Cyber AI Platform

Antigena Email

Immunität für Ihren Posteingang

Auf einen Blick

- Lernt von selbst: Versteht den Menschen und schaut nicht nur auf die E-Mail-Adresse
- Identifiziert schädliche E-Mails, die traditionelle Tools übersehen
- Wehrt raffinierte E-Mail-Angriffe jeder Art ab, auch Social Engineering
- Schnelle, virtuelle Installation

Diese E-Mail-Bedrohungen wehrt Antigena Email ab:

- Spear Phishing
- Social Engineering & Impersonation
- Kompromittierung geschäftlicher E-Mail-Systeme
- Kaperung von Supply-Chain-Konten
- Datenausschleusung
- Neuartige, unbekannte Malware

> Wir waren schockiert, was unsere traditionellen Tools alles nicht erkannten, im Gegensatz zu Antigena Email.
>
> **– CTO, Bunim/Murray Productions**

Neuartige E-Mail-Bedrohungen dringen erfolgreich ein

E-Mail-Angriffe werden immer raffinierter, da KI für schädliche Zwecke missbraucht wird und E-Mail-Angriffskampagnen in absehbarer Zukunft noch gefährlicher werden. Es ist schon jetzt schwer, gezielte Spoofing-E-Mails von legitimen Nachrichten zu unterscheiden.

Neuartige Angriffe schaffen es an traditionellen E-Mail-Sicherheitstools vorbei, weil sie einzelne E-Mails isoliert betrachten und lediglich mit Regeln und Signaturen bekannter schädlicher Angriffe abgleichen. Da die Lieferketten immer komplexer und die Mitarbeiter immer mobiler werden, wird ein KI-gestützter Self-Learning-Ansatz für die E-Mail-Sicherheit immer wichtiger.

> Mehr denn je erfordert moderne E-Mail-Sicherheit Innovation und ein Umdenken, um sich in der schnell veränderlichen Bedrohungslandschaft zu schützen.
>
> **– Gartner**

Der weltweit erste Posteingang, der sich selbst verteidigt

Antigena Email ist die weltweit erste Cyber-KI-Lösung für Posteingänge. Die Technologie lernt die normalen Verhaltensmuster – die „Patterns of Life" – jedes Benutzers und Kommunikationspartners und macht sich auf diese Weise nach und nach ein Bild von den Personen, die miteinander per E-Mail kommunizieren.

Traditionelle Sicherheitstools prüfen, ob eine E-Mail Merkmale früherer Angriffe aufweist. Antigena Email ist hingegen die einzige Lösung, welche zuverlässig untersucht, ob die Interaktion eines Empfängers mit einer bestimmten E-Mail vor dem Hintergrund seiner normalen Verhaltensmuster sowie denjenigen seiner Kommunikationspartner und des breiteren Unternehmens ungewöhnlich ist.

Dieses Kontextwissen ermöglicht es der KI, präzise Entscheidungen zu treffen und das ganze Spektrum an E-Mail-Angriffen unschädlich zu machen – von „einfachen" Spoofing-E-Mails, mit denen betrügerische Überweisungen erschlichen werden, bis hin zu heimtückischen Spear-Phishing-Versuchen.

Den Mensch hinter der E-Mail verstehen

Antigena Email ist an das menschliche Immunsystem angelehnt und nutzt die künstliche Intelligenz von Darktrace, um ein Gespür für die Verhaltensweisen jedes internen und externen Benutzers zu entwickeln. Dazu werden eingehende und ausgehende Nachrichten zusammen mit lateraler, interner Kommunikation analysiert.

Antigena Email betrachtet Empfänger als dynamische Individuen und Peers und erkennt in einzigartiger Weise subtile Abweichungen von der „Norm", sodass auf den ersten Blick unschädliche E-Mails als schädlich entlarvt werden können.

Einsatzszenario:
Kaperung eines Supply-Chain-Kontos

E-Mail-Zugangsdaten eines vertrauenswürdigen Kontakts abgreifen und sich Zugang zu dessen Postfach verschaffen.

Ist der Angreifer erst einmal in das System eingedrungen, kann er sich Einblick in frühere Korrespondenzen verschaffen und sehr überzeugende E-Mails verfassen – in die zu einem richtigen Zeitpunkt an der richtigen Stelle ein schädlicher Link oder Anhang eingebettet ist.

Während traditionelle Sicherheitstools davon ausgehen, dass es sich um einen vertrauenswürdigen Benutzer handelt, weiß Antigena Email, dass das Gegenteil der Fall ist. Die Technologie analysiert jede einzelne E-Mail vor dem Hintergrund der gelernten normalen Verhaltensmuster und erkennt subtilste Abweichungen. Dazu gehören unter anderem:

Ungewöhnlicher Anmeldeort – Antigena Email kann die lokalisierbare IP-Adresse des echten Absenders extrahieren und bestimmen, ob diese vor dem Hintergrund der üblichen Verhaltensmuster des vertrauenswürdigen Kontakts ungewöhnlich ist. Ein ungewöhnlicher Anmeldeort an sich löst möglicherweise noch keine Warnung oder eigenständige Reaktion aus, sondern fließt in die Gesamtberechnung des Systems und den Anomaliewert ein.

Ungewöhnlicher Link – Benutzer teilen oftmals Links zu Websites, die sie selbst besuchen und denen sie vertrauen. Antigena Email spürt diese Links in lateralen E-Mails auf und kann feststellen, welche Links und Domains vor dem Kontext des Unternehmens ungewöhnlich sind. Diese Vorgehensweise ist auch in anderen Bedrohungsszenarien sinnvoll, wenn es darum geht herauszufinden, ob die E-Mail-Domain eines bestimmten Absenders in geteilten internen Links vorkommt.

Ungewöhnliche Empfänger – Antigena Email modelliert grafikbasierte Beziehungen zwischen internen und externen Benutzern und Peers und versteht deren Beziehungen untereinander auf granularer Ebene. Wenn der Angreifer mehrere E-Mails an verschiedene Empfänger im Unternehmen schickt, kann Antigena Email einschätzen, wie wahrscheinlich es ist, dass diese bestimmte Gruppe eine E-Mail von derselben Quelle erhält.

Verhaltensbezogene Anomalien – Mit der Zeit lernt Antigena Email, wie verschiedene Absender ihre E-Mails aufbauen, und analysiert dabei sowohl verborgene E-Mail-Metadaten als auch Muster im Nachrichtentext. Darktrace wendet auf jede eingehende E-Mail KI an und erkennt somit subtile Veränderungen, die darauf hindeuten können, dass die E-Mail von jemand anderem als dem echten Kontoinhaber geschickt wurde.

Antigena Email setzt diese „schwachen" Indikatoren in Beziehung und kann schnell einen umfassenden Anomaliewert ermitteln. Die Technologie stellt so zuverlässig fest, dass die E-Mail schädlich ist, und neutralisiert den Angriff, bevor er Schaden anrichtet.

Testen Sie Antigena E-Mail in Ihrer eigenen Umgebung 30 Tage kostenlos

Jetzt Produktdemo buchen