Solution Brief

mimecast

Email Security 3.0

Wir sichern Sie auch innerhalb Ihres Netzwerks und Ihres Unternehmens

Zone 2

E-Mail-Sicherheit als zwingende Notwendigkeit

Bedrohungen, die innerhalb einer Organisation existieren, werden oft unterschätzt, doch diese bergen dieselben Risiken, wie solche aus externen Quellen. Angriffe können sich unbemerkt und sehr schnell von User zu User, oder schlimmer noch, von Mitarbeitern zu Kunden und Partnern ausbreiten. Und ohne ein angemessenes Sicherheitsbewusstsein sind Mitarbeiter sehr anfällig für einen unbewussten, aber verheerenden Fehler.

Wenn man bedenkt, dass...

- 60% des E-Mail-Verkehrs in Organisationen interne (von Mitarbeiter zu Mitarbeiter) sowie ausgehende Mails* sind.
- menschliches Versagen die Ursache für die große Mehrheit erfolgreicher Angriffe ist.
- 71% der Organisationen berichten, dass sich böswillige Aktivitäten in den letzten 12 Monaten von Mitarbeiter zu Mitarbeiter verbreitet haben.**

Basiert auf aggregierten Daten von Mimecast Kunden
*** 2019 State of Email Security Report*

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	Erweiterungen
Zone 1 am E-Mail-Perimeter	Kontinuität & Wiederherstellung
Zone 2 innerhalb Ihres Netzweks & Unternehmens	Webbedrohungen & Schatten-IT
Zone 3 außerhalb des Perimeters	Datenschutz & Verschlüsselung
	Governance & Compliance

Ecosystem & Threat Intelligence

Die Implementierung eines Best-Practice-Sicherheitsansatzes innerhalb Ihrer Organisation wird zu einem “Must-have” und nicht zu einem “Nice-to-have”.

In der „Zone 2“ unterstützt Sie Mimecast gezielt, Ihren internen E-Mail-Verkehr zu schützen, sowie Ihre Mitarbeiter effektiv und nachhaltig auf mögliche Cyber Bedrohungen und Gefahren zu sensibilisieren.

Stärken Sie Ihre letzte Verteidigungslinie

Selbst wenn ein robuster E-Mail-Sicherheits-Perimeter vorhanden ist, können Angreifer den Perimeter umgehen und innerhalb Ihres E-Mail-Netzwerks operieren, indem sie kompromittierte Mitarbeiterkonten, soziale Netzwerke, File Sharing Seiten und andere Techniken nutzen, um sich Zugang ins Unternehmen zu verschaffen und bösartige Mails innerhalb sowie nach extern versenden. Der integrierte Ansatz von Mimecast und die preisgekrönte Technologie helfen Ihnen dabei, interne Risiken zu bekämpfen, darunter auch:

Ein Beispiel aus der Praxis

Tausende Anwender eines großen Health Care Unternehmens erhielten einen infizierten Anhang mit dem Titel “Mitteilung an die Mitarbeiter”. Hunderte von Mitarbeitern öffneten sie innerhalb weniger Stunden und infizierten damit ihre Computer. Die IT-Abteilung versuchte den Angriff zu stoppen und begann dann mit der Säuberung aller betroffenen Systeme und der Suche nach der Ursache des Problems. Nach tagelanger manueller Arbeit wurde festgestellt, dass der Angriff von einem der Controller in der Finance Abteilung ausgegangen war. Er war sechs Monate zuvor kompromittiert worden, als er seine Anmeldedaten auf einer gefälschten Office365-Anmeldeseite eingab.

Welche Lösung bietet Mimecast?

- Kontrolle aller internen E-Mails, einschließlich URL-Kontrolle und Kontrolle der Anhänge
- Schnelle Beseitigung von Bedrohungen
- Awareness Training, so dass Sie auch gegen “menschliche Fehler“ abgesichert sind

- **Kompromittierung von einem Nutzer zum anderen und von Nutzern zu Dritten –** Wenn der interne E-Mail-Verkehr ungeschützt bleibt, können sich Angriffe leicht innerhalb Ihres Unternehmens oder auch an Kunden, Partner und Lieferanten ausbreiten. Mimecast verwendet denselben Stack von E-Mail-Sicherheitstechnologien, der am Perimeter verwendet wird, auch für den internen und ausgehenden Datenverkehr, wodurch sichergestellt wird, dass ALLE E-Mails durch Best-Practice-Sicherheitsprotokolle abgesichert werden.
- **Versteckte Malware –** Nicht alle bösartigen Inhalte werden am Gateway erkannt - einige sind so konzipiert, dass sie nach der Zustellung aktiviert werden. Um die damit verbundenen Risiken zu mindern, überprüft die Technologie von Mimecast kontinuierlich die zuvor gelieferten Dateien auf bösartige Inhalte, so dass Sie bei Bedarf Maßnahmen ergreifen können.

- **Beseitigung von Bedrohungen –** Wenn interne E-Mails ungeschützt bleiben, kann es Wochen oder Monate dauern, die Quelle eines Angriffs zu finden, ganz zu schweigen von der Zeit, die für die Behebung der Bedrohung aufgewendet werden muss. Mit Mimecast können Sie Bedrohungen schnell identifizieren und beheben. Die Technologie ermöglicht es Ihnen, Dateien nach den Kriterien Absender, Empfänger oder Nachrichten-ID zu suchen und diese nach der Zustellung automatisch oder manuell aus den Posteingängen der Benutzer zu entfernen.
- **Verbessern Sie die Awareness Ihrer Mitarbeiter –** Von Ransomware und Phishing bis hin zu unbeaufsichtigten Laptops und CEO-Fraud - die Bedrohungen sind vielfältig und betreffen jedes Unternehmen. Sie benötigen einen Plan, um das Verhalten der Mitarbeiter zu ändern und das Risiko Ihres Unternehmens zu minimieren. Das Mimecast Awareness Training kann Ihnen helfen, Cyber Risiken zu bekämpfen, die aus einfachen und leichtfertigen Fehlern resultieren, die Ihre Mitarbeiter jeden Tag begehen. Das Mimecast Awareness Training bietet effektive Online-Sicherheitsschulungen für Mitarbeiter – und das in etwa drei Minuten pro Monat. Die Trainingsmodule wirken wie witzige, moderne, 3-minütige Sitcom-Folgen und behandeln Cyber Risiken, die relevant und gegenwärtig sind.
- **Identifizierung und Support von Mitarbeitern mit einem hohen Risiko –** Die meisten Schulungsprogramme behandeln alle gleich, aber unterschiedliche User stellen unterschiedliche Risikograde dar. Mit Mimecast Awareness Training können Sie das Bewusstsein und das Risiko Ihrer Mitarbeiter auf individueller Ebene messen und dabei sowohl das Wissen als auch die Stimmung berücksichtigen. Anhand von Risikobewertungen können Sie dann das Bewusstsein im Laufe der Zeit verfolgen und bei Bedarf gezieltes Training und Unterstützung über die Plattform ausspielen.

Vertrauen Sie Ihren internen E-Mails

Machen Sie die Sicherheit der internen E-Mails zu Ihrer Stärke:

- ALLE E-Mails werden mehrstufiger Best-Practice Sicherheitschecks unterzogen
- Schutz vor latenter Malware durch kontinuierliche Überprüfung der bereits bereitgestellten Inhalte
- Automatische oder manuelle Korrektur unerwünschter E-Mails nach der Zustellung
- Verhindern Sie das Übertragen von Angriffen zwischen Mitarbeitern sowie zwischen Mitarbeitern und Dritten
- Bieten Sie effektive Awareness Schulungen, welche die Mitarbeiter gerne absolvieren und die das Verhalten der Mitarbeiter auch tatsächlich ändern
- Messen Sie das Risiko des Sicherheitsbewusstseins auf der Mitarbeiter- und Organisationsebene

Durch die Kombination bewährter Schulungstechniken mit einer Best-Practice-E-Mail-Security für den internen E-Mail-Verkehr können Sie Lücken in der „Zone-2-Verteidigung“ schließen und Ihre Sicherheitsstrategie verbessern.