Dateien versendet, die wertvolle Bandbreite verbrauchten. Bei weiteren Untersuchungen wurde festgestellt, dass der Mitarbeiter auch gegen weitere Richtlinien verstößt: Er verwendet Jabber sowie IRC und nutzt auf seinem Desktop einen nicht zugelassenen Web-Server.

Cyberslacking am Arbeitsplatz

Eine Angestellte betätigt sich gleichzeitig als Tageshändlerin. Während der Arbeitszeit greift sie vormittags und nachmittags jeweils etwa eine Stunde auf Börsenwebseiten zu. Über das unternehmenseigene VoIP-System (SIP) tätigt sie etwa sechs Telefonate pro Tag und verbringt im Yahoo! Messenger Stunden als „traderjoe“ im Chat mit „traderbob“ und „tradergill“.

Nutzung schwacher Kennwörter

In der Sicherheitsrichtlinie Ihres Unternehmens ist festgelegt, dass für alle Benutzersystem- und Anwendungskonten starke Kennwörter verwendet werden müssen. Während die strikt verwalteten Microsoft Active Directory-Konten diese Anforderung erfüllen, sind die Kennwörter für FTP- und E-Mail-Server sowie wichtige Web-Anwendungen, die nicht über Active Directory verwaltet werden, häufig schwach.

Weitere Informationen

Weitere Informationen finden Sie unter **www.mcafee.com/de/products/siem/index.aspx**.

McAfee
Together is power.

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

61322ds_app-data-monitor_0914
SEPTEMBER 2014