

McAfee Enterccept Standard Edition für Server und Desktops

Intrusion Prevention für geschäftskritische Systeme

Die Herausforderung

Die Anzahl neuer Sicherheitslücken und die Geschwindigkeit und Raffinesse, mit der diese Sicherheitslücken angegriffen und ausgenutzt werden, wächst jedes Jahr und erhöht die Risiken für die Sicherheit von Unternehmen. Neuartige komplexe Angriffe, die mithilfe zahlreicher Vektoren in die Sicherheitsinfrastruktur von Unternehmen eindringen, müssen abgewehrt werden.

Leider arbeiten herkömmliche IDS-Tools reaktiv, die Angreifer sind also immer einen Schritt voraus. Zur Gewährleistung umfassender, proaktiver Sicherheit benötigen Unternehmen ein mehrstufiges Sicherheitskonzept mit ineinandergreifenden und sich ergänzenden Technologien, die Netzwerke und Systeme von der Peripherie bis zum Kern schützen. Die McAfee® Intrusion Prevention-Lösungen bieten eine der umfassendsten, genauesten und skalierbarsten Angriffsabwehrlösungen auf dem Markt. Sie helfen Unternehmen, das Angriffsrisiko zu verringern, die Verfügbarkeit aufrechtzuerhalten und die Gesamtbetriebskosten zu reduzieren.

Die McAfee Enterccept-Lösung

Die McAfee Enterccept® Standard Edition liefert Host-basierte Angriffsabwehr für geschäftskritische Server und Desktops. Ihre patentierte, mehrfach ausgezeichnete Technologie schützt Systeme vor bekannten und unbekanntem Angriffen. Jeder zentral verwaltete Agent kombiniert Verhaltensregeln mit Signaturen, um Angriffe mit höchster Genauigkeit zu erkennen:

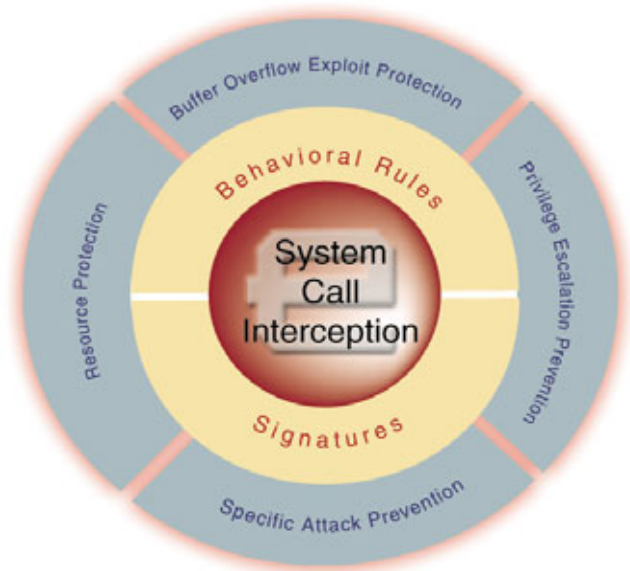
- **Systemaufrufe an das Betriebssystem** werden vor ihrer Verarbeitung mithilfe von Verhaltensregeln evaluiert. Verhaltensregeln bieten auch Schutz vor *Zero-Day* Angriffen, die durch neue Sicherheitslücken eindringen und für die es noch keinen Patch gibt
- **Signaturen** schützen Hosts, da sie bekannte schädliche Inhalte in Daten exakt identifizieren und gefährliche Schadensfunktionen blockieren, bevor sie ausgeführt werden. Dadurch lässt sich das Auftreten von Fehlalarmen erheblich reduzieren

Andere IPS Host-Produkte, die nur auf einer Erkennungstechnologie basieren, übersehen unter Umständen Angriffe. Enterccept dagegen stellt allen Servern, Desktops und Notebooks einen umfassenden, exakten und einfach zu verwaltenden Angriffsschutz zur Verfügung.

Vorteile

Umfassend

- Reduziert bei neuen Gefahren die Dringlichkeit der Patch-Implementierung
- Gewährleistet Integrität und Datenschutz für vertrauliche Daten
- IPS und Firewall schützen geschäftskritische Anwendungen vor Angriffen



McAfee Enterccept kombiniert Signaturen mit Verhaltensregeln, um bekannte und unbekannte Angriffe wie Buffer Overflows und Berechtigungs eskalation zu verhindern.

- Blockiert bekannte und sogenannte *Zero-Day* Angriffe (Angriffe auf eine neue, bisher unbekannte Sicherheitslücke)

Genau

- Signaturen verringern die falschen Einstufungen und liefern genaue und detaillierte Ereignisbeschreibungen
- Schutz vor *Zero-Day* Angriffen, z. B. Angriffe, die einen Buffer Overflow verursachen
- Vorkonfigurierte, individuell anpassbare Sicherheitsrichtlinien verringern das Auftreten von Fehlalarmen und die Sicherheitsspezialisten können sich wieder auf ihre eigentlichen Aufgaben konzentrieren

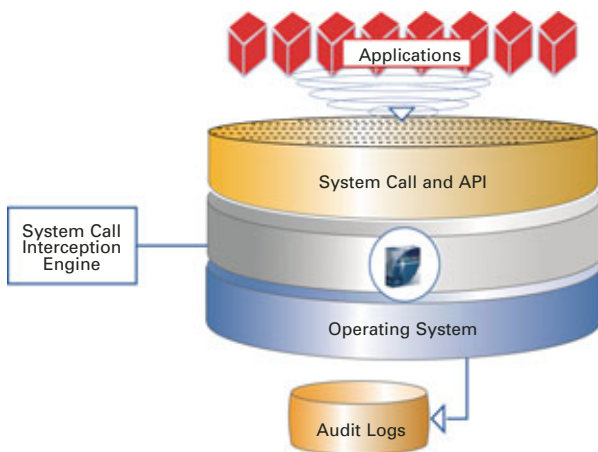
Skalierbar

- Verwaltung von mehreren Tausend Agenten mit einem einzigen Manager
- Optionale Implementierung und Überwachung von Agenten mit dem McAfee ePolicy Orchestrator® 3.5 (ab 3. Quartal 2004 verfügbar)
- Schützt die Betriebssysteme Windows®, Solaris und HP-UX mit patentierter, mehrfach ausgezeichneter Technologie
- Kein Eingreifen des Benutzers erforderlich, d. h. Anrufe beim IT-Helpdesk entfallen
- Installation bzw. Update im Hintergrund, kein Neustart erforderlich
- Individuell anpassbare Schutzebenen, von Protokollierung bis Blockierung

Funktionsweise der Enterecept Standard Edition

Jeder Agent wird mit einer vollständig konfigurierten Standardrichtlinie geliefert, die als Vorlage dient und ohne weitere Änderung verwendet werden kann. Der Agent enthält zudem leistungsstarke Optionen zur Anpassung, die erlauben, dass Sicherheitsspezialisten speziell auf ihre Umgebung abgestimmte Sicherheitsrichtlinien erstellen können, um das Auftreten von Fehlalarmen zu verringern. Agenten rufen automatisch verschlüsselte und authentifizierte Updates vom Management-System ab. Dadurch ist sichergestellt, dass jeder Agent mit den neuesten Richtlinien und neuen Angriffssignaturen arbeitet.

Der Agent überprüft zudem bestimmte System- und API-Aufrufe (diese werden von den Anwendungen zur Anforderung von Diensten des Betriebssystems verwendet). Er vergleicht dann schnell und effizient die Verhaltensregeln und bekannten Angriffssignaturen mit den verfügbaren Informationen zu jedem Aufruf (z. B. aufrufender Prozess, Sicherheitskontext des Prozesses, die aufgerufene Ressource usw.). Anschließend blockiert der Agent alle Aufrufe, die böswilliges Verhalten oder Malware auslösen würden.



Agenten der Standard Edition sind auf geschäftskritischen Systemen installiert und schützen dort Betriebssystem und Anwendungen vor Angriffen.

Features

Abwehr bekannter Angriffe — Mithilfe der umfangreichen Datenbank bekannter Angriffe kann McAfee Enterecept bekannte Angriffe blockieren und eine Infizierung der Server verhindern. Die Agenten rufen automatisch Updates neuer Angriffssignaturen aus der Datenbank ab.

Abwehr von Zero-Day Angriffen — Enterecept verhindert neue, noch unbekannte Angriffe mithilfe leistungsfähiger Verhaltensregeln. Dieser verhaltensorientierte Ansatz erzwingt von Betriebssystem und Anwendungen ein korrektes Verhalten und blockiert neue Angriffe, wenn diese die vordefinierten Regeln verletzen.

Verhindern von Buffer Overflows — Die patentierte Technologie von Enterecept verhindert die Ausführung von Code infolge eines Buffer Overflows. Agenten schützen

zudem geschäftskritische Server und Desktops vor diesen gefährlichen Angriffen. Diese Schwachstelle in der Sicherheit des Servers wird am häufigsten ausgenutzt.

Schutz der Ressourcen — Durch das Sperren wichtiger Systemressourcen (geschäftskritische Dateien, Einstellungen, Registry-Schlüssel, Services usw.) gewährleistet Enterecept sicheren Schutz.

Prozess-Firewall (nur Windows-Version) — Der Agent blockiert Netzwerkverkehr zum und vom System über einen hochgranularen Paketfilter und eine Firewall auf der Anwendungsschicht. Er analysiert mehr als 120 IP-Protokolle und kann Netzwerkangriffe wie z. B. WinNuke und Ausspähungstechniken wie z. B. Port-Scanning in Echtzeit blockieren.

Verhindern einer Berechtigungseskalation — Enterecept blockiert Angreifer, die sich unerlaubt Zugang zu Benutzerkonten ohne besondere Berechtigungen verschaffen und anschließend verschiedene Manipulationen durchführen, um Root-Berechtigungen zu erlangen.

Schneller Pfad zu Abwehrrichtlinien ohne weitere Anpassung — Auf der intuitiven Konsole von Enterecept können Benutzer geschäftskritische Systeme schnell auf eine hohe Sicherheitsstufe bringen, indem sie Richtlinien durch Ausnahmen definieren. Unternehmen können für Agenten immer höhere Sensitivitätsstufen festlegen, um ihr Schutz- und Abwehrverhalten schrittweise zu ändern. Auf diese Weise lassen sich Fehlalarme nahezu eliminieren und langfristige Anpassungen auf ein Minimum beschränken.

Implementierung und Überwachung mit dem McAfee ePO™ 3.5 — Optionen zur Installation, Aktualisierung und Überwachung von Agenten.

Ereignisaggregation — Das Enterecept Management-System fasst ähnliche Ereignisse zu einem einzigen Eintrag zusammen, um die Analyse zu vereinfachen.

Ereignisüberwachung durch Integration von HIPS und NIPS — Der IntruShield® 2.1 Manager importiert und korreliert die Alarmer der Enterecept-Agenten mit den Alarmen der IntruShield-Sensoren, um die Anzeige des Sicherheitsstatus für das gesamte System zu vereinheitlichen.

Installationsvoraussetzungen

Windows (nur englischsprachige BS-Versionen)

- Windows 2000 Server, Windows Advanced Server 2000, Windows 2003 Server
- Windows NT 4 Server oder Enterprise Server mit Service Pack 6a
- Windows XP

Solaris

- Solaris 7 (32-Bit und 64-Bit Kernel)
- Solaris 8 (32-Bit und 64-Bit Kernel)
- Solaris 9 (32-Bit und 64-Bit Kernel)

HP-UX

- HP-UX Ili (64-Bit PA-RISC)
- HP-UX II.0 (64-Bit PA-RISC)

McAfee GmbH

Ohmstraße 1, 85716 Unterschleißheim, Telefon: 089 – 37 07 0 | Luisenweg 40, 20537 Hamburg, Telefon: 040 – 25 31 0
Regus Center – Twin Tower, Wienerbergstraße 11/12 A, A-1100 Wien, Telefon: +43-(0)1-994 60 6202 | www.mcafee.de

Die Produkte von McAfee® zeichnen sich durch jahrelange Erfahrung und Engagement im Bereich Kundenzufriedenheit aus. Das PrimeSupport®-Team besteht aus hoch qualifizierten Support-Technikern, die Ihnen mit maßgeschneiderten Lösungen und detaillierter technischer Unterstützung bei der Verwaltung geschäftskritischer Projekte zum Erfolg verhelfen. Der Service-Level wird dabei jeweils an die Bedürfnisse des einzelnen Unternehmens angepasst. McAfee Research, marktführend in der Informationssysteme- und Sicherheitsforschung, führt die bahnbrechenden Innovationen bei der Entwicklung und Verbesserung unserer Technologien fort.

McAfee, Enterecept, ePolicy Orchestrator, ePO, IntruShield, und PrimeSupport 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 steht unverkennbar für alle McAfee® Markenprodukte. Alle anderen eingetragenen und nicht eingetragenen Marken in diesem Dokument sind Eigentum ihrer jeweiligen Besitzer. © 2004 Networks Associates Technology, Inc. Alle Rechte vorbehalten. 1-sps-ent-ese-gr-002-0704