McAfee Host Intrusion Prevention for Server

Verbesserter Schwachstellenschutz für Server und Anwendungen

Auf Unternehmens-Servern befinden sich die wertvollsten Informationen eines Unternehmens. Zudem sorgen die Server auch für unterbrechungsfreie Geschäftsabläufe. Deshalb besteht eine der größten Herausforderungen für IT-Mitarbeiter darin, diese Server und die darauf gehosteten Anwendungen vollständig vor bekannten sowie unbekannten Angriffen zu schützen, die geschäftliche Abläufe stören können.

McAfee Host Intrusion Prevention for Server

McAfee® Host Intrusion Prevention for Server verfügt neben speziellem Schutz für Datenbank-Server und das Web, mit dem die Systemverfügbarkeit sowie ein störungsfreier Geschäftsbetrieb aufrechterhalten wird, auch über die branchenweit einzige dynamische sowie statusbasierte Firewall zum Schutz vor hochentwickelten Bedrohungen und böswilligem Datenverkehr. Zudem bietet die Lösung Schutz durch ein signatur- und verhaltensorientiertes Eindringungsschutzsystem (IPS). McAfee Host Intrusion Prevention for Server reduziert die Häufigkeit und Dringlichkeit von Patches, gewährleistet störungsfreien Geschäftsbetrieb sowie Mitarbeiter-produktivität, schützt die Vertraulichkeit von Daten und vereinfacht die Einhaltung von Compliance-Vorschriften.

Abwehr von Angriffen auf Server und Anwendungen sowie Schutz vor Datenkompromittierung

Es kommt immer häufiger zu Angriffen auf Server, da sie nicht nur große Mengen an Unternehmensdaten beherbergen, sondern auch für die täglichen Abläufe wichtig sind. Mit McAfee Host Intrusion Prevention for Server werden unternehmenskritische Server geschützt und die Systemverfügbarkeit sowie Produktivität aufrechterhalten.

- Schutz für Web-Server:
  - Filterung von HTTP-Anfragen zur Verhinderung von Verzeichniswechsel-, Unicode- und Denial-of-Service-Angriffen (DoS)
  - Nutzung vordefinierter Schutzrichtlinien und -regeln zur Verhinderung von Angriffen und Datenverlust
- Schutz für Datenbank-Server:
  - Untersuchung von Datenbankanfragen zur Verhinderung von Angriffen wie SQL-Injektion
  - Nutzung vordefinierter Schutzrichtlinien und -regeln zur Gewährleistung normalen Verhaltens und Verhinderung von Datenmanipulation

Hauptvorteile

Besserer Schutz

- Durchsetzung von umfassendstem IPS- und Zero-Day- Bedrohungs-schutz auf allen Ebenen: Netzwerk, Anwendungen und Ausführung

Geringere Kosten

- Verringerung des Zeit- und Kosten-aufwands mit einer leistungs-starken, zentralen Konsole für Bereitstellung, Verwaltung, Reporting und Audits von Vorfällen, Richtlinien und Agenten
- Verringerte Häufigkeit und Dringlichkeit von Endgeräte-Patches

Vereinfachte Compliance

- Verwaltung der Einhaltung mit leicht verständlichen, umsetzbaren Ansichten, Workflows, Ereignisüberwachung und Reporting für prompte und gründliche Untersuchungen und Analysen

Hochentwickelter Schutz vor Bedrohungen durch unsere dynamische, statusbasierte System-Firewall

Im Gegensatz zu herkömmlichen System-Firewalls, die mit festgelegten Regeln arbeiten, verfügt McAfee Host Intrusion Prevention for Server dank der McAfee Global Threat Intelligence (McAfee GTI)-Integration über Reputationsdaten zu Netzwerkverbindungen, sodass Server vor hochentwickelten Bedrohungen wie Botnets, DDoS-Angriffen (Distributed Denial-of-Service) sowie neuem böswilligem Datenverkehr geschützt werden können, noch bevor ein Angriff beginnen kann. In Anbetracht der steigenden Anzahl hochentwickelter Bedrohungen stellt McAfee GTI den ausgereiftesten Schutz dar, den Sie implementieren können.

Durchführung von Betriebssystem- und Anwendungs-Patches ist seltener, weniger dringlich und nach eigenem Zeitplan möglich

Ein großer Teil der Angriffe erfolgt innerhalb von drei Tagen nach Entdeckung einer Schwachstelle. Viele Unternehmen benötigen jedoch bis zu 30 Tage, um Patches auf allen Endgeräten zu testen und zu implementieren.

McAfee Host Intrusion Prevention for Server schließt diese Sicherheitslücke und macht den Patch-Prozess einfacher und effizienter.

- Der Schutz umfasst Schwachstellen bei Microsoft- sowie bei Adobe-Anwendungen. Der Schwachstellenschutz aktualisiert Signaturen automatisch, um Endgeräte vor Angriffen auf Schwachstellen zu schützen.
- Für vertrauenswürdigen Schutz können Signatur-Updates automatisch und regelmäßig heruntergeladen werden.

Server sind während des Systemstarts nicht mehr gefährdet

Weil Sicherheitsrichtlinien während des Systemstarts noch nicht greifen, sind Server zu diesem Zeitpunkt besonders gefährdet. In dieser Phase sind sie beispielsweise für netzwerkbasierte Angriffe anfällig. Zudem könnten Sicherheitsdienste deaktiviert werden. McAfee Host Intrusion Prevention for Server blockiert Angriffe während dieses sensiblen Zeitfensters per Firewall und Eindringungsschutzsystem.

- Der Firewall-Schutz beim Systemstart lässt während des Startvorgangs so lange nur ausgehenden Datenverkehr zu, bis die komplette Firewall-Richtlinie greift wurde.
- Der IPS-Schutz beim Systemstart verhindert die Deaktivierung unserer Sicherheitsdienste, bis die komplette IPS-Richtlinie durchgesetzt wurde.

Vereinfachte und optimierte Verwaltung

Für große Unternehmen ist die Erstellung und Verwaltung mehrerer Firewall- und IPS-Richtlinien eine unbedingt erforderliche, gleichzeitig aber auch mühsame und zeitaufwändige Aufgabe. Dank der in McAfee Host Intrusion Prevention for Server enthaltenen Richtlinien- und IPS-Kataloge wird diese Arbeit optimiert. Zudem können Sie mehrere Firewall- und IPS-Richtlinien erstellen sowie verwalten und bei Bedarf anwenden.

Systemanforderungen

Mindestanforderungen an die Hardware

- Intel oder AMD x86 und x64
- Freier Speicherplatz (Client): 15 MB, aber 100 MB während der Installation
- Arbeitsspeicher: 256 MB RAM
- Netzwerkumgebung: Microsoft- bzw. Novell NetWare-Netzwerke; NetWare-Netzwerke benötigen TCP/IP
- Netzwerkkarte: Netzwerkschnittstellenkarte; 10 Mbit/s oder höher

Unterstützte Betriebssysteme

- Microsoft Windows Server 2003 SP2, 2003 R2, 2003 R2 SP2 (alle Editionen, 32- und 64-Bit-Versionen)
- Microsoft Windows Server 2008, 2008 SP1, 2008 SP2, 2008 R2 (alle Editionen, 32- und 64-Bit-Versionen)
- SPARC Solaris 9 sun4u (32-Bit oder 64-Bit-Version)
- SPARC Solaris 10 sun4u, sun4v (32-Bit oder 64-Bit-Version)
- Red Hat Linux Enterprise 4, 32-Bit-Version
  - 2.6.9-5.EL
  - 2.6.9-5.Elhugemem
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 4, 64-Bit-Version
  - 2.6.9-5.EL
  - 2.6.9-5.ELsmp
- Red Hat Linux Enterprise 5, 32-Bit-Version
  - 2.6.18-8.el5
  - 2.6.18-8.el5PAE
- Red Hat Linux Enterprise 5, 64-Bit-Version
  - 2.6.18-8.el5

Mit unserer Konsole McAfee® ePolicy Orchestrator® (McAfee ePO™) zur zentralen Überwachung und Verwaltung aller Schutzmaßnahmen können Sie die Verwaltung zusätzlich optimieren und vereinfachen. Durch die vollständige Vernetzung mit McAfee ePO werden Ihre Abläufe erheblich effizienter, sodass Sie Zeit und Geld sparen.

Weitere Informationen erhalten Sie von einem Vertriebsrepräsentanten oder auf unserer Webseite unter **www.mcafee.com/de**.

Kompatibilität mit den größten Virtualisierungsplattformen

Heute nutzt so gut wie jede IT-Abteilung Virtualisierungsfunktionen, wodurch die Kompatibilität mit den größten Virtualisierungsplattformen für den Erfolg eines Produkts entscheidend ist. McAfee Host Intrusion Prevention for Server 8.0 ist mit den drei größten Virtualisierungsplattformen, d. h. VMware, Citrix und Microsoft Hyper-V, kompatibel. In der folgenden Tabelle sind die unterstützten Produkte dieser drei Anbieter aufgeführt.

VMware	Citrix	Microsoft
VMware ESX 3.5 und 4.0	Citrix XenServer 5.0 und 5.5	Microsoft Hyper-V Server 2008 und 2008 R2
VMware Vsphere 4.0	Citrix XenDesktop 3.0 und 4.0	Microsoft VDI
VMware View 3.1 und 4.0	Citrix XenApp 5.0 und 6.0	Microsoft App-V 4.5 und 4.6
VMware ThinApp 4.0 und 4.5		XP-Modus unter Windows 7
VMware ACE 2.5 und 2.6		
VMware Workstation 6.5 und 7.0		
VMware Player 2.5 und 3.0		

Systemanforderungen (Fortsetzung)

Unterstützte Betriebssysteme (Fortsetzung)

- SUSE Linux Enterprise 10, 32-Bit-Version
  - 2.6.16.21-0.8-bigsmp
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 10, 64-Bit-Version
  - 2.6.16.21-0.8-default
  - 2.6.16.21-0.8-smp
- SUSE Linux Enterprise 11, 32-Bit-Version
  - 2.6.27.19-5-default
  - 2.6.27.19-5-pae
- SUSE Linux Enterprise 11, 64-Bit-Version
  - 2.6.27.19-5-default

Unterstützte Web-Server

- Microsoft Windows
  - IIS 6.0 und 7.0
- SPARC Solaris
  - Apache-Web-Server ab Version 1.3.6
  - Apache-Web-Server ab 2.0.42
  - Apache-Web-Server ab 2.2.3
  - Sun Java Web Server 6.1
  - Sun Java Web Server 7.0
- Linux (RHEL und SUSE)
  - Apache-Web-Server ab 1.3.6
  - Apache-Web-Server ab 2.0.42
  - Apache-Web-Server ab 2.2.3

Unterstützte Datenbank-Server

- Microsoft SQL Server 2005 und 2008

McAfee
Together is power.

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