Antigena Email: Social Engineering & Solicitation (Beeinflussung)

Social Engineering-Angriffe sind immer dadurch gekennzeichnet, dass versucht wird, sich die in einem Unternehmen vorherrschende Vertrauensvermutung zunutze zu machen. Die Angreifer geben sich als vertrauenswürdiger Kollege, Kontakt oder Führungskraft aus und können ihre Kommunikation dementsprechend auf den Empfänger abstimmen. So haben sie schnell einen Fuß in dem Unternehmen – um eine betrügerische Zahlung zu erwirken oder einen Mitarbeiter dazu zu bringen, sensible Dokumente und Firmendaten zu übermitteln. Diese Angriffe erfolgen typischerweise in Form von „sauberen" E-Mails, ohne schädliche Links oder Payloads, wodurch sie noch schwerer zu entdecken sind.

Da Angreifer ihre Taktiken und Techniken immer weiter verfeinern, werden Social Engineering- und Sollicitation-Angriffe immer effektiver. Es gibt mittlerweile ML-Software, die lernen kann, in welcher Art und Weise zwei Benutzer interagieren, und diese Kommunikationsmuster nachbildet. Mit diesem Wissen können sich Angreifer als vertrauenswürdiger Kontakt ausgeben und es ist kaum mehr möglich, zwischen einer legitimen E-Mail und einem KI-basierten Social Engineering-Angriff zu unterscheiden.

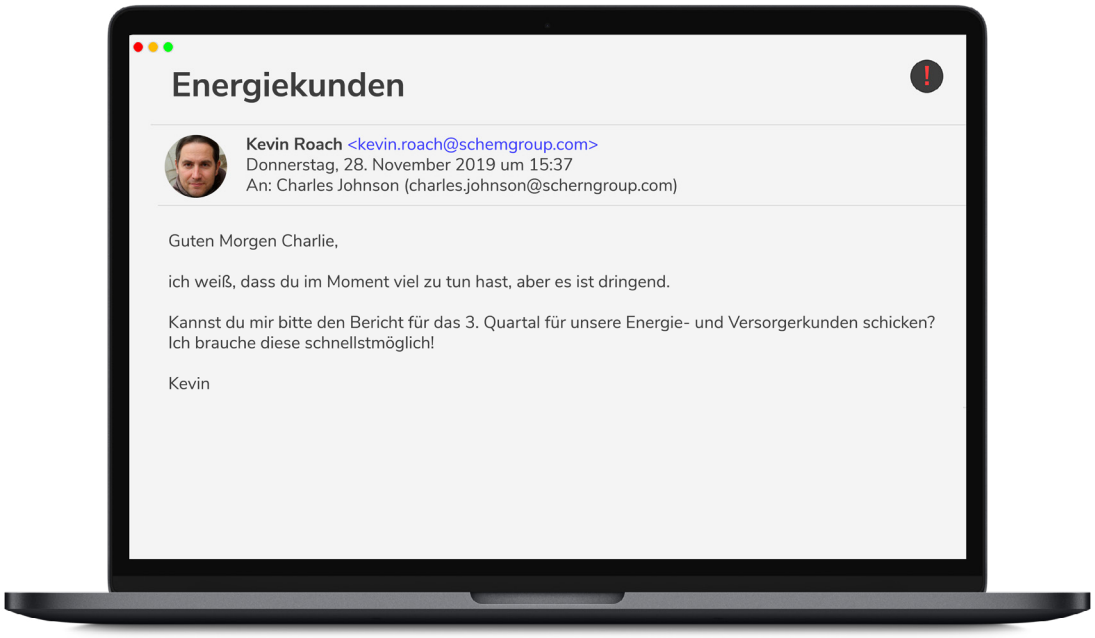

Abbildung 1: Angreifer, der sich als Führungskraft ausgibt und versucht, an sensible Dokumente heranzukommen. Man bemerke die gespoofte E-Mail-Adresse

Antigena Email: Ein Ansatz nach dem Vorbild des menschlichen Immunsystems

Antigena Email verfolgt hier einen ganz eigenen Ansatz und nutzt selbstlernende KI, um Unternehmen einen Vorsprung zu verschaffen. Die Technologie nutzt Cyber-KI, um den gesamten eingehenden, ausgehenden und lateralen E-Mail-Verkehr zu analysieren, und gewinnt auf diese Weise ein Verständnis der dynamischen Menschen und Beziehungen hinter den E-Mails. Dank dieser tiefgehenden Einblicke erkennt Antigena Bedrohungen sofort. Das ist gerade bei Sollicitation-Angriffen entscheidend, deren Ziel häufig darin besteht, die Kommunikation offline weiterzuführen und die Sicherheitsmaßnahmen zu umgehen.

Im Gegensatz zu herkömmlichen Tools am Gateway, die Informationen aus der Vergangenheit heranziehen, kann Antigena Email auf Grundlage des Bildes, das sich Darktrace von den „normalen" Verhaltensmustern macht, eigenständig auf subtile Impersonifikationsangriffe reagieren, die die E-Mail-Gateways passieren. Antigena Email trifft während des gesamten Lebenszyklus einer E-Mail Entscheidungen, sodass die Technologie ihre Analysen angesichts neuer Erkenntnisse auch nach Zustellung einer E-Mail aktualisieren kann. Da Antigena in der Lage ist, E-Mails auch nach ihrer Zustellung zu überwachen, kann die Technologie rückwirkend gesendete E-Mails abrufen, sollten sie sich später als schädlich herausstellen.

Fallstudie: Antigena Email verhindert rechtzeitig einen Impersonifikationsangriff durch Vortäuschung der Identitäten von Führungskräften

Darktrace erkannte vor kurzem einen sehr gezielten Social Engineering-Angriff, bei dem versucht wurde, die Identität von Führungskräften eines US-Technologieunternehmens vorzutäuschen. Der Bedrohungsakteur schickte eine Reihe „sauberer" E-Mails, um sich Vertrauen zu erschleichen und eine Offline-Kommunikation in Gang zu setzen – mit dem Ziel, sich eine Zahlung zu ergaunern.

Der Angreifer hatte sich gründlich über jedes Angriffsziel informiert und wusste, wer in dem jeweiligen Büro die Führungskraft war. Dieses Wissen nutzte er für den Impersonifikationsangriff. Antigena Email erkannte die Social Engineering-Versuche und verhinderte, dass die E-Mail an die Empfänger zugestellt wurde. Der Ablauf war wie folgt:

1. Abnormales Thema und Absender erkannt. Der Betreff der E-Mails enthielt den Vornamen des Angriffsopfers und die E-Mail stammte von einer Gmail-Adresse, die keinen Bezug zur üblichen E-Mail-Adresse der Führungskraft hatte. Obwohl keine schädliche Payload (z. B. Links oder Anhänge) vorhanden war, erkannte Antigena Email, dass die E-Mails schädlich waren.

2. Kein Zusammenhang erkennbar. Antigena erkannte die Impersonifikationsversuche nicht nur anhand des „Look-alike"-Domainnamens, sondern auch, weil die E-Mails nicht mit üblichen Verbindungen in Zusammenhang standen. Die Technologie kennt die E-Mail-Umgebung des Unternehmens und konnte vor diesem Hintergrund keine Verbindung zwischen dem Absender und dem Unternehmen erkennen.

3. Offline-Kommunikation verhindert. Antigena setzte diese verschiedenen schwachen Indikatoren in Beziehung und erkannte, dass die E-Mails Komponenten eines einzigen systematischen Angriffs waren. Die Technologie isolierte sie in einem Puffer, damit die Sicherheitsexperten des Unternehmens sie analysieren konnten. Antigena entschied, dass diese Maßnahme in dem betreffenden Fall am sinnvollsten war, und verhinderte damit, dass die für den Angriff ausgewählten Empfänger den Inhalt der E-Mail lesen und die Offline-Kommunikation in Gang setzen.

4. Spoofing erkannt. Antigena Email identifizierte nicht nur die drei Führungskräfte, deren Identität vorgetäuscht wurde, sondern erkannte auch, dass der Angreifer einen Spoof der legitimen externen privaten Adresse ihres CEO nutzte.

5. „Whale Spoofing" erkannt. Darüber hinaus war der Risikowert der Benutzer, deren Identität vorgetäuscht wurde, hoch, was darauf hindeutete, dass sie begehrte Angriffsziele waren und „Whale Spoofing" (Spoofing von wichtigen Personen im Unternehmen) vorlag. Die herkömmlichen E-Mail-Sicherheitstools konnten den Angriff nicht erkennen, weil sie auf statische Analysen zurückgreifen und ihre Möglichkeiten begrenzt sind. Antigena Email hingegen nutzte sein tiefgehendes Verständnis der digitalen Benutzer des Unternehmens und ihrer normalen Verhaltensmuster – die sogenannten „Patterns of Life" –, um die Bedrohung im Posteingang unschädlich zu machen.

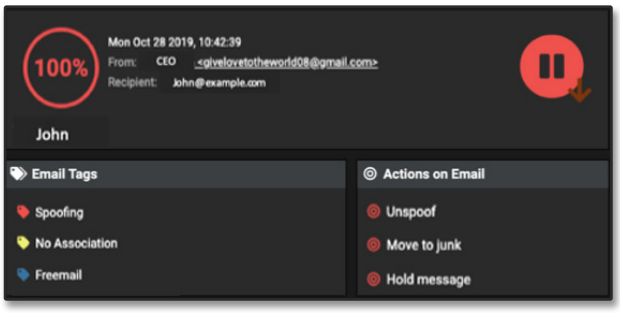

Abbildung 2: Eine von 30 E-Mails, mit einem Anomaliewert von 100%

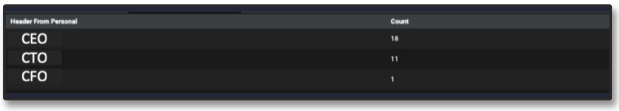

Abbildung 3: Die Modelle, die Antigena Email zum Eingreifen veranlasst haben

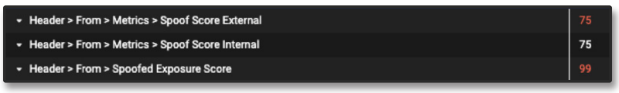

Abbildung 4: Antigena Email erkennt den Spoofing-Versuch