McAfee Email Protection

Fortschrittlicher Schutz für Postfächer – überall und jederzeit

Unternehmen benötigen mehr denn je zuvor fortschrittlichen E-Mail-Schutz. Laut dem SANS Institute sind 95 Prozent aller Netzwerkangriffe das direkte Ergebnis erfolgreicher Spearphishing-Angriffe.[1] Benutzer fallen auch weiterhin auf Social-Engineering-Techniken herein, und Internetkriminelle haben ihr Repertoire entsprechend erweitert, um mithilfe weiterer raffinierter Taktiken selbst sicherheitsbewusste Unternehmen auf dem falschen Fuß zu erwischen. Unternehmen werden heute durch hochentwickelte Malware und Diebstahl geistigen Eigentums bedroht, die den Geschäftsbetrieb erheblich beeinträchtigen können. Hinzu kommt, dass Unternehmen zunehmend zu gehosteten E-Mail-Postfächern wechseln, die das Risiko erhöhen können. Und schließlich kann auch die fehlende Flexibilität veralteter E-Mail-Schutzlösungen Unternehmen dazu zwingen, sich nach einer besseren Alternative umzusehen. McAfee® Email Protection ist die Antwort. Diese leistungsfähige Lösung bietet unternehmensgerechten Schutz vor gezielten Phishing-Bedrohungen und umfasst eine Technologie zum Schutz vor Datenkompromittierung (Data Loss Prevention, DLP) sowie eine Funktion für kontinuierliche E-Mail-Verfügbarkeit. Dank der flexiblen Bereitstellungsmöglichkeiten (Cloud-basiert, vor Ort sowie als integrierte Hybrid-Lösung) können Sie E-Mail-Sicherheit zum gewünschten Zeitpunkt und auf die gewünschte Weise implementieren.

Hauptvorteile

Schutz vor gezielten Phishing-Angriffen

- Erkennung böswilliger URL-Bedrohungen in Echtzeit dank ClickProtect
- Vernetzung mit McAfee Advanced Threat Defense zur Abwehr von Stealth-Malware
- Integrierte Technologie zum Schutz vor Datenkompromittierung

Sicherheit für gehostete Postfächer

- Schutz vor gezielten Angriffen unabhängig vom Zielort der E-Mail
- Graymail-Endbenutzerkontrollen
- Kontinuierliche E-Mail-Verfügbarkeit
- Detaillierter Schutz vor Datenkompromittierung sowie Verschlüsselungsfunktionen

Flexible Bereitstellungsoptionen

- Bereitstellung ganz nach eigenem Bedarf
- Möglichkeit zur Hybrid-Bereitstellung mit zentraler Verwaltungs- und Berichterstellungskonsole

Social Engineering war gestern: Neue Spearphishing-Taktiken

Im Fall von Phishing-Angriffen ist der Benutzer das schwächste Glied. Der *Verizon Data Breach Investigation Report 2014*[2] (Verizon-Untersuchungsbericht zur Datenkompromittierung für 2014) weist darauf hin, dass beinahe jeder fünfte Benutzer auf einen Link in einer Phishing-E-Mail klickt. Internetkriminelle nutzen diese Schwachstelle auch weiterhin mit Social-Engineering-Methoden aus, sind jedoch einen Schritt weitergegangen und setzen raffinierte Taktiken ein, durch die E-Mail-Bedrohungen schwer zu erkennen sind. Hier einige Beispiele:

- **Einmalig nutzbare URLs:** Internetkriminelle schalten böswillige URLs ab, nachdem Opfer auf Phishing-Betrug hereingefallen sind und die Infektion stattgefunden hat. Dadurch wird die Erkennung und Forensik mindestens erschwert, wenn nicht sogar unmöglich.
- **Verzögerte Infektion:** In einigen Fällen warten die Angreifer, bis die E-Mail gescannt, zugelassen und in das Unternehmenspostfach übermittelt wurde, um *anschließend* den Schadcode auf der Ziel-Webseite zu injizieren. Angestellte vertrauen im Allgemeinen E-Mails, die sie auf Arbeit erhalten, und könnten so auf einen gefährlichen Link klicken.
- **Sandbox-bewusste Malware:** Diese Art von böswilligem Code umgeht die Erkennung, indem er passiv bleibt, um zu einem späteren Zeitpunkt aktiv zu werden.

Fortschrittliche mehrschichtige Schutzmaßnahmen

Schutz zum Klickzeitpunkt
McAfee Email Protection bietet mehrere Schutzebenen, mit denen Sie raffinierte Spearphishing-Angriffe und die dazugehörige Stealth-Malware abwehren können. McAfee Email Protection nutzt die bestbewertete McAfee Gateway Anti-Malware Engine[3] von McAfee Web Gateway und integriert ClickProtect, eine Technologie für URL-Schutz zum Scan- und Klickzeitpunkt. Diese Technologie kann auf jedem Gerät und an jedem Ort Spearphishing-Angriffe abwehren. ClickProtect bietet Schutz vor Bedrohungen durch eingebettete URLs in E-Mail-Nachrichten. Die Lösung sucht nach Veränderungen in der Absicht von URLs, die zwischen dem Scan-Zeitpunkt der E-Mail (unabhängig davon, ob die Nachricht zu dieser Zeit harmlos erschien) und dem Klick-Zeitpunkt des Benutzers auftreten.

Betrachten wir das folgende Szenario mit verzögert aktivierter Malware, bei dem ein Angreifer eine E-Mail an den Finanzvorstand Ihres Unternehmens versendet, die eine scheinbar harmlose URL enthält. Ihre E-Mail-Sicherheitslösung empfängt die E-Mail, untersucht sie, befindet sie für ungefährlich und übermittelt sie ins Zielpostfach. Nachdem nun aber die E-Mail ins Posteingang des Finanzvorstands gelangt ist, legt der Angreifer Malware auf der Ziel-Webseite ab. Wenn der Vorstand auf den Link klickt, wird Ihr Netzwerk infiziert.

Wenn nun jedoch ClickProtect aktiv ist und eine URL in einer E-Mail angeklickt wird, fragt unsere Lösung: „Ist die URL noch sicher?“ Alle übermittelten URLs werden von der McAfee Gateway Anti-Malware Engine erneut untersucht, um mithilfe von Verhaltensemulation böswillige Web-Inhalte zu erkennen, ohne dass eine Signatur notwendig wird.

In einer sicheren Vorschau können die Benutzer die böswilligen Webseiten in einer geschützten Umgebung ansehen und werden dabei über empfohlene Sicherheitsmaßnahmen informiert, was eine zusätzliche Sicherheitsebene bedeutet und das Risiko insgesamt verringert. E-Mails können sicher weitergeleitet werden, und selbst wenn die Empfänger nicht über ClickProtect verfügen, ist der Schutz fest mit der E-Mail verbunden.

Erkennung und Abwehr von Stealth-Malware
Dank der Verzahnung mit McAfee Advanced Threat Defense kann McAfee Email Protection Zero-Day-Stealth-Malware in verdächtigen Dateianhängen entdecken und blockieren, noch bevor sie Ihren Posteingang erreicht. Dieser innovative und mehrschichtige Ansatz kombiniert gründliche statische (Reverse Engineering) und dynamische (Sandbox-) Analysen, um das tatsächliche Verhalten der Malware zu ermitteln. Die vollständige statische Code-Analyse bietet detaillierte Malware-Klassifizierungsinformationen, erweitert die Schutzmaßnahmen um Funktionen zur Abwehr stark getarnter sowie schwer aufzuspürender Bedrohungen und erlaubt die Identifizierung von ähnlicher Malware, die den gleichen Code verwendet. Verzögerte oder verborgene Ausführungspfade, die in einer dynamischen Sandbox-Umgebung häufig nicht ausgeführt werden, können durch das Entpacken und die vollstatische Analyse ermittelt werden.

Integrierter Schutz vor Datenkompromittierung
Gezielte Spearphishing-Angriffe haben letztendlich alle ein Ziel: die Kompromittierung wertvoller und sensibler Daten. In McAfee Email Protection integriert ist die branchenführende Technologie unserer DLP-Lösungen. Dazu zählen integrierte Wörterbücher für PCI DSS, Gesundheitswesen, Finanzdaten, regionale Datenschutzbestimmungen usw., wodurch Sie schnell Compliance-Richtlinien für die Erkennung, Speicherung und Übertragung sensibler Daten entwickeln können.

Durch die Erstellung und Speicherung von digitalen Fingerabdrücken ausgewählter Dokumente lernt McAfee Email Protection, welche Arten von Inhalten durch Richtlinien gesteuert und geschützt werden müssen. Mithilfe eines Tools für reguläre Ausdrücke, anpassbaren Wörterbüchern, Schwellenwertzählern, tiefgehenden Inhalts-Scans für mehr als 300 Dokumenttypen sowie Whitelists können Sie Richtlinien für Anhänge und Inhalte erstellen sowie für verschiedene Benutzergruppen in Ihrem Unternehmen erzwingen.

McAfee Email Protection enthält bereits im Lieferumfang Funktionen zur Push- bzw. Pull-Übertragung verschlüsselter E-Mails und beherrscht die Standards TLS, S/MIME sowie PGP. Die Lösung kann als virtuelle oder Hardware-Appliance oder als Blade-Server bereitgestellt werden, ohne dass Zusatzkosten anfallen.

McAfee Email Gateway

Virtuelle Appliance-Umgebungen und Systemvoraussetzungen

- VMware vSphere 4.x oder höher
- VMware vSphere Hypervisor (ESXi) 4.x oder höher
- Prozessor: Zwei virtuelle Prozessoren
- Verfügbarer virtueller Speicher: 2 GB
- Freier Festplattenspeicher: 80 GB

Hardware-Appliance

- Verfügbar in zwei Modellen und getrennt erhältlich
- Außerdem als Blade-Server erhältlich

Zum dritten Mal in Folge erhielt McAfee Email Protection vom **SC Magazine die Höchstpunktzahl von 5 Sternen**.

Funktionen für kontinuierliche E-Mail-Verfügbarkeit zur Gewährleistung unterbrechungsfreier Geschäftsabläufe

Die Geschäfte gehen weiter, auch wenn Ihr E-Mail-Netzwerk ausfällt. Egal, ob das Netzwerk wegen Naturkatastrophen, Stromausfall oder regulärer Wartungsarbeiten ausfällt – die McAfee Email Protection-Funktion für kontinuierliche E-Mail-Verfügbarkeit sorgt für die zuverlässige Verbindung Ihrer Mitarbeiter, Kunden, Partner und Lieferanten rund um die Uhr. Außerdem bewahrt diese Funktion alle während des Ausfalls gesendeten oder empfangenen Nachrichten auf und synchronisiert auf intelligente Weise ein präzises Verzeichnis aller E-Mail-Aktivitäten während der Ausfallzeit, bis Ihre E-Mail-Server wieder online gehen.

Intelligenz und Bedrohungsreputation

McAfee Email Protection besitzt ein weiteres leistungsfähiges Tool in seinem Arsenal – den branchenweit umfassendsten Bedrohungsanalysedienst McAfee Global Threat Intelligence (McAfee GTI). Dieser Dienst erfasst in Echtzeit Daten von mehr als 100 Millionen Sensoren über die Vektoren Datei, Web, E-Mail und Netzwerk. Die Reputationsanalyse von McAfee GTI minimiert die Risiken, indem E-Mails von verdächtigen Quellen, mit Links zu verdächtigen Webseiten oder bekannt böswilligen Dateianhängen blockiert werden.

Weil die Wahrscheinlichkeit, dass Malware, Phishing-Angriffe und hochentwickelte hartnäckige Bedrohungen Ihr Netzwerk infiltrieren, erheblich verringert wird, bleibt Ihr Unternehmen sicherer und benötigt seltener kostenintensive Behebungsmaßnahmen.

Sicherheitsprobleme bei gehosteten E-Mails

Immer häufiger werden die E-Mail-Adressen von Unternehmen bei E-Mail-Dienstleistern gehostet, beispielsweise Microsoft Office 365, Google Apps for Work und anderen. Viele gehostete E-Mail-Lösungen bieten zwar Sicherheitsfunktionen, doch erfüllen sie wirklich alle Ansprüche? Wahrscheinlich nicht, da Phishing-Versuche, Spam und Graymail auch weiterhin ein Problem darstellen und die integrierten Sicherheitsfunktionen nicht in der Lage sind, Datenexfiltration abzuwehren. Hinzu kommt, dass E-Mail-Ausfälle im Zusammenhang mit z. B. Office 365 die Produktivität unterbrechen können. McAfee Email Protection bietet unternehmensgerechten Schutz zur Abwehr gezielter Phishing-Angriffe und hochentwickelter Malware in der Testphase sowie während und nach der Migration. Unabhängig davon, wann oder wo Ihre Postfächer bereitgestellt werden, bietet McAfee Email Protection vollständige Abdeckung und unterbrechungsfreien E-Mail-Betrieb.

Flexible Bereitstellungsoptionen für heute und morgen

Mit McAfee Email Protection können Sie Ihre E-Mail-Sicherheit flexibel entsprechend den Anforderungen Ihres Unternehmens bereitstellen. Sie haben die Wahl zwischen einer Cloud-basierten Software-as-a-Service-Lösung (SaaS), einer Lösung vor Ort (virtuelle Appliance, Hardware-Appliance oder Blade-Server) bzw. einer Hybrid-Kombination beider Varianten. Bei McAfee Email Protection können Sie Ihre E-Mail-Sicherheit auf die für Sie optimale Weise bereitstellen und später skalieren oder gänzlich ändern.

Unabhängig von Ihrer Wahl stellt Ihnen McAfee Email Protection zur konsolidierten Berichterstellung eine einzelne und zentrale Verwaltungskonsole bereit, mit der Sie unkompliziert die Effektivität Ihrer E-Mail-Sicherheitsprogramme überprüfen können. Für Cloud-basierte und vor Ort eingesetzte Komponenten der Lösung werden Richtlinien angewendet.

Wenn Sie weitere Informationen wünschen oder McAfee Email Protection evaluieren möchten, wenden Sie sich bitte an Ihren McAfee-Vertriebsrepräsentanten, oder besuchen Sie **www.mcafee.com/de/products/email-and-web-security/email-security.aspx**.

1. **http://blogs.mcafee.com/business/security-connected/is-there-something-phishy-in-your-inbox**
2. **https://dti.delaware.gov/pdfs/rp_Verizon-DBIR-2014_en_xg.pdf**
3. AV-TEST: *McAfee Web Gateway Security Appliance Test* (Test der Sicherheits-Appliance McAfee Web Gateway)

McAfee. Part of Intel Security.
Ohmstr. 1
85716 Unterschleißheim
Deutschland
+49 (0)89 37 07-0
www.intelsecurity.com

Intel und das Intel-Logo sind eingetragene Marken der Intel Corporation in den USA und/oder anderen Ländern. McAfee und das McAfee-Logo sind eingetragene Marken oder Marken von McAfee, Inc. oder seinen Tochterunternehmen in den USA und anderen Ländern. Alle anderen Namen und Marken sind Eigentum der jeweiligen Besitzer. 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. Copyright © 2015 McAfee, Inc. 61523ds_email-protection-o365_0115