Acht unerlässliche Firewall-Regeln

Angesichts der Unzahl von neuen Bedrohungen, die vom Web 2.0 ausgehen, bietet Ihre vorhandene Firewall eventuell keinen ausreichenden Schutz. Diese Checkliste soll Ihnen helfen, die fortschrittlichen Funktionen von Firewalls der nächsten Generation zu verstehen und Sie durch den Bewertungsprozess führen. Wir stellen veraltete oder auslaufende Systeme von Anbietern wie Cisco und Check Point der McAfee® Firewall Enterprise V8-Appliance der nächsten Generation gegenüber. Wenn Sie ein Upgrade im "Hauruck-Verfahren" vor sich haben, kann Sie diese Liste dabei unterstützen, Ihre Investition optimal zu nutzen.

Von IRC über P2P zu HTTP

"Seit kurzem ändert sich die Art und Weise, wie Bots gesteuert werden: Statt IRC-Channels werden nun Webseiten mit dem verbreiteten HTTP verwendet. Diese Änderung begann mit der Einführung von Exploit-Kits, die überwiegend von Internetkriminellen in Russland entwickelt wurden. Einige der führenden Kits sind Mpack, ICEPack und Fiesta. Sie können Software auf Remote-Computern installieren und sie von einer Remote-Webseite aus steuern."

"Hacker müssen einfach nur Spam mit Links senden, über die die Opfer auf eine Webseite gelangen, von der aus das Exploit-Kit installiert wird. Sobald das Exploit-Kit installiert ist, kann es bestimmen, welcher Exploit verwendet werden soll. Als Kriterien für die Auswahl dienen das Land, das Betriebssystem, der Browser und die Versionen mehrerer Client-Anwendungen auf dem System."

—McAfee Threat-Report, Viertes Quartal 2009

Regel 1 - Detaillierte Kontrolle erfordert auf die Interaktionen von Anwendern und Web 2.0-Anwendungen zugeschnittene Transparenz und Durchsetzung

Da der Großteil des heutigen Datenverkehrs über HTTP (Port 80) und HTTPS (Port 443) erfolgt, müssen Sie in der Lage sein, Einblick in diese Protokolle und Ports zu nehmen und den Datenverkehr, einschließlich verschlüsselter Nachrichten, gründlich prüfen zu können. Verschlüsselung ist heutzutage eine gängige Taktik der Internetkriminellen. Angriffe auf Client-Seite, die auf anfällige Web-Browser abzielen und verschlüsselte Verbindungen nutzen, passieren Ciscos Firewall, ohne entschlüsselt und geprüft zu werden, wodurch Netzwerke völlig ungeschützt sind.

Um Kontrolle ausüben zu können sollten Sie in der Lage sein aufzudecken, was vorgeht (z.B. Skype-Aktivitäten) und wer welche Anwendungen nutzt. So können Sie unternehmensgerechte Regeln festlegen, indem Anwender, Kontext und die notwendigen und angemessenen fortschrittlichen Web-Anwendungen aufeinander abgestimmt werden. So möchten Sie beispielsweise für die Kundendienst-Organisation hinter dem Web Service Portal IRC-Chat zulassen, aber FTP-Aktivitäten blockieren. Sie möchten vielleicht die Yahoo-Suche zulassen, aber die E-Mail- und Instant Messaging-Anwendungen von Yahoo sperren. Und Sie möchten vielleicht den Zugriff auf gefährliche oder unangemessene Webseiten blockieren, wenn es sich nicht um eine wirkliche geschäftliche Notwendigkeit für eine bestimmte Anwendergruppe handelt - in welchem Fall Sie dann in der Lage sein müssen, diese Richtlinie mit einer entsprechenden Regel durchzusetzen.

Fortschrittliche Firewalls der nächsten Generation, wie die McAfee Firewall Enterprise-Appliance, geben Ihnen eine Übersicht über den Datenverkehr von Anwendungen, einschließlich des ein- und ausgehenden verschlüsselten Datenverkehrs. Während Cisco nur VoIP-Verkehr entschlüsselt, damit dieser die Firewall passieren kann, überprüft McAfee SSH-, SFTP- und HTTPS-Verkehr auf bösartige Inhalte. Check Point bietet überhaupt keine Möglichkeit, verschlüsselten Datenverkehr zu prüfen.

Wir gehen über die Anwendungskontrolle hinaus, damit Sie Richtlinien für ein- und ausgehende Aktivitäten auf Anwenderebene durchsetzen können. Dieser Ansatz ermöglicht Ihnen, auf Grundlage der in Ihrem Microsoft Active Directory oder LDAP Directory bereits vorhandenen Benutzergruppen präzise Anwendungsregeln zu erstellen, die an Ihr Unternehmen angepasst sind. Diese Abstimmung auf Anwendungen und Anwender bedeutet eine detaillierte Kontrolle bei geringerem Verwaltungsaufwand.

Regel 2 - Mehrstufiger Bedrohungsschutz sollte keine Extrakosten bedeuten

Im Laufe der Zeit hat der Mangel an detaillierten Prüfungen und Schutzmaßnahmen bei Firewalls zu einer Vielzahl an mehrstufigen oder zugeschalteten Schutzmaßnahmen geführt. Einige Architekturen zwingen Sie, zwischen verschiedenen Schutzmaßnahmen zu wählen. Bei Cisco müssen Sie sich entscheiden, ob Sie auf einem bestimmten System Virenschutz oder Intrusion Prevention wollen. Firewalls anderer Anbieter bieten keine Produktintegration an, sodass Sie gezwungen sind, zusätzliche Einzelprodukte anzuschaffen.

Und jedes einzelne Produkt bringt offensichtliche Investitions- und Betriebskosten mit sich - von der Anschaffung über die Wartung bis hin zu den einzelnen Lizenzverlängerungen. Aber diese Produkte bringen auch versteckte Kosten mit sich. So aktiviert z.B. Check Point Schutzmaßnahmen (wie z.B. Signaturen für Intrusion Prevention Systeme (IPS)) global statt über Regeln - eine große Aufgabe, die die Leistung stark beeinträchtigt. Einige Check Point-Anwender ziehen es vor, den Schutz auszuschalten, statt Leistungseinbußen hinzunehmen oder lassen zu, dass Check Point Schutzmaßnahmen deaktiviert, wenn bestimmte Grenzwerte erreicht werden. Aktivitätsspitzen sind genau die Zeitpunkte, an denen man mit einem Angriff rechnen muss.

Wenn zusätzliche Schutzmaßnahmen für denselben Datenverkehr durch einzelne Geräte implementiert werden statt integriert in einer Anwendung, verlangsamt jeder separate Prozess den Durchsatz und macht zusätzliche Hardware für die Verarbeitung erforderlich.

Mit McAfee können Sie sowohl hinsichtlich der Funktionalität als auch der Kosten einen großen Schritt nach vorn machen, denn jedes vorkonfigurierte McAfee Firewall Enterprise V8-System bietet Ihnen konsolidierte Sicherheitsdienste, die mehrere Schutzmaßnahmen vereinen. Ohne zusätzliche Kosten oder Integrationsaufwand können Sie Intrusion Prevention, Malware- und Spyware-Schutz, globale Reputationsbewertung (zur Blockierung von gefährlichen Seiten und bekannten Spammern) und URL-Filterung aktivieren. Diese Schutzmaßnahmen lassen sich über grundsätzliche Anwendungskategorien oder pro Anwendung, Protokoll und Regel steuern. Eine solch flexible, detaillierte Kontrolle ermöglicht Ihnen zu bestimmen, wie Sie Ihren Schutz am besten erhöhen können - etwa für den Datenverkehr von oder nach bestimmten Regionen - und Schutzregeln nach Bedarf zu verfeinern. Die Inline-Prüfung ermöglicht die Ausführung mehrerer Schutzvorgänge mit Hochgeschwindigkeit. Sie müssen keine kritischen Schutzmaßnahmen abschalten, um für eine akzeptable Leistung zu sorgen.

"Der Schlüssel zur Eindämmung der Kosten ist die drastische Reduzierung der Anzahl von erfolgreichen Angriffen, und dies bedeutet eine bessere Verwaltung der Firewall-Regeln. Durch die richtige Investition in Firewall-Lösungen, die mehr Sicherheit bei reduzierten Signaturen bieten, sollten Unternehmen in der Lage sein, die jährlichen Durchschnittskosten für Datenschutzverstöße von über einer Million Dollar drastisch zu senken."

—IDC, *The State of Today's Firewall Management Challenges* (Der Status aktueller Herausforderungen für die Verwaltung von Firewalls), Juni 2009

Regel 3 - Kontrolle sollte einige Momente dauern - nicht Minuten

Die Verwaltung von Richtlinien und Schutzmaßnahmen füllt herkömmlicherweise den ganzen Tag eines Firewall-Administrators aus. Bei separaten Systemen und mehreren Administratoren ist es schwierig, Regeln überhaupt richtig festzulegen, und ihre Wartung ist ein großes Problem. So müssen Anwender z.B. bei Cisco Netzwerkadressübersetzungs (NAT)- und Firewall-Regeln in separaten Fenstern konfigurieren. Jeder einzelne Schritt schafft mehr Arbeit und Fehlerquellen. Mehrere Administratoren bedeuten höhere Komplexität und ein größeres Risiko, dass sich Regeln überschneiden, was die Leistung beeinträchtigt und zu Regeln führt, die nie aktiv ausgeführt werden. Wenn Sie neue Kontrollen für Anwendungen und Anwender hinzufügen, bedeutet das für Sie zusätzliche Optionen und Entscheidungen sowie eventuell viel mehr Arbeit.

McAfee bietet Ihnen hingegen durch seine übersichtliche Ansicht einzelner Regeln alle Informationen, die Sie zur schnellen Erstellung präziser Regeln benötigen, auf einen Blick. So können Sie z.B. für den Datenverkehr über Port 80 oder 443 bestimmte Funktionen beschränken, die Reputationsbewertungen von McAfee TrustedSource™ hinzufügen, die Geolocation-Filterung anwenden und vieles mehr, wobei jede Regel je nach Bedarf auch nur auf bestimmte Anwendergruppen angewandt werden kann.

Alle diese Optionen werden in einem einzigen Fenster angezeigt. Für jede Regel benötigen Sie nur ein paar Mausklicks. So können Sie schnell und leicht alle verfügbaren Kontrolloptionen nutzen. In unserem Fenster zur Übersicht der Interaktion von Regeln können Sie dann Konflikte und Überschneidungen überprüfen. Da unsere Firewall-Lösung natürliche Arbeitsabläufe unterstützt, können Sie in einem einzigen Fenster die Anordnung der Regeln prüfen und jede Regel vollständig ansehen. Wenn Sie eine Übersicht über die Nutzung erhalten oder Fehler beheben möchten, zeigt Ihnen unsere Visualisierung die Aktivitäten nach Anwender, Anwendung und Bedrohung und ermöglicht Ihnen die direkte Navigation, um die entsprechenden Regeln anzupassen.

Regel 4 - Echtzeit-Risikobewertung muss alle Bedrohungswege abdecken und intern entwickelt werden

Neben Kosten und Leistung besteht ein weiterer Nachteil separater Sicherheitslösungen in ihrem mangelnden Schutz. Jedes Tools blockiert seinen winzigen Teil des Problems, ohne von anderen Systemen zu lernen, die neue Bedrohungen und Zero-Day-Schwachstellen aufdecken. Internetkriminelle investieren heute in clevere mehrstufige Bedrohungen über mehrere Wege, die auf diese isolierten

Tools setzen. Conficker, Operation Aurora und Mariposa verfügen allesamt über mehrere Angriffswege. Diesen hinterhältigen und komplexen Angriffen bieten reaktive, einstufige, signaturbasierte Lösungen keine Schwierigkeiten. Auch wenn signaturbasierte Technologien nach wie vor ihren Wert haben - fragen Sie unsere Forscher, die werden Ihnen sagen, dass alte Würmer nicht sterben, sondern sich nur verwandeln - können Signaturen allein keinen angemessenen Schutz mehr bieten.

Warum reichen Signaturen nicht aus? Signaturen dokumentieren bekannte Bedrohungen erst, nachdem sie validiert wurden, und die Verteilung und Installation von Signaturen kann Tage (oder länger) dauern. Viele Anbieter verwenden Schutzmaßnahmen von Drittanbietern, was für zusätzliche Verzögerung sorgt. Check Point arbeitet mit Technologien von Kaspersky, Websense und Commtouch. Wenn Sie Cisco verwenden, erhalten Sie ein wöchentliches Virenschutz-Update über Trend Micro. Das bedeutet, dass Sie neuen Bedrohungen mindestens eine Woche lang ausgesetzt sind. Es ist allgemein bekannt, dass die Signaturqualität von Anbieter zu Anbieter schwankt, je nach Anzahl der Forscher und Forschungsumfang des jeweiligen Anbieters (oder seines Zulieferers). All diese einzelnen Vorgänge sind ineffizient, wofür Sie über Lizenzen und mit lückenhaftem Schutz bezahlen.

Schutzvektor	McAfee Labs™
Malware-Erkennung	Erkennt 50.000 neue Malware-Proben pro Tag
Web-Filterung	35 Millionen Seiten für die Filterung kategorisiert
Spam/Phishing	Analysiert 20 Milliarden Anfragen pro Monat
Netzwerk-IPS	Analysiert 300 Millionen IPS-Angriffe sowie 100 Millionen IP/Port-Reputationsanfragen pro Monat
Web-Reputation	Daten aus 6 Jahren, mit einer heutigen Abdeckung von 80 Millionen Seiten
IP-Adressenreputation	Daten aus 7 Jahren
Dateireputation	Daten aus 20 Jahren

Abbildung 1. Größe und Erfahrung zahlen sich aus, wenn es um globale Bedrohungsanalyse geht.

Durch Gefährdung von Inhalten und Zero-Day-Angriffe stellen unbekannte Bedrohungen heute eine große Gefahr für Unternehmen dar. Solange eine Bedrohung nicht bekannt ist, müssen Tools Risiken aufgrund von Verhalten, Reputation, Absender- und Empfängeradressen sowie des Inhalts selbst (einschließlich getarnter Inhalte, die verschlüsselt und verschleiert wurden) bewerten. Je mehr Datenquellen und Bedrohungsvektoren zur Verfügung stehen, desto präziser und schneller ist die Bewertung. Eine sofortige Bewertung in Echtzeit bietet die besten Chancen, sich vor unbekannten Bedrohungen zu schützen. Diese breit gefächerte Perspektive ist vielleicht der wichtigste Grund, einen Anbieter zu wählen, der die gesamte Bedrohungslage überwacht und analysiert, ohne wichtige Vorgänge an kleine Unternehmen auszulagern.

Die McAfee Firewall Enterprise-Appliance bietet Ihnen präventiven Schutz durch globale Bedrohungsanalyse in Echtzeit. Über 100 Millionen Sensoren und automatische Verfahren korrelieren Bedrohungen über 15 verschiedene Host-, Netzwerk-, Web-, E-Mail- und Datenverlust-Vektoren. Wir gleichen ebenfalls neue Inhalte und Aktivitäten mit einer zentralen Datenbank für Messaging- und Kommunikationsverhalten, einschließlich Reputation, Volumen und Trends für E-Mail, Internet-Datenverkehr und Malware ab. Dieses breit gefächerte, ineinandergreifende System, das seit über 20 Jahren ständig ausgebaut wird, ermöglicht es uns, Risiken zu erkennen und Sie zu schützen, bevor eine Signatur für eine bestimmte Bedrohung vorliegt. Während andere sich auf ein einziges Protokoll oder einen einzigen Bedrohungsvektor stützen und die Reputation auf ein einziges Element wie Spam eingrenzen, berücksichtigt McAfee sämtliche Protokolle und Bedrohungstrends für die umfassendste Übersicht und den effektivsten Schutz.

Regel 5 - Ihre Firewall sollte Sie nicht anfälliger machen

Mehrstufige, gezielte Angriffe beinhalten verschiedene Malware-Arten, die sich gegen jede potenzielle Schwachstelle eines Systems richten. Ihre Sicherheitsprodukte sollten zur Lösung dieses Problems beitragen und nicht selbst Schwachstellen oder einen Katalysator für Notfall-Patches darstellen. Jedes Mal, wenn Sie einen Patch installieren müssen, laufen Sie Gefahr, den Datenverkehr zu unterbrechen oder die Systemstabilität aufs Spiel zu setzen.

Die McAfee Firewall Enterprise-Appliance, die auf der robusten McAfee SecureOS®-Plattform basiert, die vor zwei Jahrzehnten für den US-Nachrichtendienst NSA entwickelt wurde, verfügt über einen unerreichten CERT-Rekord mit null Schwachstellen in unserem Secure-Betriebssystem, null Verstößen und null Notfall-Patches.

Regel 6 - Migrieren Sie Ihre Regeln, anstatt von vorn anzufangen

Die Erstellung und Wartung von Firewall-Regeln ist der teuerste Aspekt des Besitzes einer Firewall. Wenn Sie eine Migration in Betracht ziehen, sollten Sie sich auf automatische Migrations-Tools und spezifische Dienste verlassen können, die Ihre alten Regeln in Ihre neue Umgebung importieren.

McAfee hilft Forbes Global 2000-Unternehmen und Regierungsbehörden seit Jahren bei der Migration ihrer Regeln zu unserer einfachen, zentralen Regelumgebung. Unser Tool für die Migration von Regeln übernimmt in der Regel 90 Prozent aller Konfigurationsdaten, einschließlich Objektdaten, Diensten und vorhandener Regelsätze. Sie können Ihre Konfiguration auch optimieren, indem Sie sich entscheiden, Objekte oder Dienste, die von den Regeln zurzeit nicht genutzt werden, nicht zu migrieren.

Unser spezielles Professional Service-Team für Netzwerksicherheit bietet nützliche Programme, um Ihnen den Migrationsprozess zu erleichtern. Das Team kann auf das Tool zugreifen, um Regeln von Cisco PIX-, Cisco ASA- und Check Point-Firewalls sicher zu migrieren. Tools für Juniper- und Fortinet-Lösungen werden demnächst zur Verfügung stehen.

Regel 7 - Sie verdienen Integration und Flexibilität - bis hin zum Support

Sie können Ihre Zeit besser nutzen, als Integrator zu spielen oder sich Abhilfemaßnahmen für schlecht entwickelte und beschränkte Produkte auszudenken. Heute ist jedes Unternehmen verteilt, und jedes Netzwerk ist einzigartig. Diese Tatsachen sollten bei der Sicherheit als selbstverständlich vorausgesetzt werden. Kluge Anbieter wissen das und machen es Ihnen leicht, guten Schutz schnell zu implementieren, und unterstützen Sie, wo und wann es nötig ist - rund um die Uhr an 7 Tagen die Woche.

McAfee Firewall-Lösungen sind in einer Vielzahl von kostengünstigen, robusten Konfigurationen erhältlich, die sich für Zweigstellen genauso eignen wie für anspruchsvolle Unternehmen mit einem Durchsatz von 12 GB/s. Sie können eine speziell entwickelte Appliance wählen - eine physische Multi-Firewall-Appliance mit 4, 8, 16 oder 32 Firewalls in einem kleinen 2U-Gehäuse oder eine virtuelle Firewall-Appliance für VMware ESX. Wir bieten ebenfalls McAfee Firewall Enterprise for Riverbed an, das auf mehreren Modellen der Riverbed Steelhead-Appliances installiert werden kann, und die Riverbed Services-Plattform nutzen, sowie auf widerstandsfähigen Appliances, die widrigen Umgebungsbedingungen standhalten. Das sind Tools, mit denen Sie arbeiten können.

Und diese Flexibilität ist obendrein kostengünstig. Im Gegensatz zu Cisco müssen Sie bei McAfee keine zusätzlichen Mittel für mehrere Appliances und Sicherheitsmodule ausgeben. Im Gegensatz zu Check Point haben Sie mit McAfee nicht die Komplexität und die Kosten für die Konfiguration mehrerer Einzellösungen, die auf Hardware verschiedener Anbieter installiert sind.

Da eine zentrale Verwaltung unerlässlich für die Effizienz (und das Compliance-Reporting) ist, können Sie in derselben Management-Umgebung Appliances für Großunternehmen mit SMB-Systemen mischen und aufeinander abstimmen. Der enthaltene McAfee Firewall Reporter überwacht zentral mehrere Systeme und aggregiert Protokolldaten mehrerer Geräte. Wir bieten über 500 Berichtsvorlagen ohne Aufpreis - darunter sicher auch eine, die für Ihr Unternehmen und die für Sie geltenden Vorschriften passt.

Wenn Sie Hilfe benötigen oder Fragen haben, steht Ihnen unser Support-Team rund um die Uhr an 7 Tagen die Woche für schnelle Antwort zur Verfügung - in Minuten, nicht Stunden. Wir beschränken unseren Service nicht auf Bürozeiten oder auf einen Kontinent - unsere Kunden, Forscher und Support-Mitarbeiter finden sich rund um den Globus.

Regel 8 - Integration bietet optimale Sicherheit

Wir haben die Vorteile mehrerer Schutzmaßnahmen in einer Firewall hinsichtlich Einsparungen und Einfachheit erwähnt. Da die Firewall nur ein Element Ihrer Sicherheits- und IT-Kontrollen ist, sollten Sie auch über die Firewall hinaus auf Einfachheit achten. Was ist mit anderen Netzwerksicherheitsprodukten, Bereinigungs-Tools, der Verwaltung von Sicherheitsinformationen und ähnlichen Vorgängen?
Was ist mit dem Endgeräteschutz, dem Schutz vor Datenverlust und dem Risiko-Management? Je besser Ihre Systeme kommunizieren, desto leichter wird Ihre Arbeit. Und die Kommunikation von Sicherheitslösungen ist unsere Spezialität.

McAfee ist das führende auf Sicherheit spezialisierte Unternehmen. Unsere Firewall wird von über 15.000 Kunden eingesetzt und ist mit einer Vielzahl von anderen Netzwerksicherheitsfunktionen verbunden, einschließlich Web- und E-Mail-Gateways, Netzwerkzugriffssteuerung, Network User Behavior Analysis, Network Threat Response und Intrusion Prevention-Systemen. Wir sind seit langem als führender Anbieter in der Endgerätesicherheit, dem mobilen Datenschutz, der Internetsicherheit und weiteren Bereichen anerkannt. Dieses breit gefächerte Produktangebot ist über die offene, zentrale Verwaltungsplattform McAfee ePolicy Orchestrator® (McAfee ePO™) verbunden, damit Sie jeden Schutz, den Sie ausbringen, optimal nutzen können. Und auch über 90 McAfee Security Innovation Alliance-Partner sind über die McAfee ePO-Verwaltungsplattform verbunden, wodurch andere Sicherheits- und IT-Vorgänge kostengünstiger und einfacher werden.

Das Web 2.0 ist ein neues Spiel. Spielen Sie nach den neuen Regeln.

Wenn Sie die Migration auf einen umfassenderen Schutz in Betracht ziehen, sollten Sie sich von diesen Regeln leiten lassen, um sicherzustellen, dass Ihre neue Firewall den hartnäckigen Bedrohungen von heute und den komplexen Web 2.0-Anwendungen gewachsen ist.

1. Detaillierte Kontrolle erfordert auf die Interaktionen von Anwendern und Web 2.0-Anwendungen zugeschnittene Transparenz und Durchsetzung.
2. Mehrstufiger Bedrohungsschutz sollte keine Extrakosten bedeuten.
3. Kontrolle sollte einige Momente dauern - nicht Minuten.
4. Echtzeit-Risikobewertung muss alle Bedrohungswege abdecken und intern entwickelt werden.
5. Ihre Firewall sollte Sie nicht anfälliger machen.
6. Migrieren Sie Ihre Regeln, anstatt von vorn anzufangen.
7. Sie verdienen Integration und Flexibilität - bis hin zum Support.
8. Integration bietet optimale Sicherheit.

Mit der McAfee Firewall Enterprise-Appliance können Sie Port- und Protokollkontrolle durch effektiven und präzisen Schutz ersetzen. Ihr Unternehmen profitiert von besserem Zugang zu Web 2.0-Anwendungen und wird geschützt durch identitäts- und anwendungsbewusste Kontrollen, globale Bedrohungsanalyse und mehrere Sicherheitsdienste, die nahtlos zusammenarbeiten, um Ihnen Schutz zu bieten.

Wir erleichtern Ihnen den Prozess der Migration durch unser Testprogramm mit einer virtuellen Firewall, Migrations-Tools und speziellen Professional Services. Eliminieren sie blinde Flecke und schützen Sie Ihr Unternehmen vor den hartnäckigen Bedrohungen von heute, mit weniger Notfall-Patches und Aufwand. Erfahren Sie mehr unter www.mcafee.com/de und verbessern Sie Ihren Schutz mit V8 unter www.mcafee.com/virtualtestdrive.

McAfee GmbH
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.mcafee.com/de

Die hier enthaltenen Informationen werden McAfee-Kunden ausschließlich für Fort- und Weiterbildungszwecke bereitgestellt. Die hier enthaltenen Informationen können ohne Vorankündigung geändert werden. Ihre Bereitstellung erfolgt in der vorliegenden Form ohne Übernahme einer Garantie oder Gewährleistung im Hinblick auf ihre Richtigkeit oder Anwendbarkeit für eine bestimmte Situation oder einen bestimmten Umstand. Die in diesem Dokument enthaltenen Produktpläne, Spezifikationen und Beschreibungen dienen lediglich Informationszwecken, können sich jederzeit ohne vorherige Ankündigung ändern und schließen alle ausdrücklichen oder stillschweigenden Garantien aus.

McAfee, das McAfee-Logo, McAfee SecureOS, McAfee TrustedSource, McAfee Labs, McAfee ePolicy Orchestrator und McAfee ePO sind eingetragene Marken oder Marken von McAfee, Inc. oder seinen Tochterunternehmen in den USA und/oder anderen Ländern. Alle anderen Namen und Marken sind alleiniges Eigentum der jeweiligen Besitzer. Copyright © 2010 McAfee, Inc.
8816brf_nts_nextgen-firewall_0310