Schutz der privaten Cloud

Schutz für Ihre private Cloud dank integriertem Sicherheitsansatz

Bereitstellungen in der privaten Cloud sind so konzipiert, dass sie dynamische Workloads in einer stark virtualisierten Infrastruktur ausführen und skalieren. Dadurch entstehen jedoch auch neue Sicherheitsprobleme, für die herkömmliche statische Sicherheitslösungen nicht ausgelegt sind. Als Reaktion darauf entwickelte McAfee hochentwickelte Technologien sowie ein integriertes Bereitstellungsmodell, das maximalen Schutz für private Cloud-Instanzen gewährleistet. Dazu gehören Software-definierte Rechenzentren (SDDCs) und Mehrmandantenumgebungen. Das Ergebnis: Unternehmen und Anbieter verwalteter Services können von geschäftlicher Flexibilität sowie Kosteneinsparungen durch private Clouds profitieren und gleichzeitig ihr geistiges Eigentum sowie ihre Kundendaten schützen. McAfee®-Lösungen schützen private Clouds vor internen sowie externen Bedrohungen, darunter gezielte Angriffe und Malware, und gewährleisten dabei die Einhaltung von Branchen- sowie gesetzlichen Vorschriften.

Die Herausforderungen bei der Absicherung für private Clouds

Unternehmen aller Größen setzen immer stärker auf private Clouds, um ihre Kosten zu senken und die Flexibilität zu erhöhen, ohne dabei die Kontrolle der IT-Abteilung und die Sicherheit zu beeinträchtigen. Eine Umfrage zeigte, dass mehr als 70 Prozent aller Unternehmen private Cloud-Modelle nutzen, implementieren oder in Betracht ziehen.[1] Private Clouds bieten mehr Kontrolle als öffentliche Clouds sowie im Vergleich zu herkömmlichen Rechenzentren weitere Vorteile. Gleichzeitig bringen private Clouds eigene Sicherheitsprobleme mit sich, die für maximalen Schutz und Compliance berücksichtigt werden müssen.

Eine große Herausforderung ist der fehlende Überblick über den gesamten Datenverkehr, sodass die Erkennung gezielter Angriffe erschwert wird. In einer stark virtualisierten privaten Cloud-Umgebung erfolgt der Großteil des Datenverkehrs innerhalb des Netzwerks zwischen den virtuellen Maschinen (VMs). Herkömmliche Sicherheitseinzellösungen sind für solche virtuellen Rechenzentrum-Umgebungen nicht ausgelegt, sondern decken lediglich den an der Netzwerkperipherie ein- und ausgehenden Datenverkehr ab. Diese herkömmlichen Lösungen erlauben keinen Überblick über Datenverkehr, der innerhalb des Rechenzentrums erfolgt, sodass eine Schutzlücke entsteht. Wenn Lösungen den internen Datenverkehr nicht untersuchen, können sich Bedrohungen unbemerkt innerhalb des Rechenzentrums ausbreiten.

Eine weitere Herausforderung besteht bei privaten Clouds in der Bereitstellung von Sicherheitsmaßnahmen, die mit der Geschwindigkeit der Cloud Schritt halten und gleichzeitig die Einhaltung von Vorschriften unterstützen können. Beim Wechsel der IT zu einem dynamischeren und flexibleren Verarbeitungsmodell muss die Netzwerksicherheit ebenso anpassbar sein wie die Cloud. Zusätzlich muss die IT Vorschriften wie PCI DSS (Payment Card Industry Data Security Standard) und HIPAA (Health Insurance Portability and Accountability Act) einhalten. Leider können einzelne Sicherheitslösungen nicht skaliert und daher nicht automatisch mit virtualisierten Workloads migriert werden.

Die letzte Herausforderung besteht in der eingeschränkten Möglichkeit zur vertrauenswürdigen Verwaltung von Sicherheitsrichtlinien und Gewährleistung, dass starke SLAs für geschäftliche Anforderungen eingehalten werden können. Das IT-Team verfügt häufig nicht über genügend Mitarbeiter, um die Sicherheit für die gesamte private Cloud effektiv und effizient zu verwalten. Zudem verwenden die Mitarbeiter meist herkömmliche Tools und tauschen Bedrohungsdaten selten oder gar nicht sowie nicht zeitnah untereinander aus.

Die Ziele bei der Absicherung privater Clouds

Sie müssen Ihr Unternehmen vor externen Angriffen und Insider-Bedrohungen schützen. Das bedeutet, dass alle Lücken in der privaten Cloud-Sicherheit geschlossen werden müssen. Bei externen Bedrohungen sollen eingehende Angriffe bereits an der Peripherie erkannt und blockiert werden. Das gleiche gilt für die Kommunikation mit Befehls- und Steuerungs-Servern.

Bei internen Bedrohungen müssen Sie Malware auf virtuellen Servern innerhalb des Rechenzentrums erkennen sowie entfernen und Angriffe erkennen sowie blockieren, die von Benutzerkonten mit erhöhten Berechtigungen stammen.

Um diese Ziele zu erreichen, benötigen Sie für die gesamte private Cloud vollständige Sicherheitstransparenz, dynamischen Schutz sowie effiziente Richtlinienverwaltung. Die vollständige Sicherheitstransparenz aller privaten Cloud-Workloads ist für den Schutz Ihres Unternehmens unerlässlich, da Sie nur das schützen können, was Sie sehen. Der dynamische Schutz bietet die Möglichkeit, eine private Cloud-Umgebung mit Sicherheitsmaßnahmen zu schützen, die sich an die sich stets verändernde Umgebung anpassen, in der virtuelle Maschinen immer wieder auf unterschiedliche Hosts verschoben werden. Nicht zuletzt benötigen Sie eine einfache Sicherheitsverwaltung, mit der Ihre vorhandenen Mitarbeiter effizient die SLAs einhalten und den Schutz der Geschäftsabläufe gewährleisten können.

Das koordinierte McAfee-Modell

McAfee bietet eine der umfassendsten und am vollständigsten integrierten Sicherheitslösungen, mit der Unternehmen die Compliance-Vorschriften für stark virtualisierte private Cloud- oder SDDC-Umgebungen effizient und effektiv gewährleisten können, ohne Flexibilität, operative Effizienz und Kosteneinsparungen zu gefährden.

Mit einer Kombination aus nahtlos zusammenarbeitenden Produkten, die den spezifischen Herausforderungen stark virtualisierter privater Cloud-Bereitstellungen und SDDCs Rechnung tragen, bieten wir bestmöglichen Schutz vor hochentwickelten gezielten Angriffen. Hier ist ein Beispiel dafür, wie das integrierte McAfee-Modell Bedrohungen an der Peripherie des Rechenzentrums abwehrt.

Abwehr neu aufkommender Bedrohungen

Die Erkennung und Eindämmung eines gezielten Angriffs läuft in einer privaten Cloud anders ab. Eine Datei wird an der Peripherie von McAfee Virtual Network Security Platform, einem virtuellen Inline-System für Eindringungsschutz (IPS) untersucht. Dabei wird sie mithilfe zahlreicher signaturloser Module geprüft, die entsprechend der Richtlinie für hochentwickelte Malware aktiviert sind. Wenn die Datei verdächtig ist, ihr Status jedoch nicht mit Sicherheit bestimmt werden kann, wird sie von der McAfee Virtual Network Security Platform an McAfee Advanced Threat Defense gesendet, wo sie gescannt und ihre Reputation in McAfee Threat Intelligence Exchange veröffentlicht wird. Diese Information wird an McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) auf dem Server weitergegeben. Von dort werden Maßnahmen ergriffen und die Datei gelöscht.

Maximaler Schutz und Compliance mit McAfee-Lösungen

Folgende McAfee-Produkte bilden die Grundlage für die Transparenz, den dynamischen Schutz und die effiziente Richtlinienverwaltung:

McAfee Virtual Network Security Platform

Dieses IPS mit vollem Funktionsumfang wurde speziell für die Anforderungen virtueller Umgebungen konzipiert. Mit dieser virtuellen Instanz der McAfee Network Security Platform können Sie schnell virtuelle Sensoren bereitstellen und damit verschiedene Netzwerkarchitekturen schützen. Durch die enge Vernetzung mit anderen Technologien wie Intel Open Security Controller und McAfee Advanced Threat Defense gestattet McAfee Virtual Network Security Platform die umgehende Ergreifung von Maßnahmen, wenn eine Datei als böswillig eingestuft wird. Durch den koordinierten Sicherheitsansatz können Sie ohne erneute Analyse sofort weitere Kopien dieser Datei blockieren, sobald sie in das Netzwerk gelangen. Zudem kann die Lösung einen infizierten Host isolieren und so einen Übergriff böswilliger Aktivitäten im Netzwerk verhindern.

McAfee MOVE AntiVirus

McAfee MOVE AntiVirus sorgt für einen optimierten Malware-Schutz für virtualisierte Desktop-Rechner und Server. Zur Vermeidung von Scan-Engpässen und Verzögerungen lagert die Lösung Scans, Konfigurationen und DAT-Aktualisierungen aus den einzelnen Gast-Abbildern in die gesicherte virtuelle Appliance bzw. auf den Offload-Scan-Server aus. Dank eines globalen Caches gescannter Dateien stellt McAfee MOVE AntiVirus sicher, dass bereits geprüfte und als sicher bestätigte Dateien bei späteren Zugriffen durch VMs nicht erneut geprüft werden.

McAfee Threat Intelligence Exchange

McAfee Threat Intelligence Exchange ermöglicht die adaptive und kollaborative Bedrohungserkennung sowie Reaktion, sodass Unternehmen neue und gezielte Angriffe dank hervorragender Transparenz und Kontrolle abwehren können. Die Lösung kombiniert wichtige globale Bedrohungsdaten mit lokal erfassten Informationen und macht diese Erkenntnisse in Echtzeit für alle Server-, Gateway-, Netzwerk- sowie Rechenzentrum-Sicherheitslösungen verfügbar. Durch den sofortigen Austausch der Informationen können Ihre Sicherheitslösungen als eine Einheit agieren, die basierend auf gemeinsam erfassten Daten Maßnahmen ergreift. Durch diesen adaptiven Bedrohungsschutz können Sie die Lücke zwischen Angriff und Eindämmung auf Millisekunden verkleinern – im Vergleich zu Tagen, Wochen oder gar Monaten bei herkömmlichen Sicherheitsmodellen.

McAfee Advanced Threat Defense

Mit McAfee Advanced Threat Defense können Sie hochentwickelte gezielte Angriffe erkennen und basierend auf Bedrohungsinformationen Aktionen und Schutzmaßnahmen starten. Im Gegensatz zu

gewöhnlichen Sandboxes bietet McAfee Advanced Threat Defense weitere Analysemöglichkeiten, die die Erkennung verbessern und verschleierte Bedrohungen aufdecken. Dabei setzt die Lösung zur Erkennung von Zero-Day-Malware auf einen innovativen, mehrstufigen Ansatz. Hierfür verbindet sie Schutzmaßnahmen mit geringem Ressourcenverbrauch – Virenschutzsignaturen, Reputationsdaten und Echtzeitemulation – mit gründlicher statischer Code-Überprüfung sowie dynamischer Analyse (Sandbox), um das tatsächliche Verhalten von Malware zu analysieren. Um auch Sandbox-sensitive Bedrohungen zu erkennen, enthält McAfee Advanced Threat Defense umfassende Entpackfunktionen, die Verschleierungstechniken aufheben und so den ausführbaren Original-Code offenlegen. Die Lösung bietet statische Code-Analysen, um nicht nur grundlegende Dateiattribute zu untersuchen, sondern auch Anomalien zu erfassen. Dabei werden alle Attribute und Anweisungen auf das resultierende Verhalten untersucht.

McAfee ePolicy Orchestrator® (McAfee ePO™)

Die Software McAfee ePO bietet für alle Cloud-Bereitstellungsvarianten integrierte Sicherheits- und zentrale Richtlinienverwaltung. Durch die Erkennung von und die Übersicht über alle VMs wird die Absicherung von Clouds vereinfacht. Administratoren können Hypervisor-zu-VM-Beziehungen sowie den Sicherheits- und Energiestatus beinahe in Echtzeit überwachen.

Erreichung Ihrer Schutz- und Compliance-Ziele für die private Cloud:

Mit dem integrierten McAfee-Portfolio zum Schutz Ihrer privaten Clouds können Sie Ihre wichtigsten Sicherheitsziele erreichen:

- Sie erhalten einen Überblick über die zu schützenden Ressourcen sowie hochentwickelte Bedrohungen. Dadurch können Sie nicht nur die Sicherheit der privaten Clouds verbessern, sondern auch die darin gespeicherten Kundendaten und das geistige Eigentum schützen.
- Der integrierte dynamische Schutz ist ebenso flexibel wie die private Cloud-Umgebung. Dadurch können Sie hochentwickelte Bedrohungen abwehren, die Compliance gewährleisten und den Datenverkehr innerhalb der privaten Cloud-Umgebung kontrollieren. Dadurch lässt sich die Einhaltung der Branchen- und gesetzlichen Compliance-Vorschriften erreichen und nachweisen.
- Dank der erweiterten und automatisierten Richtlinienverwaltung für die gesamte Infrastruktur können Sie Sicherheitsrichtlinien für private Clouds effizient bereitstellen. Die Kosten für Sicherheit, Bedrohungsbehebung und Wartung im Software-definierten Rechenzentrum lassen sich dadurch senken. Gleichzeitig wird die Zeit zur Erkennung und Behebung externer sowie interner Bedrohungen und Angriffe verkürzt.

Wichtige Vorteile von McAfee

- **Vollständiges Portfolio:** Nutzen Sie ein vollständiges Portfolio aus Lösungen, die nahtlos zusammenarbeiten und die Sicherheitsherausforderungen von privaten Cloud-Umgebungen lösen können.
- **Dynamischer Schutz und Behebung:** Dank IPS-Diensten der nächsten Generation haben Sie die Möglichkeit, Ihre private Cloud dynamisch zu schützen, Bedrohungen zu verwalten sowie zu beheben und die Compliance zu gewährleisten.
- **Abwehr externer Angriffe:** McAfee-Lösungen erkennen sowie blockieren Angriffe, Malware und Bedrohungen an der SDDC-Peripherie sowie eingehende Kommunikation mit Befehls- und Steuerungs-Servern an der Peripherie.
- **Abwehr von Bedrohungen durch Insider:** Sie können Malware auf virtuellen Servern innerhalb des SDDC aufspüren sowie entfernen und Angriffe erkennen und blockieren, die von Benutzerkonten mit erhöhten Berechtigungen stammen.
- **Bessere Einhaltung von Compliance-Vorschriften:** Erreichen Sie die Einhaltung der Branchen- und gesetzlichen Compliance-Vorschriften, und weisen Sie dies nach.
- **Schnellere Reaktionen:** Dank des adaptiven Bedrohungsschutzes wird die Zeit zur Erkennung und Behebung externer sowie interner Bedrohungen und Angriffe verkürzt.
- **Geringere Kosten:** Senken Sie die Kosten für Sicherheit, Bedrohungsbehebung und Wartung im SDDC.
- **Verbesserte Transparenz:** Erfahren Sie sofort, wenn hochentwickelte gezielte Angriffe in Ihrem Unternehmen stattfinden.

Weitere Informationen

Weitere Informationen erhalten Sie unter **www.mcafee.com/de/solutions/secure-cloud/index.aspx**.

1. „State of the Market: Enterprise Cloud 2016“ (Bericht zur Marktsituation: Die Unternehmens-Cloud 2016), Verizon, November 2015.

McAfee
Together is power.

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