McAfee Web Gateway Cloud Service

Cloud-basierte Web-Sicherheit mit allgegenwärtigem Schutz

Die Abwehr raffinierter Web-Bedrohungen erfordert hochentwickelte Technologien, muss jedoch nicht zwangsläufig mehr Kosten und Komplexität bedeuten. Durch die Implementierung von Web-Sicherheit über die Cloud erzielen Sicherheitsteams denselben erweiterten Bedrohungsschutz wie mit lokalen Appliances, sparen allerdings Hardware-Kosten und Wartungsressourcen. Da der Web-Zugriff zunehmend außerhalb der Netzwerkperipherie stattfindet, wird die Cloud zum dauerhaften Kontaktpunkt für mobile Geräte und Benutzer. Statt Sicherheitskonzepte für Datenverkehr zu einem einzelnen Standort zu entwickeln, ist es effektiver, den Schutz vom jeweiligen Endgerät ausgehend aufzubauen. Die Anbindung von Endgeräten und sogar kompletten Standorten an die Cloud bietet allgegenwärtigen Schutz innerhalb der neuen Peripherie, die nicht per durch physische Grenzen begrenzt wird.

Kosteneffektiver, allgegenwärtiger Schutz

Die Verwaltung lokaler Web-Sicherheits-Appliances ist teuer und belastet die ohnehin schon angespannten Ressourcen der Sicherheitsteams zusätzlich.
Die Implementierung der Web-Sicherheit als Cloud-Dienst kann die Gesamtbetriebskosten senken, da keine Hardware-Appliances mehr angeschafft, betrieben und gewartet werden müssen. Alle Ressourcen, die zuvor in die Wartung der Appliances flossen (z. B. für Software-Upgrades und Patches), können nun auf strategischere Initiativen innerhalb der IT oder IT-Sicherheit gerichtet werden.

Appliances und Cloud-Dienste können zusammen in einer hybriden Implementierung genutzt werden. Die meisten Unternehmen entscheiden sich für dieses Modell, da sie so die Zuständigkeit für und Kontrolle über die Appliances im Netzwerk behalten und gleichzeitig den Cloud-basierten Schutz auf kleine externe Niederlassungen und mobile Benutzer ausdehnen können.

IT-Teams, die den Web-Datenverkehr externer Niederlassungen über MPLS-Schaltungen (MultiProtocol Label Switching) leiten (Backhauling) und durch eine Web-Gateway-Appliance im Netzwerk filtern lassen, profitieren unmittelbar von Cloud-

Wichtige Vorteile

- Kosteneffektivste Methode für die Implementierung von Web-Sicherheit – keine lokale Hard- oder Software erforderlich
- Mehr als nur Basisschutz – Verhaltensemulation wehrt Zero-Day-Malware während der Verarbeitung des Datenverkehrs innerhalb von Millisekunden ab
- Schutz für Benutzer auch außerhalb des Netzwerks – Cloud-Übertragung hebt Grenzen traditioneller Netzwerke auf
- Unerreichte Verwaltungseffizienz durch die McAfee® ePO™ Cloud-Plattform als einheitliche Verwaltungskonsole für alle McAfee-Cloud-Dienste
- Native Integration und nur eine Richtlinie, die über McAfee Cloud Threat Detection, McAfee Cloud Data Protection und McAfee Cloud Visibility – Community Edition hinweg verwendet wird

basierter Web-Sicherheit. Backhauling ist teuer und erhöht die Komplexität im Netzwerk. Alternativ können externe Niederlassungen ihren Datenverkehr für den Schutz direkt in die Cloud leiten. Damit können MPLS-Schaltungen minimiert und die Netzwerkarchitektur vereinfacht werden.

Zudem entfällt die Beschränkung, dass Mitarbeiter nur innerhalb der Netzwerkperipherie Web-Zugriff haben und Benutzer sowie Geräte außerhalb des Netzwerks ohne Schutz und für die IT nicht sichtbar sind. Die Verlagerung der Web-Sicherheit in die Cloud invertiert diese Peripherie. Web-Datenverkehr von Benutzern und Geräten außerhalb des Netzwerks kann automatisch vom Endgerät in die Cloud geleitet werden. Dies gewährleistet Benutzern eine sichere Verbindung bei der Arbeit von zu Hause, am Flughafen, im Café oder an anderen netzwerkexternen Standorten. Das Netzwerk ist nicht mehr auf den Datenverkehr innerhalb physikalischer Grenzen beschränkt, sondern wird stattdessen vom jeweiligen Endgerät aus aufgebaut.

Globale Hochleistungsarchitektur

McAfee® Web Gateway Cloud Service wurde für Unternehmen konzipiert. Viele Firmen erzielen damit bessere Leistungswerte als mit ihrer aktuellen lokalen Lösung. Wenn beispielsweise lokale Kapazitäten ausgebaut werden müssen, ist es Aufgabe der IT-Abteilung, eine neue Appliance zu beschaffen und bereitzustellen. Dies kann Tage oder gar Wochen dauern. Aufgrund der elastischen Struktur unserer Cloud, die in den Service integriert wurde, dauern Kapazitätserweiterungen nur etwa 15 Minuten.

Wenn eine lokale Appliance ausfällt und repariert werden muss, kann der Internetzugriff ausfallen und die Sicherheitslage gefährdet sein, falls ein Fail-Open über das Web zugelassen wurde. Bei einem Fehler in einem unserer Rechenzentren leitet unser Cloud-Dienst den gesamten Web-Datenverkehr zum schnellsten, nächstgelegenen Rechenzentrum um, sodass der Betrieb weiterhin gewährleistet ist.

Darüber hinaus kann unsere Cloud-Dienst-Architektur als „Peer“ mit dem Internet-Backbone an den größten Internetknoten (IXPs) der Welt kommunizieren. So entfallen Routing-Hops vermittelnder Internet-dienstanbieter (ISPs), die die Latenz der Verbindung erhöhen würden. Durch die geringe Anzahl der Hops bei der Verbindung zu beliebten Inhaltsanbietern wie Microsoft Office 365 und Google erhalten die Benutzer mit unserem Cloud-Dienst schnellere Verbindungen als über das offene Internet.

McAfee Web Gateway Cloud Service ist global. Web-Inhalt kann in der jeweiligen Landessprache bereitgestellt werden. So erhält ein Benutzer beispielsweise an jedem Zugriffsort lokale Google-Suchergebnisse. Einen Überblick über die aktuellen Standorte und den Status der Rechenzentren, in denen Web-Datenverkehr verarbeitet wird, finden Sie unter **https://trust.mcafee.com**.

Abwehr raffinierter Bedrohungen

Sicherheitsteams sind bei extrem raffinierter Malware und gezielten Angriffen, die herkömmliche Abwehr-maßnahmen umgehen, häufig im Nachteil. Folgen sind eine starke Bindung von Ressourcen und ständige

- Bewährte Architektur: McAfee Web Gateway Cloud Service ist als Mehrmandantenversion von McAfee Web Gateway konzipiert, der lokalen Appliance, der Unternehmen auf der ganzen Welt vertrauen

„Feuerwehreinsätze“, um bei der Behebung der Endgeräteprobleme Schritt zu halten. Im Gegensatz zur herkömmlichen URL-Filterung und zu signaturbasierten Ansätzen bei der Abwehr von Web-Bedrohungen schützt McAfee Web Gateway Cloud Service Endgeräte mittels Inline-Emulation von Dateien, JavaScript und HTML vor Zero-Day- und dateiloser Malware. Zero-Day-Malware wird zum Beispiel bereits bekämpft, bevor sie den Benutzer erreicht. Zudem verbessert sich die Blockierungsrate um etwa 20 Prozent im Vergleich zur URL-Filterung und zu signaturbasierten Lösungen. Das Sicherheitskontrollzentrum profitiert von geringeren Kosten und flexibleren Ressourcen, weil die Gesamtzahl der Malware-Vorfälle sinkt. Alle noch verbleibenden verdächtigen Dateien können an McAfee Cloud Threat Detection gesendet werden. Diese Cloud-basierte Lösung zur erweiterten Bedrohungsanalyse ist als kostenloser Dienst verfügbar, der nativ bereits in McAfee Web Gateway Cloud Service enthalten ist.

Web-Bedrohungen werden oft im verschlüsselten Datenverkehr transportiert, um sich vor Abwehrmechanismen der Web-Sicherheitsmaßnahmen zu verstecken. Nahezu alle Cloud-Anwendungen, wie Cloud-Speicher oder soziale Medien, nutzen standardmäßig verschlüsselten Datenverkehr. McAfee Web Gateway Cloud Service kann HTTPS-verschlüsselten Datenverkehr vollständig entschlüsseln und inspizieren, um Malware abzuwehren und Cloud-Anwendungen in verschlüsselten Kanälen sichtbar zu machen.

Die meisten IT-Teams haben Probleme, die Verbreitung von Cloud-Anwendungen zu kontrollieren. Dies gilt insbesondere für die „Schatten-IT“ sowie für Risiken durch Dienste, die von Benutzern gewählt werden. Dank des vollständigen Überblicks über den gesamten Datenverkehr (einschließlich HTTPS) können alle Zugriffe auf Cloud-Anwendungen aufgedeckt werden. McAfee Web Gateway Cloud Service integriert sich nativ in McAfee Cloud Visibility – Community Edition, unseren kostenlosen Dienst für McAfee-Kunden mit einer McAfee-Lösung zum Schutz vor Datenverlusten oder einer unserer Verschlüsselungs- oder Web-Schutzlösungen. Hierfür erhalten Sie ein unkompliziertes Dashboard mit einer Übersicht über Cloud-Anwendungszugriffe, Risikostufen und Datenklassifizierungen. Nach der Aktivierung werden die Datenverkehrdaten automatisch und ohne zusätzliches Setup vom Dienst erfasst. Dank der Automatisierung der Übersichtsfunktionen können Sie sich auf den tatsächlichen Schutz der Daten konzentrieren, die in die Cloud übertragen werden, und so Sie das Risiko für Ihr Unternehmen reduzieren. McAfee Cloud Data Protection ist der nächste Schritt für mehr Kontrolle über Ihre Daten. Dies wird mithilfe von APIs (Application Programming Interface) zur Integration verbreiteter Cloud-Anwendungen ermöglicht. McAfee Cloud Data Protection ist ein weiterer kostenloser Dienst, der nativ in McAfee Web Gateway Cloud Service enthalten ist und über diese Lösung verwaltet wird.

Auch Cloud-Anwendungen, insbesondere Cloud-Speicher, werden zunehmend als Übertragungsmechanismus für Malware genutzt. Die Kenntnis der Anwendungen, die Malware übertragen haben, ermöglicht fundiertere Entscheidungen bei der Richtliniendefinition. Durch den umfassenden Überblick über die aufgerufenen Cloud-Dienste

Wo finde ich McAfee Web Gateway Cloud Service?

Unter **https://trust.mcafee.com** erhalten Sie Live-Updates und einen Überblick über die Standorte unserer Rechenzentren, Verfügbarkeitsstatus und mehr.

zur Risikominimierung können Kontrollen für tausende Cloud-Anwendungen implementiert werden, die zum Beispiel Uploads, Nachrichtenaustausch oder komplette Anwendungen blockieren.

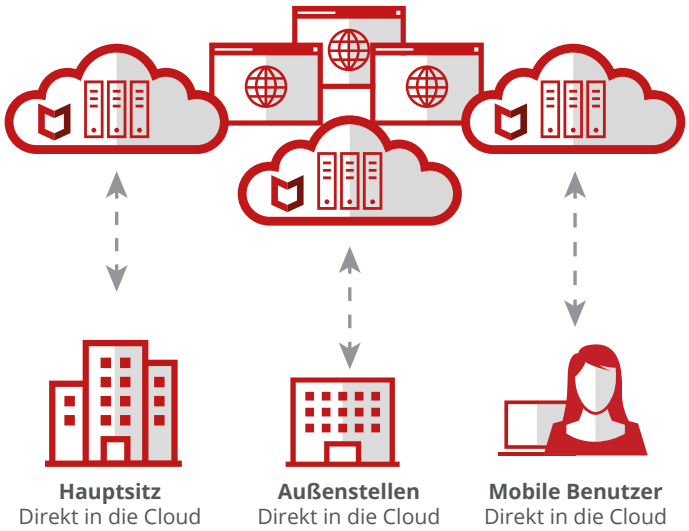

Abbildung 1. McAfee Web Gateway Cloud Service-Implementierung

Effiziente Sicherheitsverwaltung

Die konsolen- und richtlinienübergreifende Verwaltung der Sicherheit ist beschwerlich, insbesondere wenn lokale und Cloud-basierte Web-Sicherheitsmaßnahmen separat verwaltet werden. In einer hybriden Umgebung gibt es eine Verwaltungskonsole für lokale und Cloud-Implementierungen sowie einen gemeinsamen Satz Richtlinien und eine Schnittstelle für die Berichterstellung.

Bei einer eigenständigen Implementierung ohne lokale Hard- oder Software wird McAfee Web Gateway Cloud Service zusammen mit der Endgerätesicherheit von McAfee ePO™ Cloud verwaltet, der einheitlichen Verwaltungskonsole für alle Cloud-basierten Sicherheitsdienste von McAfee. Dadurch ergibt sich eine bisher einmalige Effizienz für die Sicherheitsverwaltung.

Die Implementierung der Web-Sicherheit für Endgeräte ist eine anspruchsvolle Aufgabe, insbesondere in Bezug auf Routing und Authentifizierung. Der optionale Endgeräte-Client McAfee Client Proxy automatisiert das Routing und die Authentifizierung bei unserem Cloud-Dienst, um eine jederzeit verfügbare Verbindung zur Cloud bei konsistenter Richtlinienanwendung sicherzustellen. McAfee Client Proxy funktioniert in einer hybriden Implementierung nahtlos mit lokalen Appliances. Dabei wird der Datenverkehr automatisch zur Appliance geleitet, wenn der Benutzer im Netzwerk arbeitet, bzw. zum Cloud-Dienst, wenn er sich außerhalb des Netzwerks befindet. Weitere Routing- und Authentifizierungsoptionen sind verfügbar und können je nach den Anforderungen des Unternehmens ausgewählt werden.

Weitere Informationen

Weitere Informationen finden Sie unter **www.mcafee.com/de/products/web-gateway-cloud-service.aspx**.

McAfee
Together is power.

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