Solution Brief

mimecast

Email Security 3.0

Wir sichern Sie am E-Mail-Perimeter - an Ihren Unternehmensgrenzen

Zone 1

E-Mail Security als zwingende Notwendigkeit

Weiterhin gehört die Abwehr von Cyber-Attacken über E-Mails zu den größten Herausforderungen für IT- und Sicherheitsteams. Malware, Spam, Phishing, Ransomware, Identitätsmissbrauch - es gibt so viele Möglichkeiten für Angreifer und Angriffstaktiken ändern sich laufend und werden immer anspruchsvoller. E-Mail ist das wichtigste Kommunikationsmedium für Unternehmen und der Geschäftsbetrieb ist davon abhängig. Dieses „Einfallstor" zu sichern ist der wichtigste Schritt Ihr Unternehmen vor Datenverlusten, Geschäftsunterbrechungen und finanziellen Schäden zu schützen.

Mimecast schützt Sie mehrschichtig am Perimeter, Ihrer Unternehmensgrenze. Mimecast Advanced Email Security mit Targeted Threat Protection nutzt mehrere hochentwickelte Erkennungsmodule und verschiedene Bedrohungsdatenquellen, um E-Mails vor modernen Bedrohungen zu schützen.

Email Security 3.0

Mimecast Email Security 3.0 hilft Ihnen dabei, sich von einer auf dem Perimeter basierenden Sicherheitsstrategie zu einer umfassenden und allgegenwärtigen Strategie zu entwickeln, die Schutz in drei Zonen bietet. Diese Schutzmaßnahmen werden durch ein breites Portfolio an ergänzenden Lösungen, umsetzbar Threat Intelligence und eine wachsende Auswahl an APIs ergänzt.

Zonen-basierte Abwehr

Zone 1
am E-Mail-Perimeter

Zone 2
innerhalb Ihres Netzweks & Unternehmens

Zone 3
außerhalb des Perimeters

Erweiterungen

Kontinuität & Wiederherstellung

Webbedrohungen & Schatten-IT

Datenschutz & Verschlüsselung

Governance & Compliance

Ecosystem & Threat Intelligence

E-Mail-Sicherheit auf dem neuesten Stand der Technik

Mimecast Email Security kombiniert alle Funktionalitäten in einer cloud-basierten Plattform. Die Mimecast Plattform wurde entwickelt, um mit einer sich rasch ändernden Bedrohungslandschaft mitzuhalten und kombiniert ein sicheres E-Mail Gateway mit Data Leak Prevention, Inhaltskontrollen, Targeted Threat Protection und unterstützt Sie Cyber Attacken zu bekämpfen.

Ein Beispiel aus der Praxis

Paul hat seine Organisation zu Office 365 migriert. Bald darauf stürmte sein CFO, Markus Tegel, in sein Büro und fragte, warum sein Team immer wieder E-Mails von einem "Markus Tegel" erhält, in denen er um Überweisungen bittet. Paul öffnete ein Ticket bei Microsoft und wartete auf eine Antwort. Kurze Zeit später hatte Microsoft Probleme mit dem Active Directory, die alle Office 365-Anwendungen, einschließlich Exchange Online, verlangsamten. Markus kam zurück in Pauls Büro und fragte sich dieses Mal, warum er keine E-Mails senden oder empfangen konnte. Wieder öffnete Paul ein Ticket bei Microsoft. Als der Zustrom von Spam und gezielten Angriffen anhielt, wurde Paul klar, dass er eine Lösung brauchte, die in der Lage war, unerwünschte E-Mails zu blockieren, bevor sie Office 365 erreichten.

Welche Lösung bietet Mimecast?

Mehrstufige Inspektion von eingehenden und ausgehenden E-Mails, Schutz vor gezielten Angriffen wie Social Engineering und Identitätsmißbrauch.

- **Kompromittierung geschäftlicher E-Mails, Phishing und Spear-Phishing –** Identitätsmißbrauch nimmt zu, wobei Cyber-Kriminelle zunehmend Social Engineering und andere ausgeklügelte Techniken einsetzen. Erhalten Sie umfassenden Schutz durch die Echtzeitprüfung des angezeigten Namens und des Inhalts der eingehenden E-Mail sowie durch die Erkennung von Zeichenwechsel, zusätzliche Prüfungen auf Ähnlichkeiten sowie die Verwendung langer URL-Strings.
- **Bösartige Anhänge –** Es ist für Angreifer nur allzu leicht, Anhänge mit Skripten zu infizieren, die bösartige Inhalte wie Ransomware, Trojaner und Botnets herunterladen. Schützen Sie Ihre Enduser mit einem mehrschichtigen Schutz, einschließlich Umwandlung von Dateien in sichere Formate, statischer Dateianalyse und Sandboxing.
- **Bösartige URLs –** URLs, die auf Phishing-Websites verweisen oder zur Installation von Malware, Viren oder Trojanern bestimmt sind, stellen eine große Sicherheitsherausforderung dar. Mimecast bietet eine mehrstufige Erkennung und blockiert bösartige URLs, einschließlich URL-Erkennung vor dem Klicken, Schutz im und außerhalb des Unternehmensnetzwerks von jedem Gerät aus, Neuschreiben aller URLs in eingehenden E-Mails und Echtzeit-Scans bei jedem Klick.

- **Verlust von sensiblen Informationen –** Datenverlust ist ein hochaktuelles Thema, das das Vertrauen schnell untergraben kann. Schützen Sie sensible Daten und geistiges Eigentum mit Mimecast Data Leak Prevention. Sowohl vorgefertigte als auch benutzerdefinierte Bibliotheken sowie automatisierte Kontrollen verhindern, dass Mitarbeiter versehentlich oder absichtlich Informationen an Personen senden, die hierauf keinen Zugriff haben sollten. Es können auch Richtlinien ausgelöst werden, die die Verwendung von Secure Messaging erfordern.
- **Schlanke IT –** Eine schlanke IT-Infrastruktur wird für immer mehr Organisationen zum Standard, was zu kleineren Teams, begrenzter Kapazität und ggf. auch fehlendem Know-how im Unternehmen führen kann. Entlasten Sie Ihr Personal und reduzieren Sie sowohl Kosten als auch Komplexität mit einem umfassenden Package von E-Mail-Security Services, die in einer einzigen, Cloud-basierten, benutzerfreundlichen Plattform bereitgestellt werden.
- **Lücken in der Sicherheit von Office 365 –** Es steht außer Frage, dass Office 365 ein großartiger E-Mail-Dienst ist, aber Sie benötigen eine ebenso effektive E-Mail-Sicherheitstechnologie. Unternehmen, die sich allein auf die Sicherheit von O365 verlassen, stellen oft fest, dass das, was wie eine einfache Lösung aussah, stattdessen eine Menge Probleme schafft - geringere Wirksamkeit, mehr Spam und begrenzter Support. Mimecast Email Security ergänzt O365, indem mehrere Schutz-Layer sowie Ausfallsicherheit hinzufügt werden, so dass Sie die Vorteile des Wechsels zur Cloud nutzen können, ohne das Risiko zu erhöhen.

Vertrauen Sie Ihren E-Mails wieder

Sichern Sie Ihren wichtigsten Kommunikationskanal:

- Schutz gegen Speer-Phishing und erweiterte E-Mail-Bedrohungen
- Schutz der Mitarbeiter vor Identitätsdiebstahl-Angriffen, die einen vertrauenswürdigen Absender vortäuschen
- Neutralisierung von Bedrohungen durch Malware-Anhänge und bösartige URLs
- Nutzung der Kosten- und Leistungsvorteile der Multi-Tenant-Cloud
- Vereinfachung der Verwaltung und Verringerung der Belastung für IT und Sicherheit
- Reduzierung von Kosten und Komplexität
- Bereitstellung eines Dienstes der stets auf dem aktuellsten Stand ist und den Wettlauf mit der Bedrohungslandschaft gewinnt
- Bereitstellung von „Self-Service-Funktionen“ für Endbenutzer, so dass diese selbst über Outlook, Web und mobile Anwendungen zugreifen können.