Link-Spoofing-Angriff

Darktrace hat einen Link-Spoofing-Angriff auf ein Finanzinstitut in Atlanta erkannt, bei dem die Empfänger animiert werden sollten, auf einen schädlichen Link zu klicken. Ein Bedrohungsakteur hatte eine ähnliche Domain wie diejenige des Unternehmens, das er angreifen wollte, registriert. Der Firmenname lautete etwas anders, sah aber dennoch aus wie die Echte. Ein Beispiel hierfür wäre es einen Buchstaben im Namen zu ändern, oder einen Bindestrich im Domainnamen hinzuzufügen.

Der Bedrohungsakteur konnte sich in den E-Mail-Austausch einklinken. Sobald einige Nachrichten hin- und hergeschickt worden waren, konnte der Angreifer das aufgebaute Vertrauen nutzen, um eine E-Mail mit einem schädlichen Link zu senden. Beachten Sie in der Abbildung der gespooften E-Mail die falsche Schreibweise des Wortes ‚example'. Diese subtile Abweichung bemerkte der Empfänger nicht und klickte auf den Link. Der Benutzer wurde zu einer sorgfältig nachgeahmten Website mit täuschend ähnlicher Anmeldeseite für Example.org geleitet, wo er seine Zugangsdaten eingegeben hat. Diese können nun vom Angreifer abgegriffen werden, und für das legitime Zahlungssystem genutzt werden.

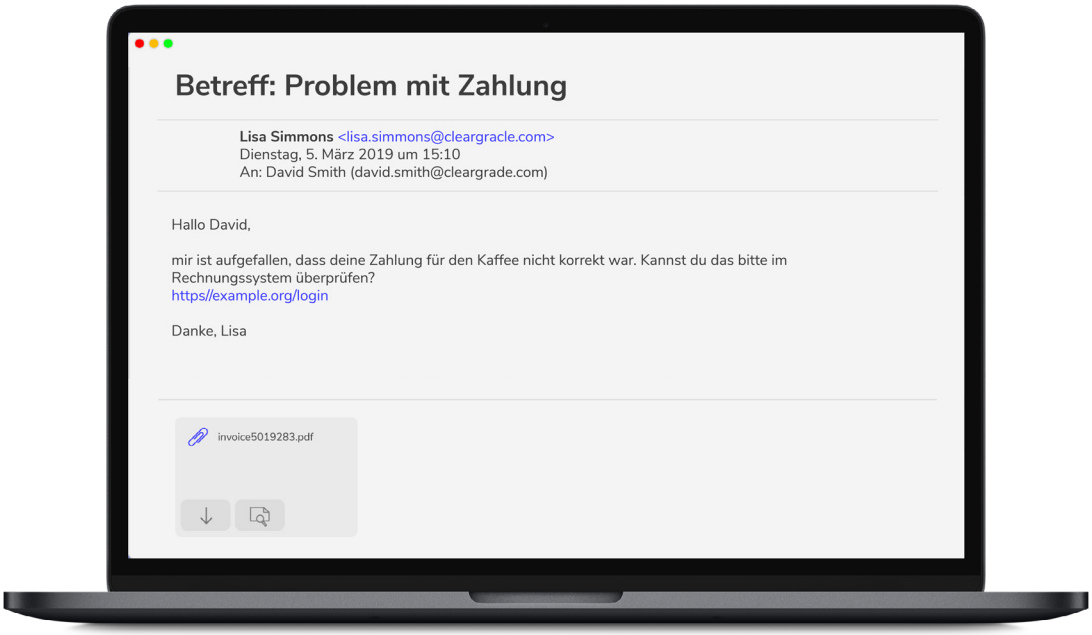

Abbildung 1: Eingehende E-Mail, die einen Link zu einer gespooften Domain enthält.

Stoppen von Link-Spoofing-Angriffen

Im Gegensatz zu anderen Lösungen können Antigena Email und das Immune System Netzwerk-, Cloud- und E-Mail-Daten in Beziehung setzen und auf diese Weise herausfinden, ob mit einem Link verbundene Domains und Absender abnormal sind, die Platzierung eines Links in einer E-Mail ungewöhnlich ist, die Diskussionsthemen und Inhalte unüblich sind oder ob Muster im URL-Pfad verdächtig sind.

Dank dieses einzigartigen Ansatzes kann Darktrace viel genauere Entscheidungen treffen als andere Tools und angemessene, gezielte Maßnahmen ergreifen, um großangelegte Phishing-Angriffe unschädlich zu machen.

Darktrace erkannte nicht nur den Impersonifikationsversuch anhand des „Look-alike"-Domainnamens, sondern auch, dass die E-Mails nicht mit üblichen Verbindungen in Zusammenhang standen – die Technologie kennt die E-Mail- und Netzwerkumgebung des Unternehmens und konnte in diesem Fall keine Verbindung zwischen dem Absender und dem Unternehmen erkennen.

Antigena Email reagierte eigenständig, um die Bedrohung zu neutralizieren, und verwehrte den Zugriff auf den Link. Zusätzlich wurden der Benutzer und das Sicherheitsteam mit einem Warnhinweis-Banner von der potenziellen Bedrohung informiert. Das Darktrace Immune System war darauf vorbereitet, weitere Maßnahmen zu ergreifen, sollte dieser Link an andere Benutzer im Unternehmen geschickt worden sein, um eine Ausbreitung des Angriffs zu verhindern.

Darüber hinaus war der Risikowert der Benutzer, deren Identität vorgetäuscht wurde, hoch, was darauf hindeutete, dass sie begehrte Angriffskomponenten waren und eine Modellabweichung bei „Whale Spoof" (Spoofing von wichtigen Personen im Unternehmen) vorlag. Die KI von Darktrace erkannte, dass wichtige interne Benutzer angegriffen wurden, und priorisierte den Angriff. Die Technologie leitete in Echtzeit angemessene Maßnahmen ein.

Antigena Email: Social Engineering & Solicitation (Beeinflussung)

Bei Angriffen in Form von Social Engineering & Solicitation versuchen getarnte Angreifer ähnlich wie bei einem Impersonifikationsangriff, den Empfänger dazu zu bringen, auf die E-Mail zu antworten, offline zu kommunizieren oder eine Offline-Transaktion vorzunehmen – und geben vor, dass es dringend ist. Ihre Ziele sind ganz unterschiedlich – von Überweisungsbetrug über Industriespionage bis hin zu Diebstahl von geistigem Eigentum. Unternehmen sollten dringend in Sicherheitstraining investieren und ihre Mitarbeiter schulen, damit sie Warnsignale erkennen, dennoch gibt es keinen hundert- prozentigen Schutz vor diesen immer raffinierteren Angriffen.

Während sich bei traditionellen Phishing-Kampagnen in der Regel eine schädliche Payload hinter einem Link oder einem Anhang verbirgt, werden bei Social Engineering-Angriffen häufig reine E-Mail-Nachrichten gesendet, die nur Text enthalten. Diese Angriffe werden von traditionellen Sicherheitstools, die Links und Anhänge mit Blacklists und Signaturen abgleichen, nicht erkannt. Hinzu kommt, dass dieser Angriffsvektor auf neue „Look-alike"-Domains zurückgreift, die den Empfänger nicht nur täuschen, sondern auch traditionelle Sicherheitsmechanismen umgehen.

Antigena Email kennt die „normalen" Verhaltensmuster im E-Mail- und Netzwerkverkehr und passt seine Erkenntnisse laufend an. So lassen sich die subtilsten Versuche einer Beeinflussung erkennen. Reine Text-E-Mails, die traditionelle Sicherheitsmechanismen umgehen, können durch Abgleich mit einer Vielzahl von Indikatoren binnen Sekunden identifiziert werden, darunter verdächtige Ähnlichkeiten mit bekannten Benutzern, abnormale Verbindungen zwischen internen Empfängern und auch Anomalien im Nachrichtentext und Betreff.

Meist wird mit Social Engineering-Angriffen bezweckt, dass schnell eine Offline-Kommunikation stattfindet, sodass die traditionellen reaktiven Sicherheitstools erst eingreifen, wenn bereits Schaden entstanden ist. Antigena Email kennt ganz genau die Verhaltensmuster von jedem Benutzer und Gerät sowie die Beziehungen innerhalb des Unternehmens und kann daher proaktiv und frühzeitig mit hoher Zuverlässigkeit reagieren.

Es gibt zahlreiche Möglichkeiten, wie Antigena Email reagieren kann, unter anderem: Benachrichtigung des Sicherheitsteams, Warnung der E-Mail-Empfänger, indem ein Warnhinweis-Banner an den Inhalt der E-Mail angehängt wird, Umschreiben und Sperren von Links und Zurückhalten von E-Mails. Die Fähigkeit von Antigena, die Reaktion intelligent und eigenständig auf bestimmte Bedrohungsarten abzustimmen, ist einzigartig.

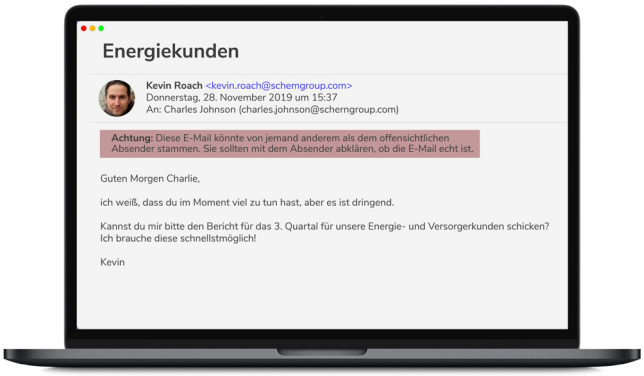

Abbildung 2: Ein Warnhinweis-Banner wird an eine gespoofte eingehende E-Mail angehängt, mit der sensible Unternehmensdokumente angefordert werden.

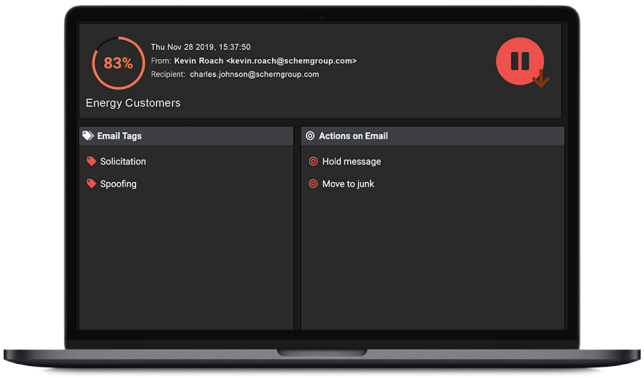

Abbildung 3: Antigena Email stufte die oben stehende E-Mail aufgrund von Hinweisen auf Sollicitation und Spoofing als 83 % anormal ein.

Unternehmensweiter Kontext

Darktrace Antigena Email ist in der Lage verborgene Links und Anhänge in Verbindung mit dem gesamten E-Mail-Verkehr und den normalen „"Lebensmustern" der digitalen Umgebung zu analysieren. Bei Phishing-Angriffen erkennt Darktrace, dass weder der Empfänger noch irgendjemand in der Peer-Group die verdächtige Domain jemals zuvor besucht hat. So kann die Technologie eine Warnmeldung über die erkannte Bedrohung herausgeben und eigenständig gezielte Maßnahmen ergreifen.

Sie untersucht auch, an welcher Stelle in der E-Mail sich die potenziell schädliche Payload befindet, und erkennt zum Beispiel auch, wenn sie sich hinter Schaltflächen verbirgt, die denen auf vertrauenswürdigen Websites ähnlich sind. Darüber hinaus werden Muster in der URL-Adresse untersucht und es erfolgt ein Abgleich mit früheren abgewehrten Angriffen, um verdächtige Links aufzuspüren. Durch Anwendung dieses reichhaltigen Kontextes auf jede ein- und ausgehende E-Mail in Ihrem Unternehmen kann Antigena Email eigenständig intelligente Entscheidungen treffen und in Echtzeit gezielte Maßnahmen ergreifen.

Je nach wahrgenommener Art der Bedrohung gehören dazu das Verkleinern von Anhängen, das Sperren schädlicher Links, sobald sie in das Netzwerk gelangen, und auch ein rückwirkendes Entfernen von E-Mails aus Posteingängen, wenn neue Erkenntnisse gewonnen werden.