Datenblatt

mimecast

Mimecast CyberGraph

Künstliche Intelligenz schränkt die Möglichkeiten des Angreifers zur Informationsbeschaffung ein, deckt sehr gezielte E-Mail-Bedrohungen auf und unterstützt dadurch die Benutzer bei der Erkennung der Gefahr

Mimecast CyberGraph kombiniert drei wichtige Technologien zum Schutz vor gezielten E-Mail Angriffen:

- Schutz vor E-Mail-Trackern
- Identity Graph mit Machine Learning
- Dynamische, kontextbezogene Banner eingebettet in E-Mails

Begrenzt das Sammeln von Informationen

Ein Angreifer kann in der Spähphase Tracker in E-Mails einbetten, die aus der Ferne Informationen von einem anderen Server abrufen. Dadurch werden die IP-Adresse des Geräts, der Standort, der Grad der Interaktion des Empfängers mit dem E-Mail-Inhalt, das Betriebssystem und die Browser-Versionen des Geräts mitprotokolliert.

Mimecast CyberGraph ersetzt diese Tracker und “projiziert” den Inhalt, sodass der Standort des Empfängers und dessen Aktivitäten abgeschirmt werden. Dies hindert Angreifer daran, herauszufinden, ob sie z.B. die richtige Person für den Betrug ausgewählt haben. Es schränkt auch ihre Fähigkeit ein, wichtige Informationen zu sammeln, die ihnen bei der Erstellung einer authentischen Spear-Phishing-E-Mail helfen würden z. B. durch Nennung des Standorts der Zielperson.

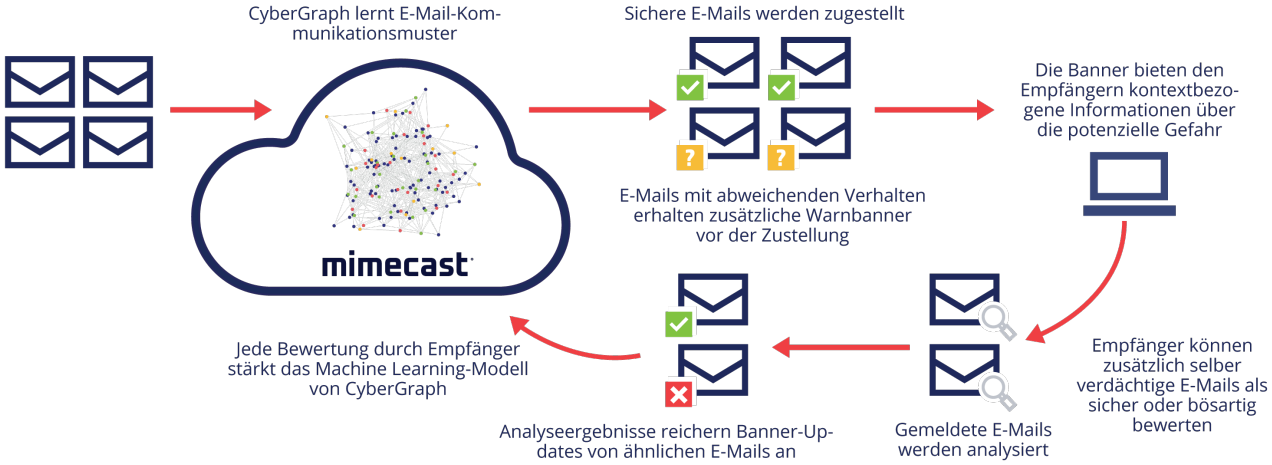
Die wichtigsten Funktionen:

- Begrenzt das Sammeln von Informationen, wodurch einem Angreifer eine gezielte Attacke erschwert wird
- Verhindert die Offenlegung von potenziell ausnutzbaren Software-Schwachstellen
- Die Identity Graph-Technologie erkennt ausgefeilte, sehr gezielte E-Mail-Bedrohungen
- Machine Learning stärkt den Schutz, ohne den Aufwand für die Konfiguration einzelner Regeln
- Warnt Benutzer nur in verdächtigen/ riskanten E-Mails mit dynamischen Bannern („Ampel-System“)
- Benutzer können besser Entscheidungen fällen und durch ihr Feedback - ob eine E-Mail bösartig oder sicher ist - das Machine Learning-Modell optimieren

Künstliche Intelligenz erkennt gezielte E-Mail-Bedrohungen

Die CyberGraph Machine Larning KI lernt Verhaltensweisen, um einen Identity Graph zu erstellen. Dieser speichert Informationen über Beziehungen und Verbindungen zwischen allen Absendern und Empfängern, sowie eine Bewertung der Beziehung und der Nähe. Es lernt, was “normal” ist und erkennt abweichende Verhaltensweisen, die mit anderen verdächtigen Indikatoren kombiniert werden können, um das Risiko einer E-Mail zu bestimmen.

Wie es funktioniert



Warnbanner warnen die Empfänger vor Risikoindikatoren

Farbige Banner, die den Grad des Risikos anzeigen, werden verdächtigen E-Mails vor der Zustellung hinzugefügt. Sie geben den Empfängern vielfältige Informationen über die Art der Gefahr, um sie am Zeitpunkt des größten Risikos zu warnen - wenn sie gerade dabei sind, die E-Mail zu lesen und zu bearbeiten. Die Banner und der Wortlaut für jeden Indikator können auf die Bedürfnisse und den Wissensstand der Benutzer Ihrer Organisation angepasst werden. Die Banner werden unabhängig vom Gerätetyp oder E-Mail-Client angezeigt und sind kompatibel mit dem Anzeigeformat der E-Mail-Vorschau oder Betreffzeilen.

Die Empfänger tragen zu einem erhöhten Schutz bei

Empfänger können E-Mails als bösartig oder sicher melden. Dies stärkt das maschinelle Lernmodell und aktualisiert CyberGraph mit Informationen über Vertrauensbeziehungen zwischen Absendern und Empfängern. Je mehr Benutzer die Reports nutzen um den E-Mail-Inhalt zu klassifizieren und somit Mimecasts Bedrohungsdaten zu speisen, desto mehr profitieren letztlich alle Kunden davon.

Dynamische Banner informieren alle Nutzer schnell über neue Bedrohungen

Links zu den Bannern werden in E-Mails eingebettet, sobald diese geprüft und als verdächtig eingestuft wurden. Auf diese Weise kann jeder beliebige Banner mit neuen Informationen über die Risikoindikatoren zu jeder Zeit aktualisiert werden, einschließlich der Änderung seiner Farbe. Zum Beispiel wird eine E-Mail mit einem blauen Informationsbanner als bösartig gemeldet und dies nach einer Analyse bestätigt.

Der Banner kann nun automatisch auf rot geändert werden, sodass ein Empfänger, der eine ähnliche E-Mail öffnet, einen roten Banner angezeigt bekommt.
Dies ist eine sehr effektive Methode um die Aufmerksamkeit der Benutzer aufrechtzuerhalten anstatt statische Banner zu verwenden, welche die Benutzer oft ignorieren.