

Mimecast blockiert Bedrohungen, die Microsoft übersieht

Die Zahlen

Für jede 1 Million E-Mails, die durch Microsofts erweiterte Sicherheit gesendet wurden:



87.205

Unerwünschte oder schlechte E-Mails. Das ist mehr als **1 von 11**



475

BEC (Geschäfts-E-Mail-Kompromittierung) und **VIP** Impersonationsangriffe



122

Malware und böartige **Anhänge**



86.472

Spam und opportunistische **Angriffe**

JETZT ENTDECKEN

Unentdeckt

Die Ergebnisse zeigen, dass viel zu viele Angriffe durch die Sicherheit von Microsoft 365 schlüpfen.



Für Betrüger steht Microsoft 365 besonders dafür:

mehr Einstiegspunkte und mehr Daten um Nutzer zu bestehlen zu können.



Es zeigt sich eine Zunahme von **speziell entwickelten Bedrohungen**, die sich der Erkennung in Microsoft-abhängigen Umgebungen entziehen.

Warum Mimecast?

Angesichts der Raffinesse und Unerbittlichkeit von Cyberangriffen reicht Microsofts Sicherheit nicht mehr aus.



Mimecast ist eine unschätzbare Ergänzung zu M365s grundlegendem Anti-Spam, Malware- und Spoofing-Schutz.



Mimecast schützt Sie vor dem Risiko des Arbeitens in einer Sicherheitsmonokultur.



Mimecast bietet die notwendigen E-Mail-Sicherheitsvorkehrungen für Microsoft 365.



Mimecast hilft, Bedrohungen zu stoppen, die durchkommen.

Mimecast führt ausführliche Email Security Risk Assessments (ESRA) für Unternehmen durch, die derzeit einen anderen Email Security Provider nutzen. Eine typische ESRA dauert in der Regel einen Monat. In dieser Zeit überprüft Mimecast alle eingehenden E-Mails, die von ihrem Sicherheitsanbieter an Unternehmen geliefert werden, um festzustellen, wie Mimecast das Risiko gemindert hätte. Im Jahr 2023 untersuchten die ESRA mehr als 4.405.658 E-Mails, die von Microsofts Defender für Office 365 zugestellt wurden. Alle Zahlen in diesem Dokument sind pro 1 Million E-Mails angegeben.