

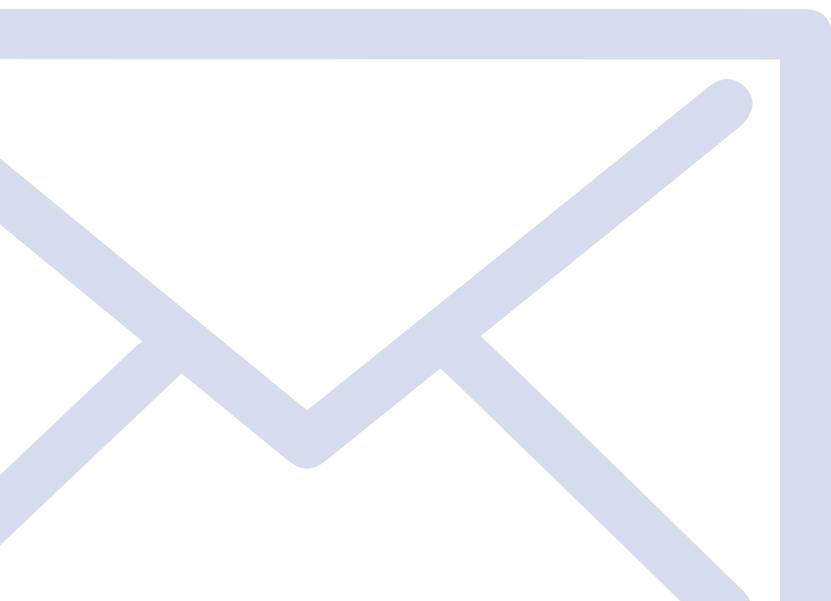


Darktrace Cyber-KI

Ein „Immunsystem“ für E-Mail-Sicherheit

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

– Peter Firstbrook, VP Analyst, Gartner



Einleitung

Bedrohungen im Überblick

Spear Phishing & Payload-Einschleusung	4
WeTransfer-Angriff	6
Versteckte Malware in gefälschten Rechnungen	7
Kompromittierung des Adressenverzeichnisses einer Gemeindeverwaltung	7
Kaperung eines Supply-Chain-Kontos	8
Versteckte Schaddatei auf OneDrive-Seite	13
Social Engineering & Solicitation (Beeinflussung)	14
Impersonation-Angriff	16
Spoofing-Angriff „stellvertretender Finanzvorstand“	17
Kompromittierung von Mitarbeiterzugangsdaten	18
Ungewöhnliche Anmeldung bei einer Bank in Panama	20
Zugriffsversuch aus einer ländlichen Gegend in Japan	20
Kompromittierung und Sabotage eines Office 365-Kontos	21
Automatisierter Brute-Force-Angriff	21

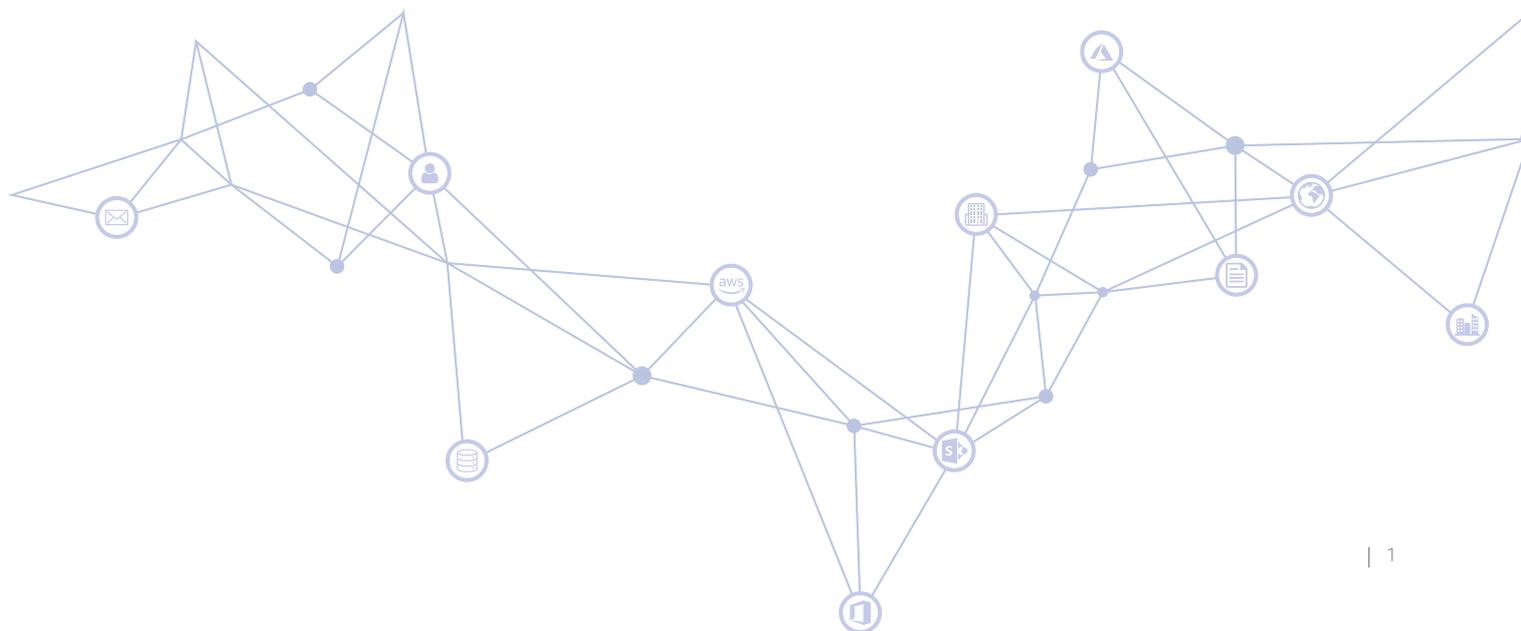
E-Mail- und Kollaboration-Plattformen sind das Fundament der digitalen Infrastruktur jedes Unternehmens. Im digitalen Bereich der Korrespondenz werden Informationen ausgetauscht, Pläne geschmiedet und Allianzen gebildet. E-Mail-Systeme sind ein Medium, welches auf menschlicher Interaktion und Vertrauen beruht – dieser vorweggenommene Vertrauensvorsprung ist die eigentliche Schwachstelle in der Sicherheitsstrategie eines Unternehmens.

Diese Vertrauensvermutung ist grundlegend für Zusammenarbeit und Wachstum, bedeutet aber, dass E-Mail-Systeme sich mehr als jeder andere Bereich des Unternehmens strukturell der „Zero Trust“-Prämisse entziehen. Es überrascht daher kaum, dass 94 % der Cyberbedrohungen immer noch in E-Mails lauern.

Um den Einfluss der menschlichen Fehlbarkeit in diesem Bereich zu minimieren, setzte die Branche auf Technologien, um schädliche E-Mails aufzuspüren, die selbst scharfsinnige und bestens geschulte Mitarbeiter nicht erkennen. Bisher konnten traditionelle Abwehrmechanismen kaum mit den Entwicklungen in der Cyberbedrohungslandschaft mithalten.

Vor allem Spear Phishing, Impersonations-Angriffe und Kontokaperungen stellen nach wie vor lohnende Angriffsmöglichkeiten für Cyberkriminelle dar, die sich ohne großen Aufwand in ein Unternehmen einschleusen wollen. Gezielte E-Mail-Angriffe dieser Art in Verbindung mit den Schwächen traditioneller Abwehrmechanismen stellen eine enorme Herausforderung für Unternehmen dar, auch wenn ihre Sicherheitsstrategien vielschichtig und ausgereift sind.

Peter Firstbrook, VP Analyst bei Gartner, fasst die Marktdynamik treffend zusammen: „Herkömmliche Kontrollmechanismen wie standardisierte reputationsbasierte Anti-Spam-Lösungen und signaturbasierte Virenschutzsysteme sind ausreichend für gängige Angriffe und Scam-Kampagnen, aber nicht für den Schutz vor gezielten, ausgefeilten und hochkomplexen Angriffen. Mehr denn je erfordert moderne E-Mail-Sicherheit Innovation und ein Umdenken, um sich in der schnell veränderlichen Bedrohungslandschaft zu schützen.“



Darktrace KI: Eine Plattform nach dem Vorbild des menschlichen Immunsystems

Im Zuge der Herausbildung von KI für den Unternehmenseinsatz hat dieses „Umdenken“ zur Entwicklung eines Ansatzes für E-Mail-Sicherheit geführt, der an das menschliche Immunsystem angelehnt ist.

Wie Firstbrook so schön sagt, sind traditionelle E-Mail-Schutzmechanismen vielleicht für einfache und unkritische Bedrohungen ausreichend, aber sie können nichts gegen komplexere, personalisierte Angriffe auf bestimmte Empfänger und Unternehmen ausrichten.

Ältere E-Mail-Gateways und native Kontrollmechanismen beruhen auf hartkodierten Regeln und Erkenntnissen über Angriffe aus der Vergangenheit. Ihre Wirksamkeit beschränkt sich daher auf Bedrohungen, die bereits bekannt sind oder die zumindest einfach konstruiert sind, sodass eine statische und binäre Regel anwendbar ist. Aber – und das werden viele Unternehmen aus leidvoller Erfahrung bestätigen – das ist nicht die eigentliche Herausforderung.

Der Paradigmenwechsel in der E-Mail-Sicherheit vollzieht sich im Spannungsfeld zwischen dem „herkömmlichen Ansatz“ nach Firstbrook und einer neuartigen Anwendung von KI für den Unternehmenseinsatz. Das ist fast so wie die Unterscheidung zwischen der „schützenden Haut“ eines Unternehmens und seinem selbstlernenden „Immunsystem“ für Bedrohungen, die den Schutz durchbrochen haben.

Während Ihre schützende Haut alles über Angriffe in der Vergangenheit weiß und bekannte Bedrohungen abwehren kann, kennt Ihr „Immunsystem“ die „normalen Verhaltensmuster“ der digitalen Workflows jedes einzelnen Mitarbeiters. Diese „normalen Verhaltensmuster“ manifestieren sich nicht nur im E-Mail-Verkehr, sondern auch im Netzwerk- und Cloud-Verkehr – und lassen sich für jeden Benutzer zu einem Gesamtbild zusammensetzen, das laufend angepasst wird.

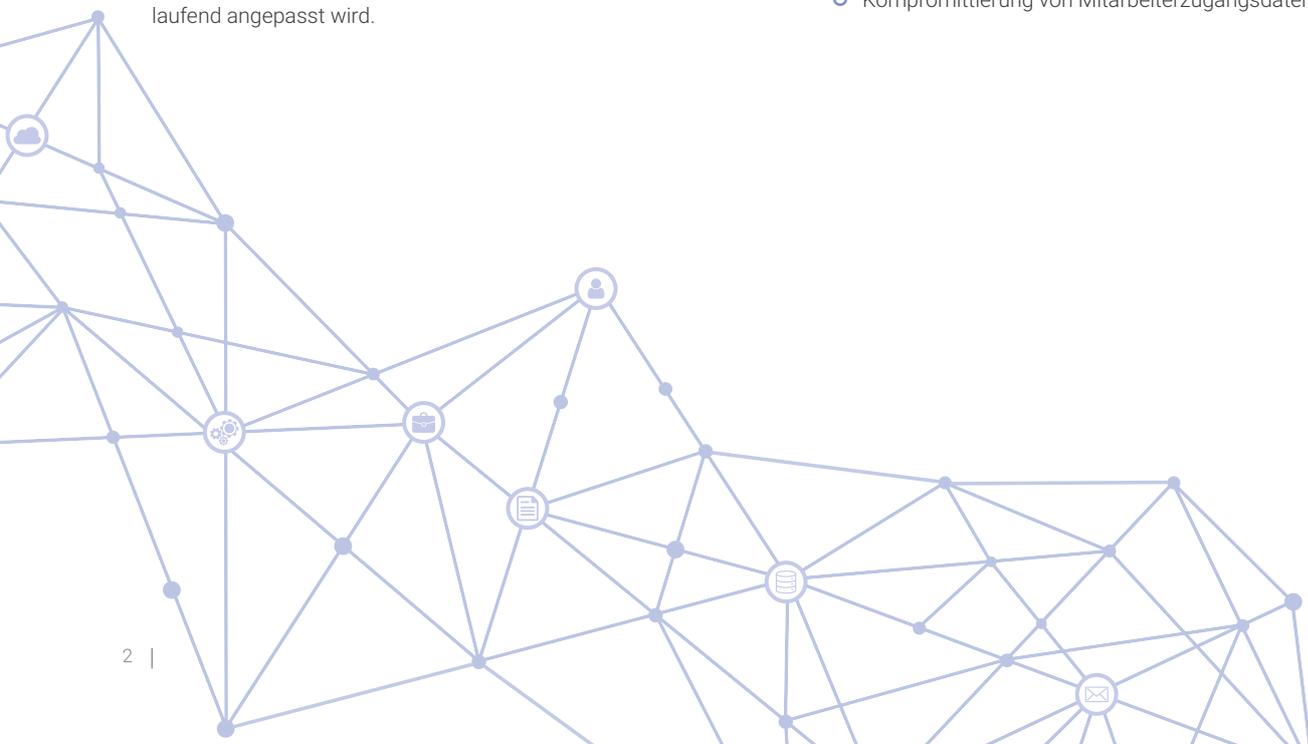
Dieses individuelle unternehmensweite Verständnis des „Normalen“ ermöglicht es Unternehmen, gezielte Angriffe, wie sie heute gang und gäbe sind, abzuwehren. Dieser Ansatz ist als einziger in der Lage, genügend Informationen zu sammeln, um festzustellen, ob subtile Abweichungen im E-Mail-Verkehr tatsächlich schädlich sind.

Unser System für den E-Mail-Schutz ist das erste überhaupt, das hinterfragt, ob es normal ist, dass ein Benutzer eine bestimmte E-Mail erhält. Dabei wird all das berücksichtigt, was das System über die „normalen Verhaltensmuster“ des betreffenden Mitarbeiters, seiner Kollegen und des breiteren Unternehmens weiß – nicht nur im E-Mail-System, sondern auch in der Cloud und im Unternehmensnetzwerk.

Außerdem ist dies der einzige Ansatz, der seine Entscheidungen und Maßnahmen angesichts neuer Erkenntnisse aktualisiert, auch nach Zustellung einer E-Mail. Dabei ist es unerheblich, ob sich diese Erkenntnisse im E-Mail-Verkehr oder in schädlichen Verhaltensweisen im Netzwerk manifestieren.

Mit diesem Whitepaper möchten wir aufzeigen, warum ein Ansatz, der auf zentralen und individuellen Einblicken in Netzwerk-, Cloud- und E-Mail-Verkehr basiert, einen Paradigmenwechsel in der E-Mail-Sicherheit darstellt. Darktrace leistete mit der Entwicklung von Antigena Email und seinem Enterprise Immunsystem Pionierarbeit. Die folgenden Fallstudien lassen sich jeweils einer von vier hochkomplexen Angriffskategorien zuordnen, die regelmäßig Ihre „schützende Haut“ durchdringen, aber von der KI von Darktrace binnen Sekunden unschädlich gemacht werden:

- Spear Phishing & Payload-Einschleusung
- Kaperung eines Supply-Chain-Kontos
- Social Engineering & Solicitation (Beeinflussung)
- Kompromittierung von Mitarbeiterzugangsdaten



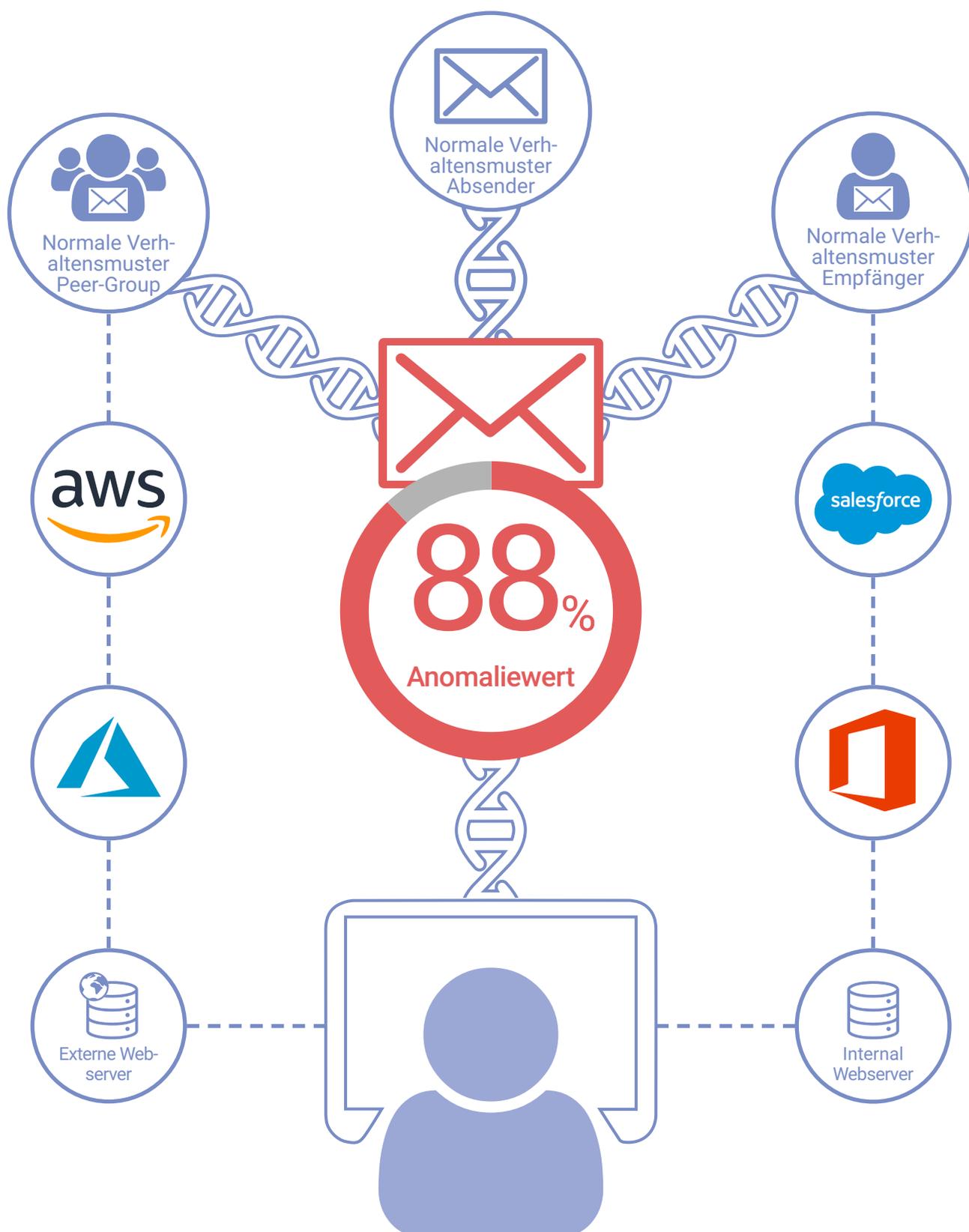


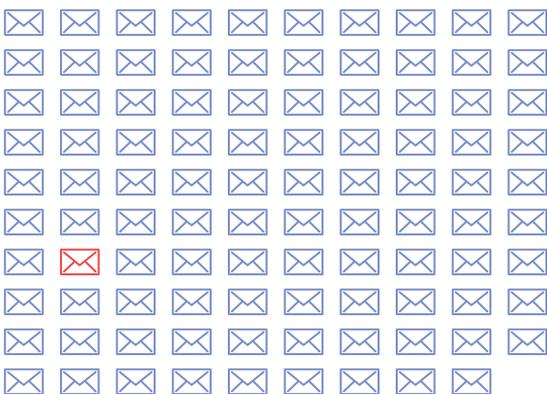
Abbildung 1: Antigena Email ist die einzige Lösung, die E-Mails im Kontext des breiteren Unternehmens analysiert – nicht nur E-Mail-Daten. Dank dieses unternehmensweiten Verständnisses erkennt das System schädliche E-Mails, die sich an traditionellen Abwehrmechanismen vorbeischnuggeln.

Spear Phishing & Payload-Einschleusung

„Antigena Email ist unschlagbar bei der Abwehr von Bedrohungen, weil es die „normalen Verhaltensmuster“ von E-Mail- und Netzwerkverkehr kennt.“

– Head of IT, Entegrus

1 von 99 E-Mails ist ein Phishing-Angriff



Quelle: Avanan



Die meisten Phishing-Kampagnen versuchen, die Benutzer zu verleiten, auf schädliche Links oder Anhänge in einer E-Mail zu klicken. Auf diese Weise sollen Zugangsdaten abgegriffen oder zerstörerische Malware in das Unternehmen eingeschleust werden. Diese Angriffe können entweder wahllose Kampagnen sein, die sich gleich gegen Tausende von Unternehmen richten, oder als Spear Phishing-Angriffe konzipiert sein, die auf einen bestimmten Empfänger oder ein bestimmtes Unternehmen zugeschnitten sind.

Zum Schutz vor Phishing-Kampagnen gehen traditionelle Abwehrsysteme in der Regel so vor, dass sie E-Mails auf Grundlage von Erkenntnissen über frühere Angriffe, Blacklists und Signaturen analysieren. Cyberkriminelle wissen aber um diesen reaktiven Ansatz und sind sehr erfinderisch, was neue Taktiken und Techniken anbelangt, gegen die herkömmliche Sicherheitssysteme nichts ausrichten können.

Solche Angriffe sind ganz neuartig und können daher die traditionellen Abwehrsysteme umgehen. Aber sie sind in hohem Maße anormal für den Benutzer oder das Unternehmen, dem der Angriff gilt – zumindest, wenn die „normalen Verhaltensmuster“ der gesamten digitalen Umgebung berücksichtigt werden. Genau aus diesem einfachen Grund ist es so wichtig, die traditionelle Wissenslücke zwischen dem, was die externe E-Mail-Ebene betrifft, und dem, was das breitere Netzwerk anbelangt, zu schließen – genau das macht die Cyber AI / Immunsystem Technologies Plattform von Darktrace.

Mithilfe von KI analysiert Antigena Email Links, Anhänge, Domains, Text und andere Elemente einer E-Mail und nimmt einen Abgleich mit den „normalen Verhaltensmustern“ in der Cloud und im Netzwerk vor. Dabei wird eine umfassende Konstellation von Datenpunkten in Beziehung gesetzt, sodass augenscheinlich legitime E-Mails als eindeutig schädlich entlarvt werden können.

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

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

Das Immunsystem ist auch in einzigartiger Weise in der Lage, eine Infektion in jeder beliebigen Umgebung zu erkennen und automatisch eine Ursachenanalyse vorzunehmen, um in Erfahrung zu bringen, ob sie über das E-Mail-System eingedrungen ist. Sollte dies der Fall sein, schützt die Lösung sofort alle anderen Mitarbeiter, die ebenfalls Ziel dieses Angriffs sind. Wir nennen das „strategische Autonomous Response“ – gleich beim ersten Betroffenen werden Erkenntnisse gewonnen, die den strategischen Schutz des übrigen Unternehmens ohne menschliche Intervention ermöglichen. Es ist zwar immer noch jemand aus dem Sicherheitsteam nötig, der das Notebook des ersten Betroffenen säubert, aber das ist immer noch besser, als 200 Geräte oder mehr zu säubern.

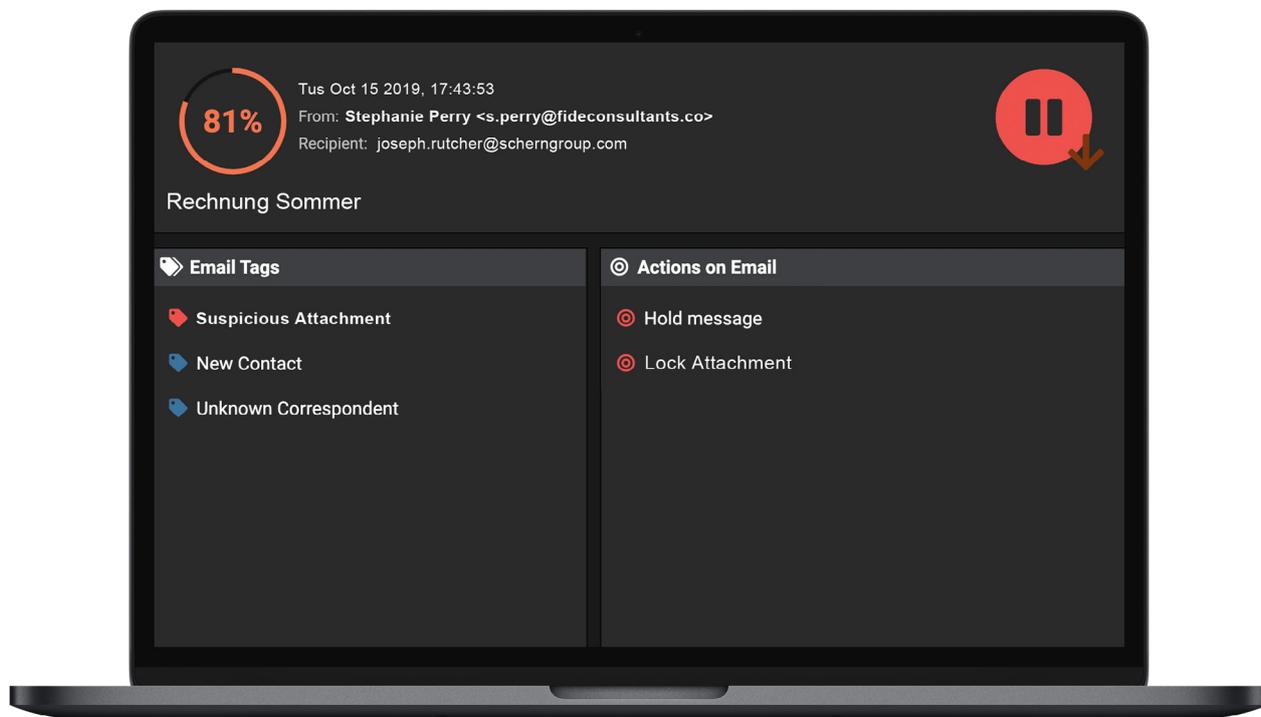
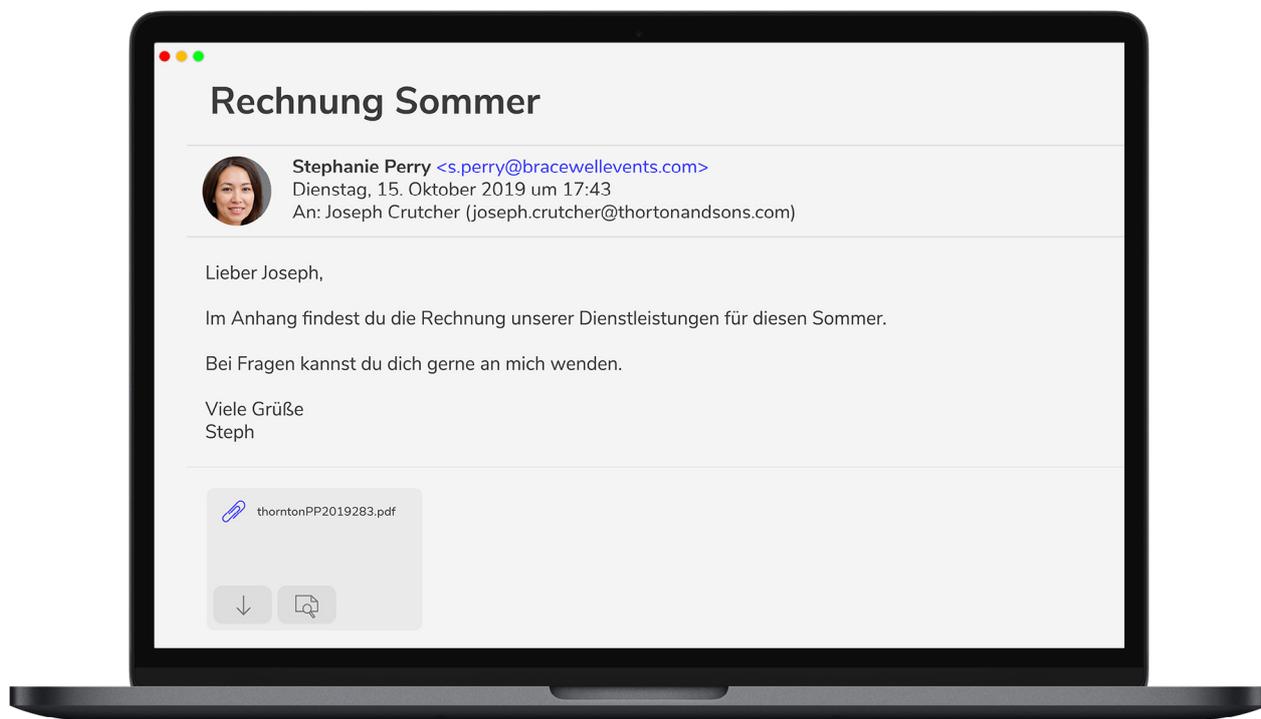


Abbildung 2: E-Mail, in der ein Mitarbeiter verleitet wird, auf einen Anhang mit schädlicher Payload zu klicken, und die entsprechende Ansicht in Darktrace, die die Anomalie Merkmale und die ergriffenen Maßnahmen zeigt.

WeTransfer-Angriff

Darktrace erkannte einen sorgfältig konzipierten Phishing-Angriff auf fünf hochrangige Benutzer eines akademischen Instituts in Singapur, die animiert werden sollten, auf einen schädlichen Link zu klicken.

Antigena Email wies diesen E-Mails einen Anomaliewert von 100 % zu und ergriff die Maßnahme „Zurückhalten“, um eine Zustellung zu verhindern. Es erkannte auch die subtilen Hinweise auf Service-Spoofing, obwohl die Einrichtung eine bekannte Beziehung zum Absender unterhielt.

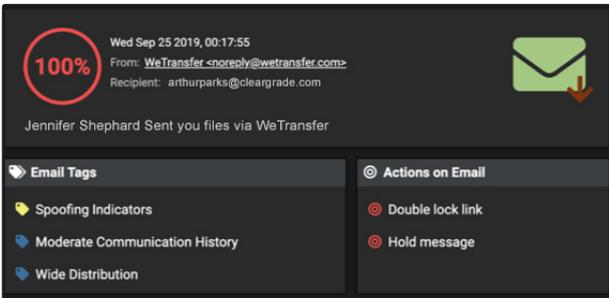


Abbildung 3: Benutzeroberfläche mit Übersicht der Abweichungen von den Modellen und der ergriffenen Maßnahmen

1. An den Headerdaten konnte man nicht erkennen, dass diese E-Mail von einer anderen Quelle als WeTransfer stammte, daher wäre sie dem Empfänger ganz normal vorgekommen. „Width“ und „Depth“ zeigen, dass diese E-Mail-Adresse über mehrere Tage mit vielen Personen in der Einrichtung kommunizierte.

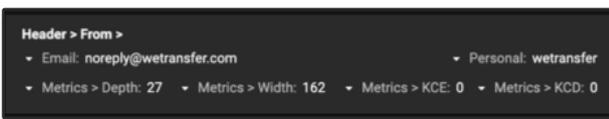


Abbildung 4: Verbindungsdaten der betreffenden E-Mails

2. Antigena Email stellte jedoch beim Abgleich mit den „normalen“ Verhaltensmustern des Geräts und der Einrichtung, sowie unter Berücksichtigung des aus der Netzwerkebene gewonnenen Kontexts, eine Reihe subtiler Anomalien fest.

a. Anfangs war der Anomaliewert der IP-Adresse hoch (63 %). Dieser Indikator gibt an, wie ungewöhnlich es im Vergleich zu den bisherigen Mustern ist, dass die betreffende E-Mail-Adresse von dieser IP aus E-Mails sendet, und ist typischerweise ein Hinweis auf ein gespooftes oder gekapertes Konto.

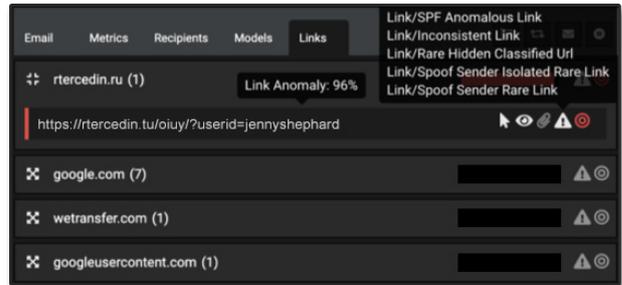


Abbildung 5: Aufschlüsselung der in den E-Mails enthaltenen Links

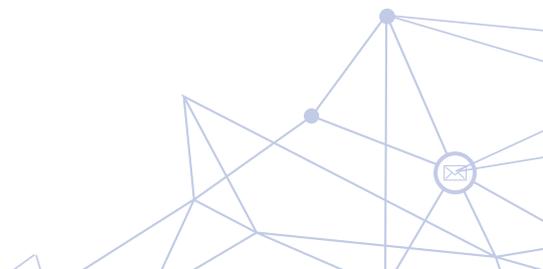
b. Da Darktrace laufend das „normale“ Verhalten für jeden externen Absender modelliert, konnte das System eine entscheidende Anomalie im Textteil der E-Mail feststellen – einen Link, der in hohem Maße von dem Verhalten abwich, das Darktrace bei WeTransfer bisher beobachtet hatte. So konnte Antigena Email den Link als schädliche Payload in der E-Mail identifizieren.



Abbildung 6: Antigena konnte feststellen, an welcher Stelle in der E-Mail der Link platziert war

c. Dem betreffenden Link wurde ein Anomaliewert von 96 % zugewiesen. Der Link verbarg sich hinter „Hier klicken“-Schaltflächen in verschiedenen Teilen der E-Mail, darunter ein gefälschter „https://wetransfer.com/...“-Link (unten abgebildet) und im Text „Inquiry Sheet.xls“ und „Get Your Files“.

Dieser Angriff war völlig neuartig und wurde von keinem der signaturbasierten Tools erkannt, welche die Universität installiert hatte. Da der Link eine völlig legitime Domain verwendete und nicht zu einer offensichtlich schädlichen Payload führte, wären vermutlich auch die heuristische Erkennung und Sandboxing gescheitert.



Versteckte Malware in gefälschten Rechnungen

Eine große Anwaltskanzlei war eines der Hauptziele einer raffinierten Phishing-Kampagne, bei der Malware – mit der Zugangsdaten abgegriffen werden sollten – in ISO-Dateien versteckt war, welche an gefälschte Rechnungen angehängt waren. Die traditionellen Tools für den Schutz von E-Mail-Systemen setzen ISO-Dateien in der Regel auf eine Whitelist und die Betriebssysteme mounten automatisch ihre Images, sobald geklickt wird. Somit sind sie für Bedrohungsakteure sehr interessant.

Während der traditionelle E-Mail-Schutz der Kanzlei die E-Mails durchließ, wehrte Darktrace die Kampagne ab, weil die Technologie eine ganze Reihe anormaler Indikatoren feststellte. Eines der KI-Modelle zum Beispiel, das durch die E-Mails ausgelöst wurde, war „Anhang/Unerwünschte anormale MIME“. Das heißt, der MIME-Typ des Anhangs war für den Benutzer und seine Peer-Group äußerst ungewöhnlich und der Empfänger hatte zuvor keinen Kontakt mit dem Absender und demnach auch keine Datei angefordert.

Da Darktrace die Herkunft der Bedrohung genau bestimmen konnte, ergriff das System gezielte, „minimal-invasive“ Maßnahmen zur Neutralisierung, anstatt einfach nur alle potenziell verdächtigen E-Mails mit generischen Warnungen zu versehen, die vermutlich ignoriert worden wären. Um die schädlichen ISO-Dateien unschädlich zu machen, konvertierte Darktrace die Anhänge in harmlose PDFs und verschob die E-Mails in den Spam-Ordner. Und das Entscheidende war: Nachdem die erste E-Mail der Kampagne entdeckt worden war, neutralisierte die Technologie sofort automatisch 20 weitere, bevor sie dem Unternehmen hätten schaden können.

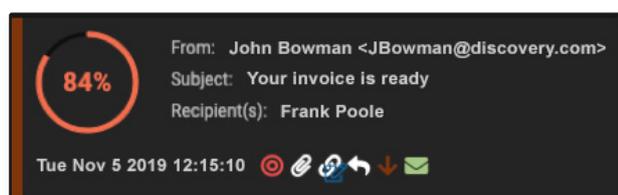


Abbildung 7: Header der schädlichen E-Mails mit vorgeschlagener Maßnahme

Kompromittierung des Adressenverzeichnisses einer Gemeindeverwaltung

Einem Bedrohungsakteur gelang es, das Adressenverzeichnis einer Gemeindeverwaltung in den USA zu beschaffen, und startete einen Angriff in alphabetischer Reihenfolge von A bis Z. Jede E-Mail war an den jeweiligen Empfänger angepasst und die Nachrichten enthielten allesamt eine schädliche Payload. Diese verbarg sich hinter einer Schaltfläche, die als Link zu Netflix, Amazon oder anderen vertrauenswürdigen Diensten getarnt war.

Als die erste E-Mail eintraf, erkannte Darktrace sofort, dass weder der Empfänger noch eine andere Person in seiner Peer-Group noch irgendein anderer Mitarbeiter der Stadtverwaltung diese Domain jemals zuvor besucht hatte. Das System erkannte auch, dass die Art und Weise, wie die Links hinter der Schaltfläche verborgen waren, äußerst verdächtig war. Es gab sofort eine Warnmeldung über die zuverlässig erkannte Bedrohung heraus und schlug eine eigenständige Blockierung jedes Links vor, der in das Netzwerk gelangte.

Antigena wurde von der Stadtverwaltung im „Passive Mode“ genutzt und konnte eindrucksvoll unter Beweis stellen, dass es selbst in diesem Modus in der Lage ist, subtile Angriffe aufzudecken, die andere Tools nicht bemerken: Während Antigena die Kampagne bereits beim Buchstaben „A“ erkannte und unschädlich machte, wurden die Legacy-Tools des Sicherheitsteams erst bei „R“ auf die Bedrohung aufmerksam. Im „Active Mode“ hätte Antigena den Angriff neutralisiert, noch bevor er überhaupt einen Benutzer erreicht hätte.

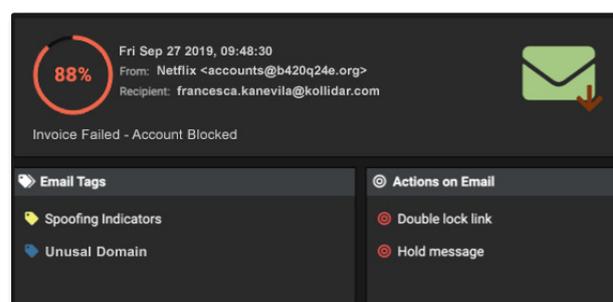
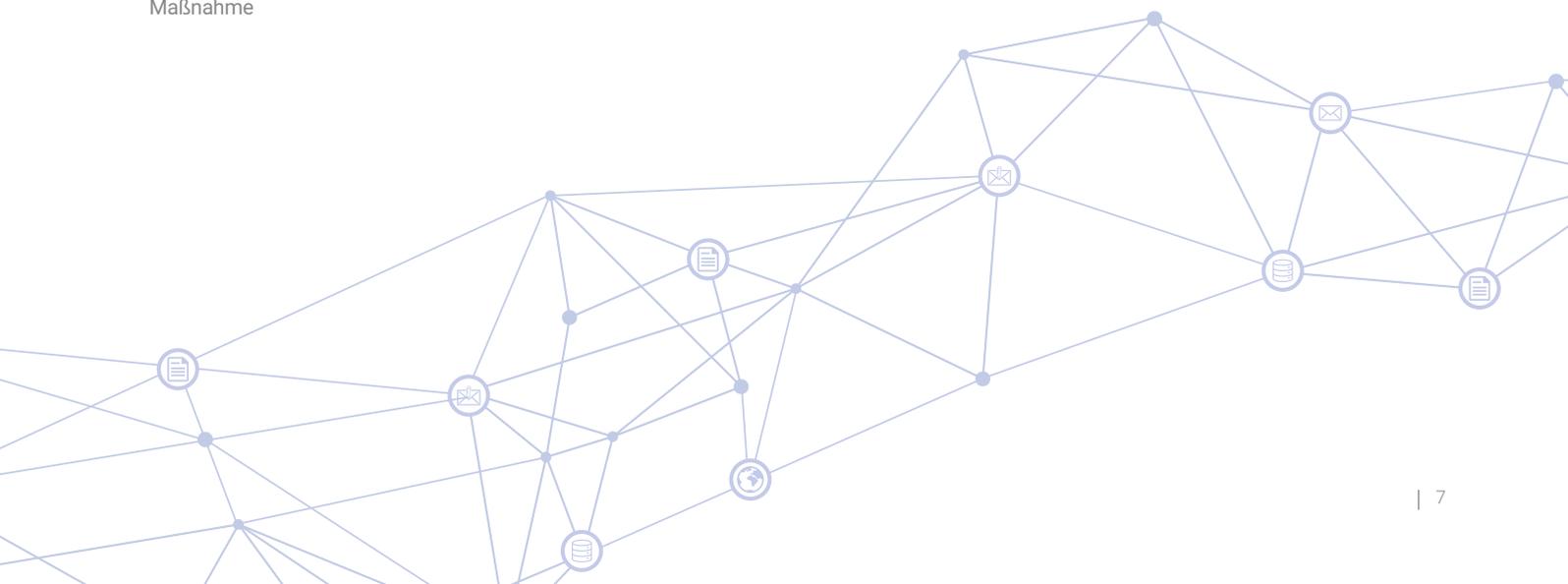
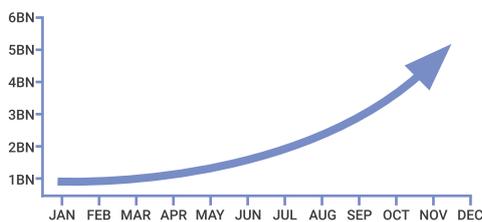


Abbildung 8: Antigena Email zeigt Anomaliewert von 88 %



Kaperung eines Supply-Chain-Kontos

Verluste durch Kontokaperungen haben sich im vergangenen Jahr auf 5,1 Mrd. US-Dollar mehr als verdreifacht



Quelle: Javelin

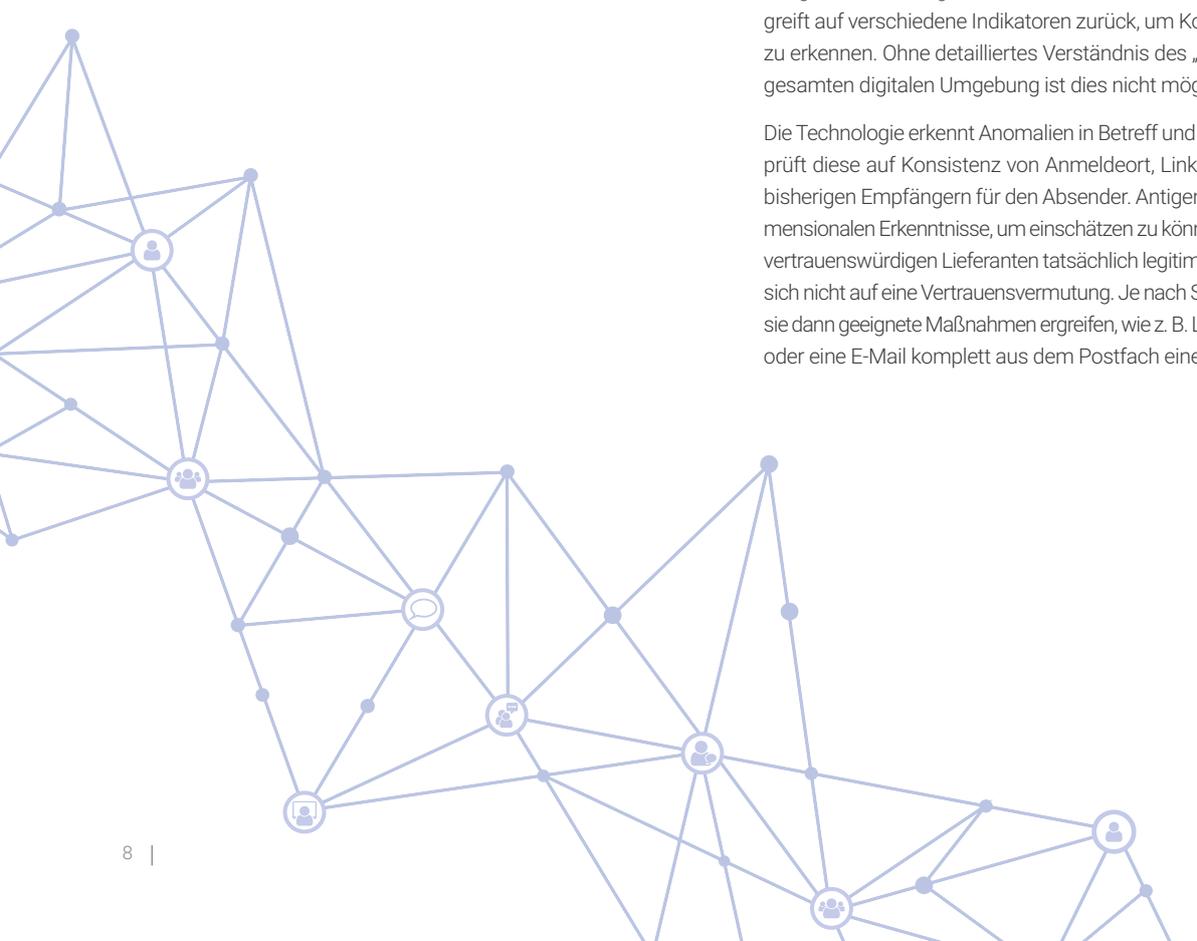
Indem sie die Kontodaten eines vertrauenswürdigen Kontakts in der Lieferkette eines Unternehmens kapern, können Bedrohungsakteure leicht das Vertrauen eines Empfängers im Netzwerk gewinnen und dazu bringen, auf einen schädlichen Link zu klicken oder Gelder in Millionenhöhe aus dem Unternehmen zu transferieren. Ältere Systeme für E-Mail-Schutz basieren auf einer Vertrauensvermutung, mit der Konsequenz, dass ausgeklügelte Kontokaperungen oft nicht bemerkt werden.

In den letzten Jahren waren kompromittierte Konten Auslöser für einige spektakuläre Angriffe auf große Unternehmen. Cyberkriminelle machen sich für ihre Angriffe zunehmend Lieferketten – Lieferanten, Partner und Vertragsnehmer – zunutze, um ein Unternehmen zu infiltrieren oder Offline-Kommunikation in Gang zu setzen. Anfang des Jahres wurde ein Bericht zum sogenannten „Island Hopping“ veröffentlicht, bei dem Angreifer ganze Lieferketten in ihre Gewalt bringen. Dieser Methode ist mittlerweile die Hälfte der heutigen Angriffe zuzurechnen.

Angreifer, die vollen Zugriff auf das E-Mail-Konto eines Lieferanten haben, können den bisherigen E-Mail-Verkehr einsehen und eine gezielte Antwort auf die letzte Nachricht schicken. Die verwendete Sprache ist meist unauffällig, sodass traditionelle Tools für E-Mail-Sicherheit, die nach Schlüsselbegriffen oder -phrasen suchen, welche auf Phishing hindeuten, diese Angriffe nicht erkennen.

Antigena Email kann für jeden internen Benutzer genau beschreiben, wie dessen normale Verhaltensmuster aussehen, und erkennt daher ungewöhnliche Verteilungen von Wörtern und Sätzen, auch wenn die Formulierungen einem Außenstehenden – egal ob Mensch oder Maschine – noch so plausibel erscheinen. Bei der Analyse von Kommunikationsmustern berücksichtigt Antigena Email den gesamten Kontext allen E-Mail- und Netzwerkverkehrs und greift auf verschiedene Indikatoren zurück, um Kontokaperungen zuverlässig zu erkennen. Ohne detailliertes Verständnis des „normalen“ Verhaltens in der gesamten digitalen Umgebung ist dies nicht möglich.

Die Technologie erkennt Anomalien in Betreff und Inhalt jeder E-Mail und überprüft diese auf Konsistenz von Anmeldeort, Links und Anhängen sowie den bisherigen Empfängern für den Absender. Antigena Email nutzt diese mehrdimensionalen Erkenntnisse, um einschätzen zu können, ob eine E-Mail von einem vertrauenswürdigen Lieferanten tatsächlich legitim ist. Die Technologie verlässt sich nicht auf eine Vertrauensvermutung. Je nach Schwere der Bedrohung kann sie dann geeignete Maßnahmen ergreifen, wie z. B. Links und Anhänge blockieren oder eine E-Mail komplett aus dem Postfach eines Mitarbeiters entfernen.



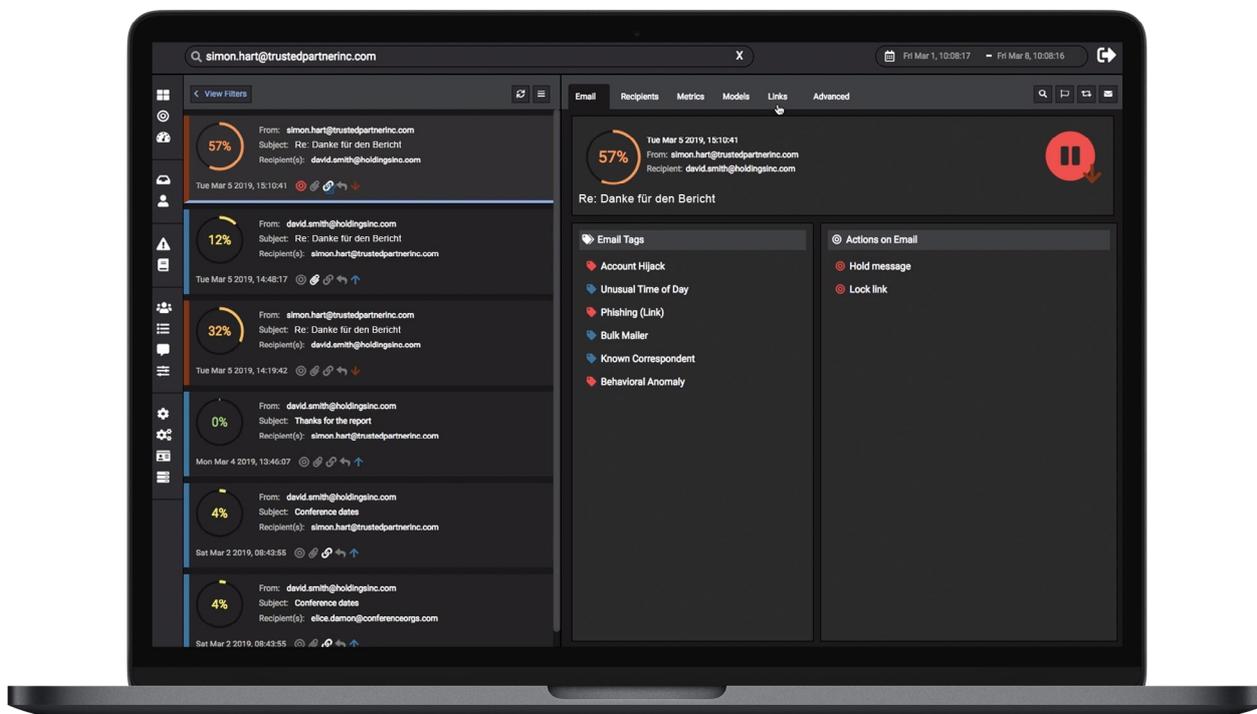


Abbildung 9: Eine plausible Antwort, gesendet von einem kompromittierten Konto eines vertrauenswürdigen Lieferanten, nachdem der Verlauf der E-Mail-Korrespondenz verfolgt worden war. Der Link enthielt eine schädliche Payload.

Anschließende Supply-Chain-Angriffe

Bei einem Kunden, der Antigena Email testweise installiert hatte, ereigneten sich binnen weniger Tage zwei schwerwiegende Vorfälle, bei denen die E-Mail-Konten vertrauenswürdiger Lieferanten für eine schädliche Kampagne missbraucht wurden – sehr wahrscheinlich, nachdem diese Konten kompromittiert worden waren.

„Antigena Email war noch nicht so konfiguriert, dass die Technologie eigenständig Maßnahmen ergreift, daher waren die Benutzer nicht vor dem Inhalt der E-Mails geschützt. Aber Antigena Email informierte darüber, dass es die E-Mails zurückgehalten und die Link-Payloads doppelt blockiert hätte – die integrierten Sicherheitstools von Microsoft erkannten nichts Verdächtiges und ließen alle E-Mails durch.“

Vorfall 1 – Beratungsfirma

Im ersten Fall erkannte Antigena Email, dass der Absender dem Unternehmen bekannt war, weil einige interne Benutzer bereits direkt mit ihm kommuniziert hatten. Es war sogar so, dass diese Benutzer an dem betreffenden Tag ganz normal über das Konto kommuniziert hatten, das später gekapert werden sollte. Der betreffende Dienstleister war eine in Großbritannien ansässige Umweltberatungsfirma.

Nicht einmal zwei Stunden nach diesem regulären E-Mail-Austausch wurden zeitgleich E-Mails an 39 Benutzer gesendet, die jeweils einen Phishing-Link enthielten. Der Betreff und die in der E-Mail enthaltenen Links waren individuell angepasst, was darauf hindeutete, dass der Angreifer gut vorbereitet war und die E-Mails ganz gezielt personalisiert hatte. Die Links hätten dazu dienen können, Zahlungen anzufordern, Kennwörter abzugreifen oder Malware zu installieren.

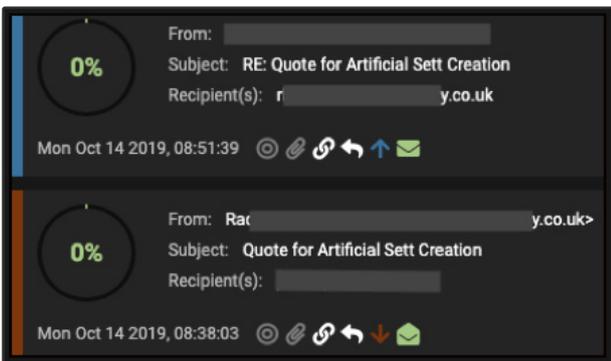


Abbildung 10: Frühere „normale“ Korrespondenz mit dem Absender – mit einem Anomaliewert von 0 %

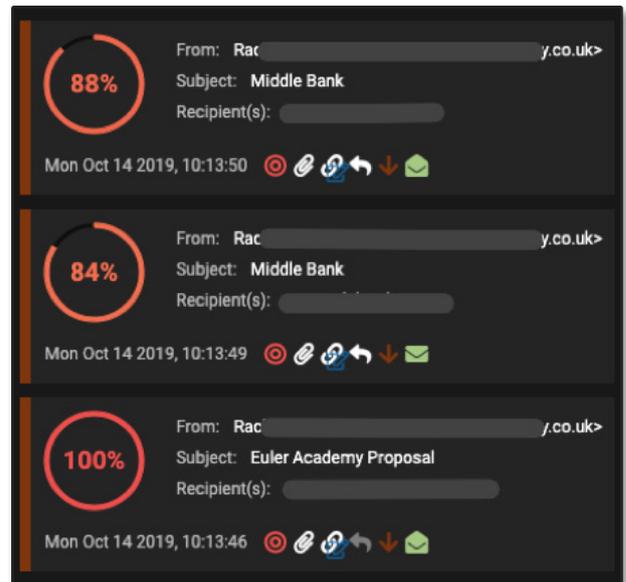


Abbildung 11: E-Mails, die am selben Tag zu einem späteren Zeitpunkt gesendet wurden und schädliche Anhänge enthielten



Antigena Email erkannte alle Warnzeichen, die typischerweise auf eine Kaperung von Supply-Chain-Konten hindeuten:

1. Ungewöhnlicher Ort der Anmeldung: Antigena Email stellte fest, dass die E-Mails von einem echten Outlook Webserver aus gesendet wurden. Das war an sich nichts Ungewöhnliches bei dem Dienstleister, aber aus den Verbindungsdaten ließ sich die geolokalisierte IP-Adresse herauslesen – dabei stellte sich heraus, dass der Angreifer sich über eine IP in den USA angemeldet hatte und nicht wie sonst in Großbritannien.

2. Link-Inkonsistenz: Die in den E-Mails enthaltenen Phishing-Links wurden alle auf der Microsoft Azure Entwicklerplattform gehostet – vermutlich, um die Reputationsprüfungen auf der Host-Domain zu umgehen. Trotz der allgemein angenommenen Legitimität von azurewebsites.net im Web erkannte Antigena Email, dass diese Domain basierend auf dem bisherigen Kommunikationsverlauf sehr unüblich für den Absender war. Die Subdomain war zudem so ungewöhnlich, dass dem Hostnamen im Kontext des sonst üblichen Netzwerkverkehrs des Unternehmens der höchste Ungewöhnlichkeitswert zugewiesen wurde. Da andere Produkte für E-Mail-Sicherheit nicht auf solche kontextbezogenen Daten zurückgreifen, wären sie unmöglich zu diesem Schluss gelangt.

3. Ungewöhnliche Empfänger: Es gibt einen Anomaliewert für „Assoziation“, der Auskunft darüber gibt, wie wahrscheinlich es ist, dass diese Empfängergruppe eine E-Mail von derselben Quelle erhält. Da Antigena Email seine Analysen sukzessive mit Kontext anreichert, konnte die Technologie bereits bei der dritten E-Mail erkennen, dass diese Empfängergruppe 100 % anomal war.

Property	Value
Usage > Darktrace Host Rarity	100
Usage > Domain External User Hostnames	0
Usage > Domain Inconsistency Score	88

Abbildung 12: Indikatoren, die durch den ungewöhnlichen Charakter und die Inkonsistenz des Links ausgelöst wurden

4. Themen-Anomalie: Die Betreffzeilen dieser E-Mails sind unauffällig und professionell formuliert, sodass signaturbasierte Tools keine Schlüsselbegriffe finden würden, die auf einen Phishing-Angriff hindeuten. Antigena Email hingegen erkannte, dass diese Empfänger in der Regel keine E-Mails mit geschäftlichen Angeboten in diesem Schreibstil erhalten.

Property	Value
Recipient > Metrics > Association Anomaly	100

Abbildung 13: Antigena Email erkannte schnell, dass es keine enge Verbindung zwischen den Empfängern dieser Gruppe gab

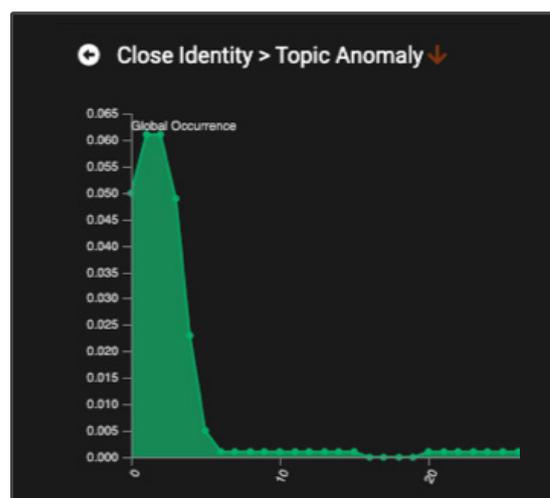
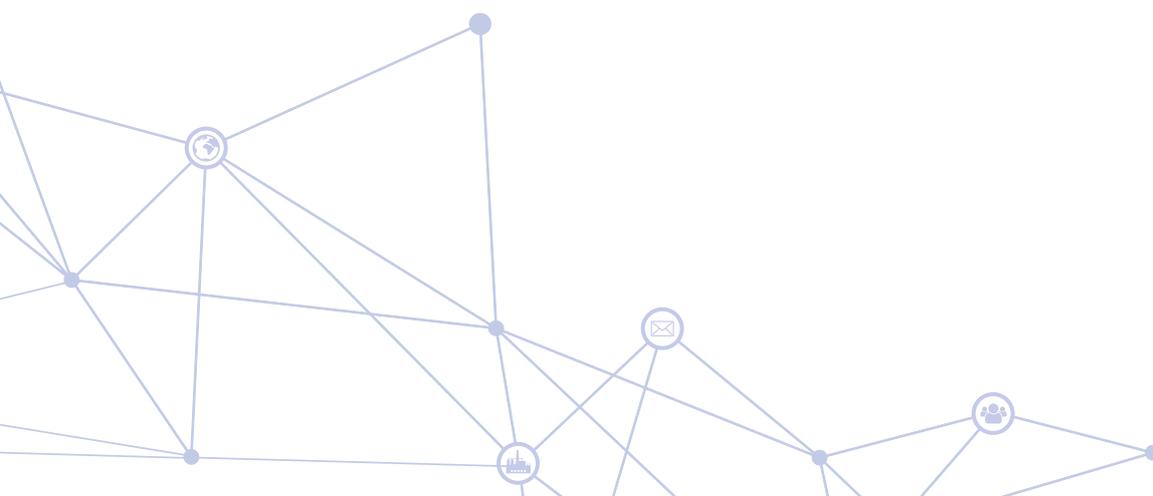


Abbildung 14: Übersicht zum Indikator „Themen-Anomalie“



Vorfall 2 – Kompromittierter SaaS-Anbieter

Bei einem zweiten Angriff am nächsten Tag wurden E-Mails von einem SaaS-Anbieter, der dem Unternehmen bekannt war, an 55 interne Benutzer gesendet. Da Microsoft keine Maßnahmen ergriff, wurden über 50 % dieser E-Mails von den Empfängern gelesen. Antigena Email empfahl, diese E-Mails zurückzuhalten, damit sie gar nicht erst in die Posteingänge gelangen.

1. Auch hier wurden die E-Mails von einem kompromittierten Konto aus gesendet und enthielten jeweils einen schädlichen Phishing-Link. In diesem Fall jedoch blieb der Link länger aktiv, sodass eine genaue Rekonstruktion dessen, was die Benutzer erwartet hätte, möglich war.

2. Zum Glück konnten dank des Zusammenspiels von Antigena Email und dem Darktrace Immunsystem im Netzwerk diejenigen Mitarbeiter, die mit der E-Mail interagiert hatten, leicht auffindig gemacht und die Sicherheit der Konten wiederhergestellt werden. Das Immunsystem konnte auch sehen, dass sich Geräte im physischen Netzwerk mit dem Phishing-Host verbanden. Da das Immunsystem synchron mit Antigena Email arbeitet, brachte es diese Interaktionen mit verdächtigen Phishing-Domains im Netzwerk in Verbindung.

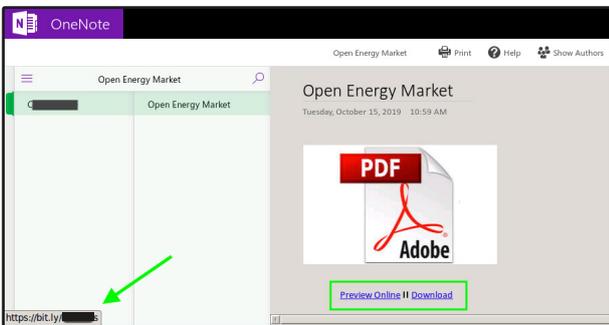


Abbildung 15: Screenshot mit verborgenem Link

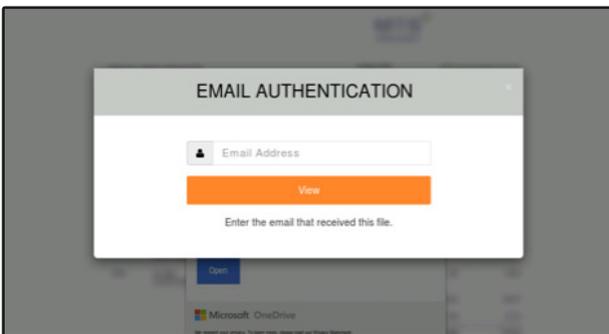


Abbildung 16: Daraufhin wurde er zu einem Formular geleitet, mit dem seine Zugangsdaten abgegriffen wurden

3. Obwohl die Links in Microsoft ATP-sichere Links eingebettet waren (was bedeutet, dass Microsoft eine Echtzeitüberprüfung der Links vorgenommen hätte, wären diese vom Benutzer angeklickt worden), machte die Tatsache, dass Verbindungen zu den tatsächlichen Endpoints im Netzwerkverkehr aufgebaut wurden, deutlich, dass Microsoft anhand der damals zur Verfügung stehenden Informationen davon ausging, dass die Links sicher waren – damit waren die Benutzer dem schädlichen Endpoint ausgesetzt.

4. Der Link an sich wurde auf der bekannten File-Sharing-Plattform SharePoint gehostet. Beim Anklicken des Links wurde der Benutzer zu einem Dokument geleitet, das als Bericht über den Energiemarkt getarnt war. Eine Schaltfläche jedoch, die den Benutzer zum Download der Datei aufforderte, leitete den Benutzer zu einer anderen überzeugenden Webseite weiter, die eingerichtet worden war, um E-Mail-Adresse und Kennwort des Benutzers abzugreifen – damit war er dem Angreifer ausgeliefert.

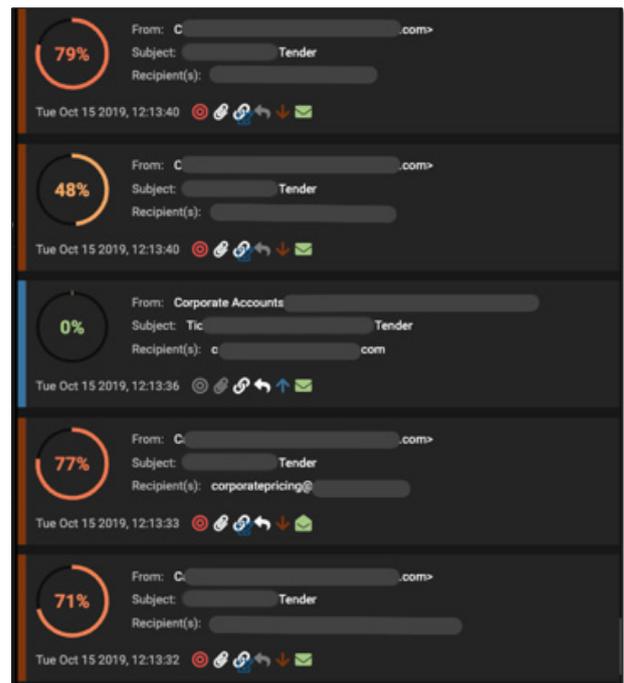


Abbildung 17: E-Mails von Vorfall 2, wie sie in der Antigena Email-Konsole angezeigt wurden, einschließlich derjenigen, die als Antwort darauf gesendet wurden. Es ist zu sehen, dass der „Corporate Accounts“-Benutzer die E-Mail bestätigt hat, indem er ein Ticket geöffnet hat.

Versteckte Schaddatei auf OneDrive-Seite

Ein raffinierter Bedrohungsakteur kaperte das E-Mail-Konto eines Lieferanten einer großen Hotelgruppe und nutzte das vertrauenswürdige Konto, um eine schädliche Payload in das Unternehmen einzuschleusen. Der Angriff konnte die traditionellen Sicherheitstools des Unternehmens umgehen, wurde aber binnen Sekunden von Antigena Email unschädlich gemacht.

1. Aus Analysen früherer E-Mails schloss Antigena Email, dass es eine Verbindung zwischen den beiden Absendern gab.

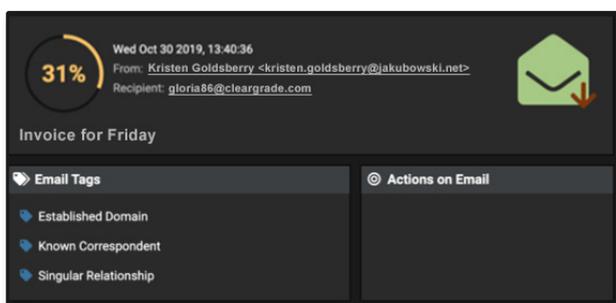


Abbildung 18: Beispiel für bisherigen Nachrichtenverlauf

2. Eine spätere E-Mail wurde als äußerst anormal gegenüber den bisherigen Kommunikationsmustern des Absenders gekennzeichnet.

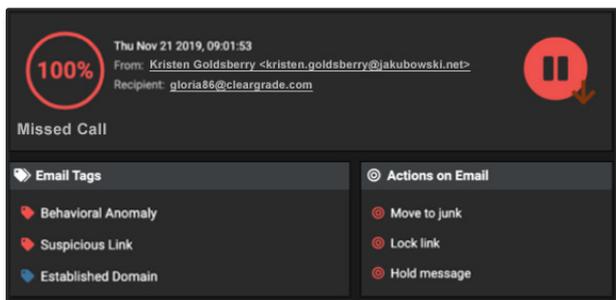


Abbildung 19: Getaggte spätere E-Mail und drei Modellabweichungen

3. Wie wir sehen können, wurden diese E-Mails alle mit dem Merkmal „Verhaltensanomalie“ getaggt und Antigena Email entschied, dass die beste Maßnahme darin besteht, diese E-Mails zurückzuhalten und nicht an die Empfänger zuzustellen.

4. Antigena Email erkannte mehrere Abweichungen vom normalen „Verhaltensmuster“ des externen Absenders, darunter „Anormales Ursprungsland“ und „Anormale Quell-IP-Adresse“.

5. Der schädliche Link in der E-Mail war zudem in hohem Maße inkonsistent mit den „Verhaltensmustern“ des Unternehmens im E-Mail- und Netzwerkverkehr und wurde daher von Antigena Email blockiert.

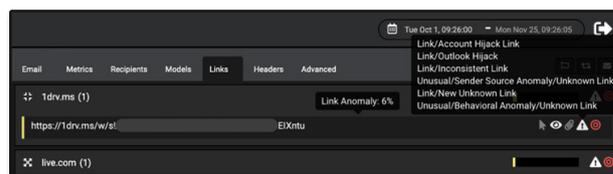
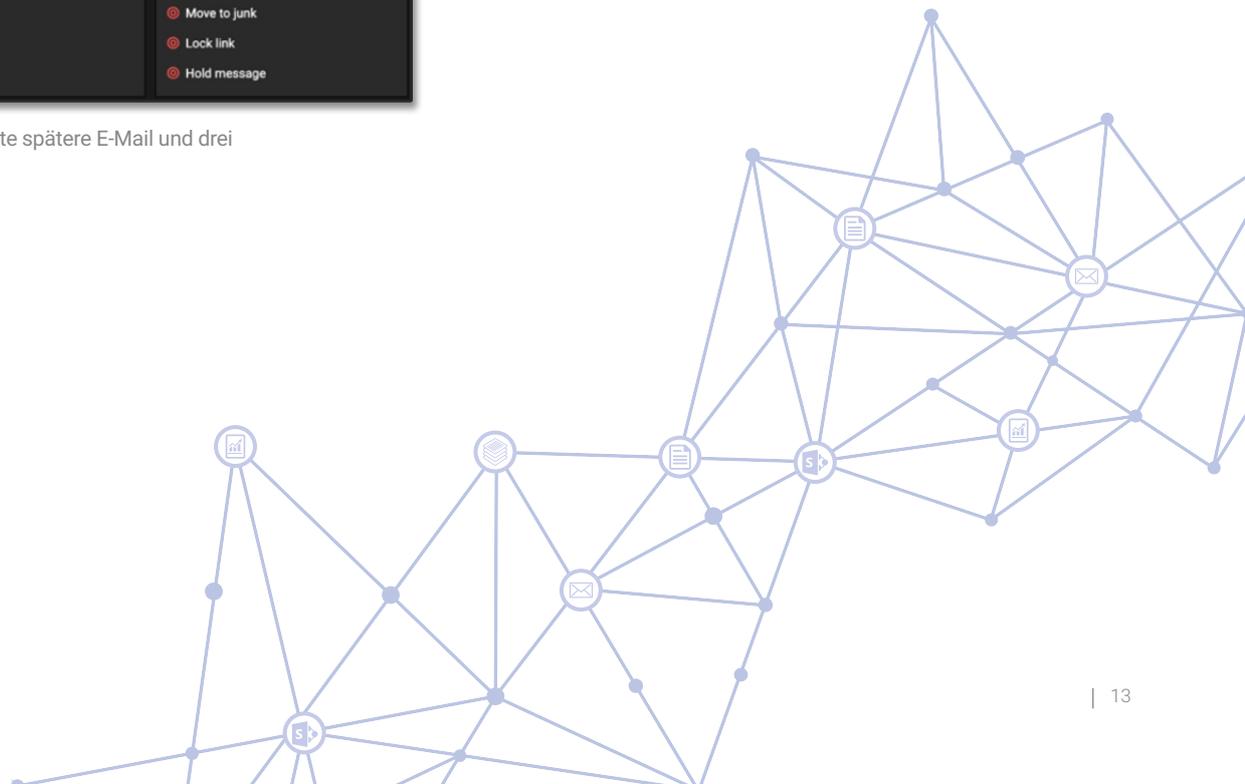


Abbildung 20: Schädlicher Link identifiziert

6. Der Link selbst verbarg sich hinter dem angezeigten Text „Retrieve Message“ und führt zu einer OneDrive-Seite. Die Verwendung von Dateispeicher-Domains für das Hosting von schädlichem Content ist mit einem traditionellen Ansatz nur schwer festzustellen, da Dienste wie SharePoint nicht auf die Blacklist gesetzt werden können. Um feststellen zu können, ob ein Link wie dieser schädlich oder unschädlich ist, muss die E-Mail im Kontext des breiteren Unternehmens beurteilt werden.



Social Engineering & Solicitation (Beeinflussung)

„ Wir haben Antigena Email zusätzlich zu traditionellen Sicherheitstools installiert. Wir waren schockiert, was die traditionellen Tools alles nicht erkannten, im Gegensatz zu Antigena Email. “

– CTO, Bunim Murray Productions



98%
der Angriffe auf
Posteingänge der
Benutzer enthielten keine
Malware

Bei Angriffen in Form von Social Engineering & Solicitation versuchen getarnte Angreifer ähnlich wie bei einem Impersonation-Angriff, den Empfänger dazu zu bringen, auf die E-Mail zu antworten, offline zu kommunizieren oder eine Offline-Transaktion vorzunehmen – und sie geben vor, dass die Sache 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 hundertprozentigen 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.

Einzigartig ist auch die Fähigkeit von Antigena, die Response intelligent auf bestimmte Bedrohungsarten abzustimmen. Die Technologie weiß, dass das „gefährliche“ Element bei einem Solicitation-Angriff oftmals der Inhalt der E-Mail selbst ist, und verhindert die Zustellung, bevor der Empfänger überhaupt die Möglichkeit hat, der dringenden Aufforderung des Angreifers Folge zu leisten.

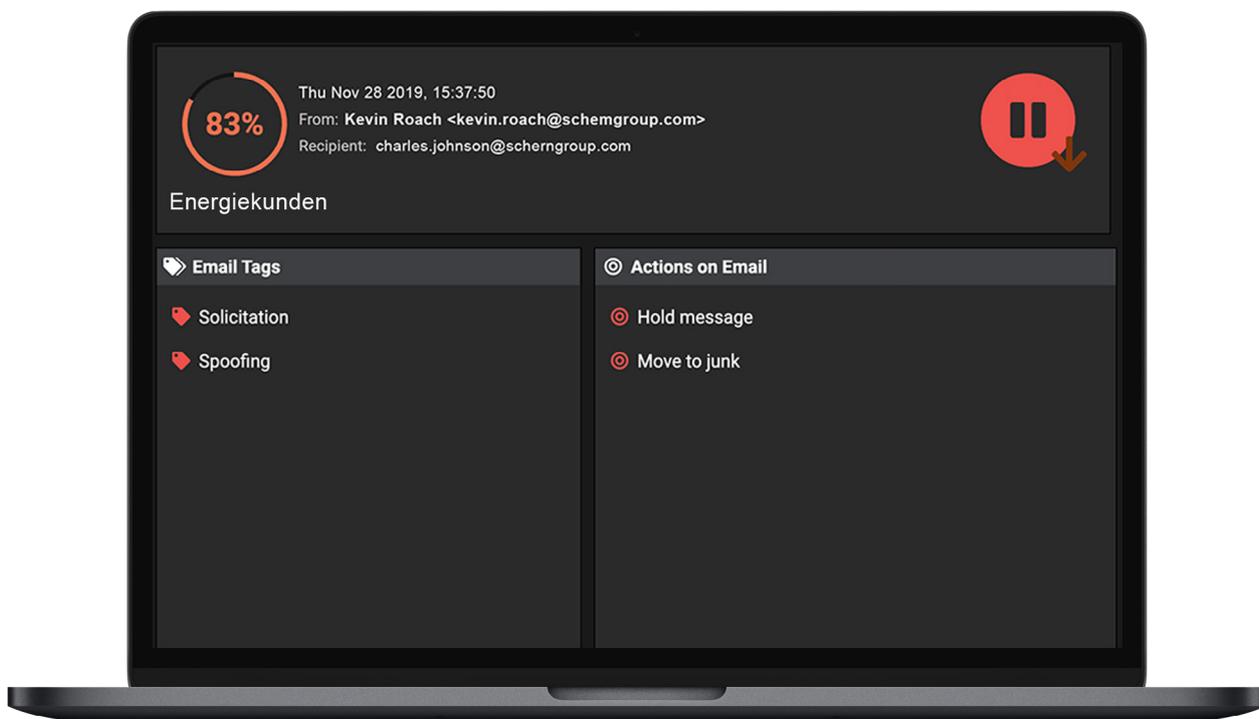


Abbildung 21: Angreifer, der sich als Führungskraft ausgibt und versucht, an sensible Dokumente heranzukommen. Man bemerke die gespoofte E-Mail-Adresse.

Impersonation-Angriff

Antigena Email erkannte einen gezielten Angriff gegen 30 Mitarbeiter eines multinationalen Technologieunternehmens. Der Angreifer hatte sich zuvor über jeden Benutzer genau informiert und sich dann als Führungskraft ausgegeben, mit der die Mitarbeiter am wahrscheinlichsten kommunizieren würden. Antigena Email erkannte den Social Engineering-Angriff und verhinderte, dass die E-Mail an die Empfänger zugestellt wurde.

1. Der Betreff jeder E-Mail 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. Darktrace erkannte nicht nur die Impersonation-Versuche 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 vor diesem Hintergrund keine Verbindung zwischen dem Absender und dem Unternehmen erkennen.

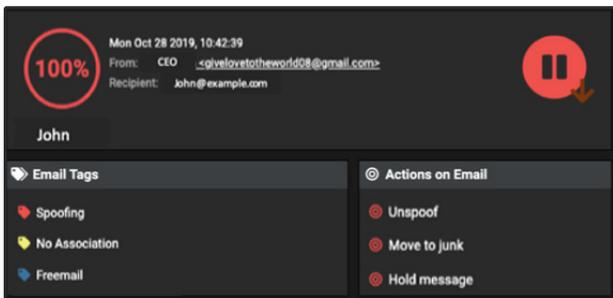


Abbildung 22: Eine von 30 E-Mails, mit einem Anomaliewert von 100%

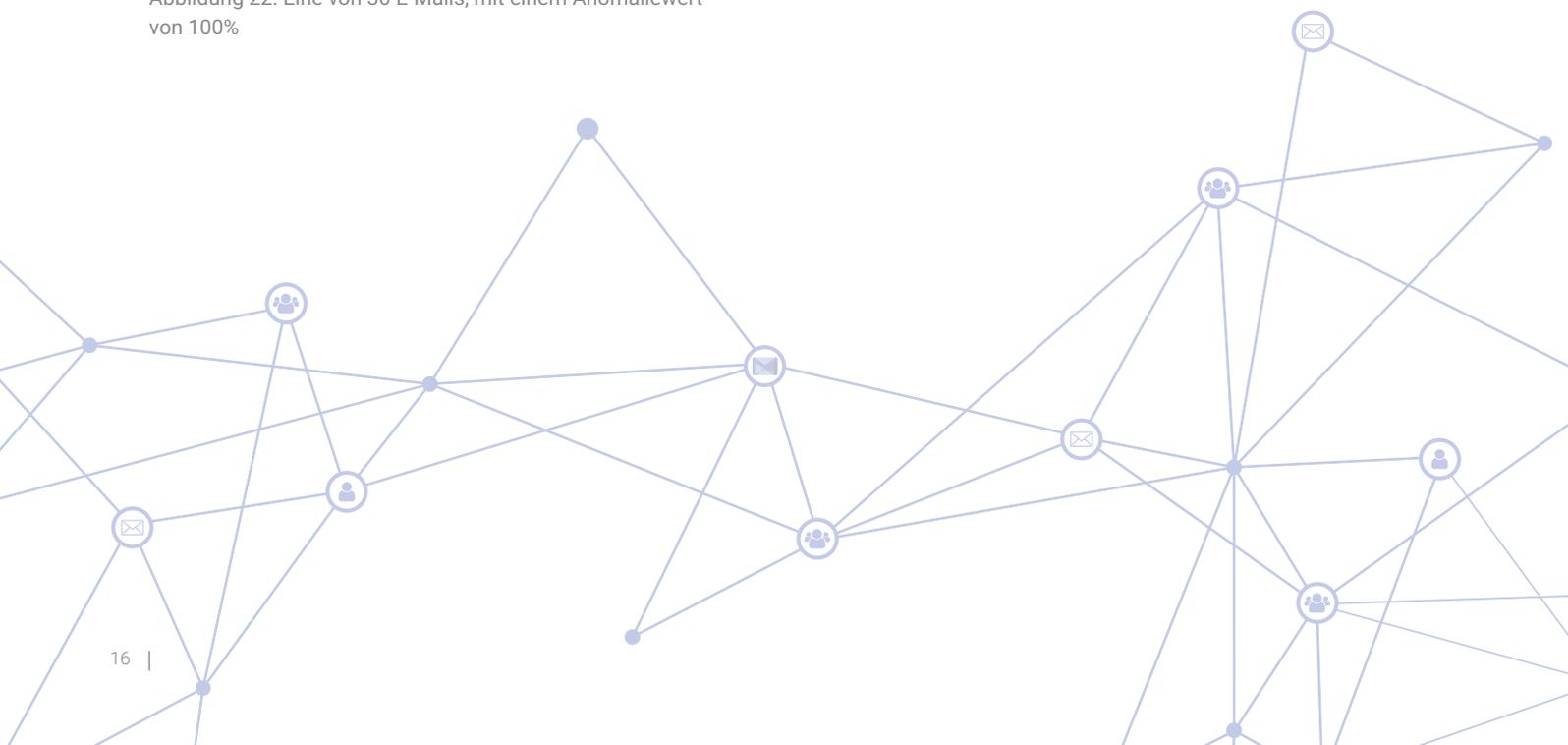
3. Antigena setzte mehrere schwache Indikatoren in Beziehung und erkannte, dass diese E-Mails Komponenten eines koordinierten Angriffs waren. Die Technologie isolierte sie in einem Puffer, damit das Sicherheitsteam des Unternehmens sie analysieren konnte.

4. 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.

Header From Personal	Count
CEO	18
CTO	11
CFO	1

Abbildung 23: Drei Führungskräfte identifiziert

5. 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 verhältnismäßige Maßnahmen ein.



Lohnbuchhaltung erhält schonbar vom Geschäftsführer eine Anfrage zur Aktualisierung von Kontodaten

Bei einem Stromversorger erkannte die KI von Darktrace einen sehr überzeugenden Spoofing-Versuch in Verbindung mit einem Office 365 E-Mail-Konto. Dem Empfänger der E-Mail, einem Mitarbeiter aus der Lohnbuchhaltung, wurde vorgegaukelt, es handle sich um eine Nachricht des Geschäftsführers, der um Aktualisierung seiner Kontodaten bittet.

Da die E-Mail den typischen Schreibstil des Geschäftsführers nachahmte, wäre der Versuch fast geglückt, hätte die KI von Darktrace nicht den E-Mail-Verkehr des Unternehmens im Kontext des breiteren Unternehmens analysiert.

1. Da Darktrace die normalen „Verhaltensmuster“ des Mitarbeiters, des Geschäftsführers und des breiteren Unternehmens im Cloud- und Netzwerkverkehr kannte, wurden sofort diverse subtile Anomalien in der E-Mail festgestellt, darunter die gefälschte Absenderadresse.

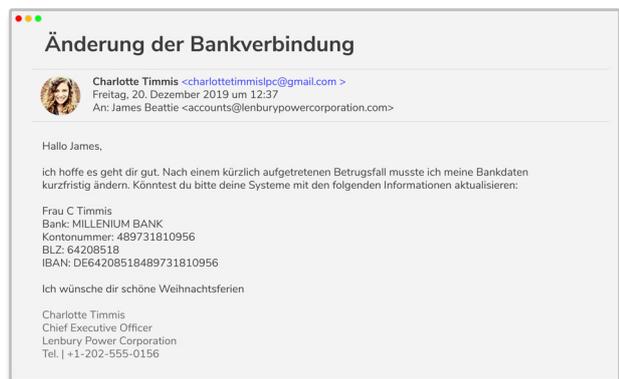


Abbildung 24: Screenshot der E-Mail, mit der die Identität des Geschäftsführers vorgetäuscht wurde

2. Zu weiteren schwachen Indikatoren gehörte, dass die KI von Darktrace automatisch die anormale Nähe der Domain zu denjenigen interner Mitarbeiter und vertrauenswürdiger Kontakte berechnete.

3. Die KI reagierte sofort, indem sie die Links in der E-Mail blockierte und die Nachricht deutlich als Spoof markierte, bevor sie zur Lohnbuchhaltung gelangen konnte. Dank umfassender Einblicke in den Cloud- und Netzwerkverkehr konnte Darktrace eine schwerwiegende Bedrohung neutralisieren, die signaturbasierte Tools nicht erkannt hätten.

Spoofing-Angriff „stellvertretender Finanzvorstand“

Bei diesem Vorfall ging es um die Vortäuschung der Identität des stellvertretenden Finanzvorstands bei einem bekannten Finanzinstitut. Die Bedrohungsakteure schickten 11 ähnliche E-Mails an das Unternehmen, aber Antigena Email hielt sie alle zurück, weil es Abweichungen von dem mehrdimensionalen Bild gab, das sich die Technologie im Laufe der Zeit von den „normalen“ Verhaltensmustern im Netzwerk-, Cloud- und E-Mail-Verkehr gemacht hat. Durch Analyse der eindeutig anomalen E-Mail-Adresse ohne Bezug in Verbindung mit dem Inhalt der E-Mails erkannte Darktrace diesen Spoofing-Versuch, während das Legacy-Gateway des Unternehmens alle 11 E-Mails durchließ.



Abbildung 25: Screenshot der E-Mail mit dem verdächtigen Link

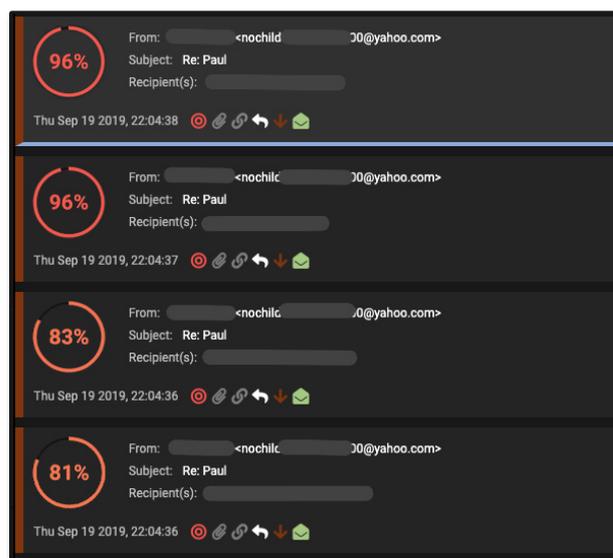
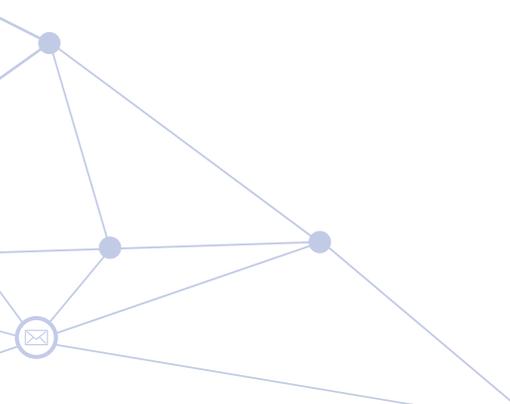
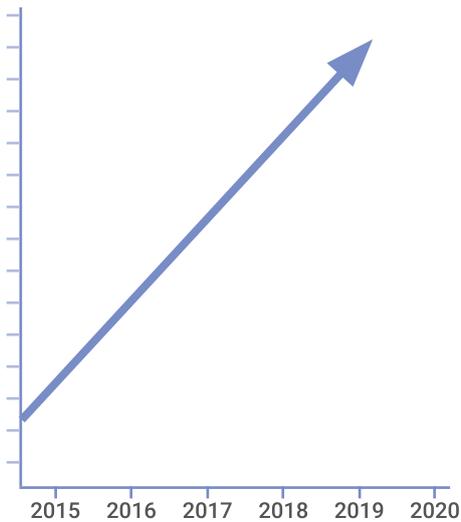


Abbildung 26: Vier der 11 E-Mails; zu sehen sind der hohe Anomaliewert und die von Antigena Email ergriffenen Maßnahmen



Kompromittierung von Mitarbeiterzugangsdaten

Kompromittierungen von Zugangsdaten haben zwischen 2016 und 2019 um 280% zugenommen



Unternehmen werden sich erst dann bewusst, wie wertvoll ein E-Mail-Postfach ist, wenn es in die falschen Hände gelangt. Sind die Bedrohungsakteure erst einmal eingedrungen, bieten sich ihnen jede Menge Angriffsmöglichkeiten. Es ist alarmierend, wie einfach sich Angreifer Zugriff verschaffen können, sei es durch Phishing-Kampagnen, Brute-Force-Angriffe oder Austausch im Dark Web.

In vielen Fällen plündern die Angreifer Posteingänge, weil sie es auf die darin enthaltenen wertvollen Daten abgesehen haben. Persönliche Informationen aus privaten Chats oder Abrechnungsdaten können für Betrug oder Erpressung missbraucht werden, während aus alten E-Mail-Threads streng vertrauliche Unternehmensinformationen herausgefiltert werden können. Kundenlisten, Preislisten oder Informationen zu Roadmaps und geistigem Eigentum sind meist schnell gefunden.

In anderen Fällen nutzen Cyberkriminelle das Konto als Startrampe für die nächsten Phasen eines Angriffs. Sie lauern im Verborgenen und sammeln seelenruhig Informationen über Führungskräfte oder Partner, die für sie von hohem Nutzen sind – dazu lesen sie Dokumente, verfolgen Korrespondenz und finden heraus, wie sie unbemerkt zuschlagen können. Wie bei der Kaperung von Supply-Chain-Konten ist die Fähigkeit, den E-Mail-Verkehr zu verfolgen und mit einer plausiblen Antwort anzugreifen, häufig der effizienteste Weg, einen Angriff zu starten, ohne dass Verdacht geschöpft wird.

Die Möglichkeiten für die Angreifer sind nahezu unendlich, für die Verteidiger hingegen sind sie begrenzt. Einfache und statische Sicherheitsmechanismen (einschließlich „Impossible Travel“-Regeln) überwachen zwar Unternehmenskonten, damit diese nicht gekapert werden. Gewiefte Angreifer jedoch, die genau wissen, wie sie in das Unternehmen eindringen können, lassen sich dadurch nicht abhalten. Das Darktrace Immunsystem ergänzt diese regelbasierten Ansätze und fängt diejenigen Bedrohungen ab, die die Verteidigungslinie passieren.

Indem es sich ein Bild von den normalen „Verhaltensmustern“ jedes Benutzers macht, erkennt das Immunsystem subtile Abweichungen, die selbst den vorsichtigsten Angreifer verraten –

ganz gleich, ob diese Abweichungen sich in verdächtigem Anmeldeverhalten, der Erstellung von Posteingangsregeln oder Änderungen der Benutzerrechte manifestieren. Da Cyberbedrohungen immer ausgefeilter werden, ist selbstlernende KI der einzig wirksame Weg, um Posteingänge vor Kriminellen zu schützen.



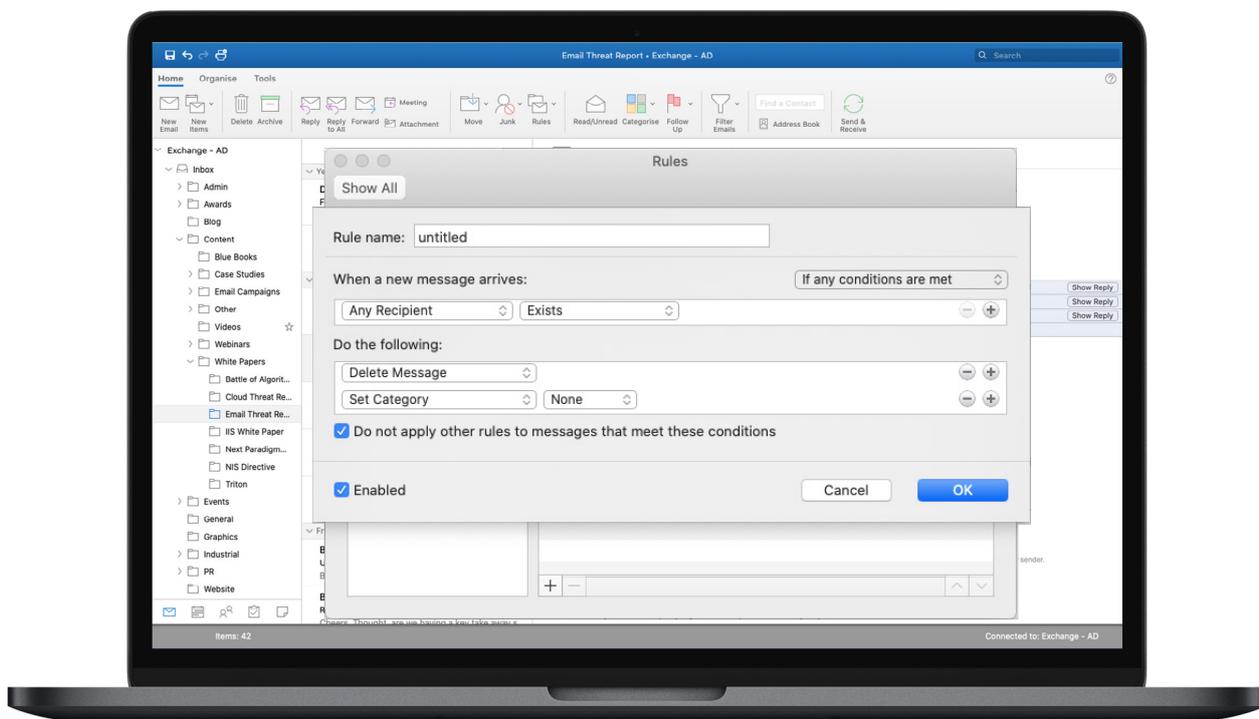


Abbildung 27: E-Mail-Verarbeitungsregel, die für ein kompromittiertes Konto eingerichtet wurde, und Threat Visualizer, der die geografischen Anmeldeorte anzeigt.

Ungewöhnliche Anmeldung bei einer Bank in Panama

Für einen Brute-Force-Angriff auf eine bekannte Bank in Panama wurde ein Office 365-Konto missbraucht. Die Anmeldungen erfolgten von einem Land aus, das unter Berücksichtigung der normalen „Verhaltensmuster“ des Unternehmens ungewöhnlich war.

Darktrace registrierte 885 Anmeldevorgänge über einen Zeitraum von 7 Tagen. Während die meisten Authentifizierungen über IP-Adressen in Panama erfolgten, gingen 15 % von einer IP-Adresse in Indien aus, die 100 % ungewöhnlich war. Eine weitergehende Analyse ergab, dass dieser externe Endpoint auf mehreren Spam-Blacklists stand und in letzter Zeit mit missbräuchlichem Online-Verhalten – möglicherweise unbefugtes Internet-Scanning oder -Hacking – in Verbindung stand.



Abbildung 28: Benutzeroberfläche; hier werden die Anmeldeorte angezeigt

Darktrace stellte dann einen augenscheinlichen Missbrauch der Funktion zum Zurücksetzen des Kennworts fest – der Benutzer in Indien änderte in äußerst ungewöhnlicher Art und Weise die Kontoberechtigungen. Die Aktivität war so verdächtig, da nach dem Zurücksetzen des Kennworts fehlgeschlagene Anmeldeversuche von einer IP, die normalerweise mit dem Unternehmen verknüpft ist, beobachtet wurden. Diese deuteten darauf hin, dass der legitime Benutzer ausgesperrt worden war.

03/12 20:45:39	SaaS:Admin	Regular	UpdateUser
03/12 20:45:39	SaaS:Admin	Regular	ChangeUserLicense
03/12 20:26:43	SaaS:Login	Regular	UserLoggedIn
03/12 20:26:43	SaaS:FailedLogin	Regular	UserLoginFailed
03/12 20:26:36	SaaS:FailedLogin	Regular	UserLoginFailed
03/12 18:31:31	SaaS:Login	Regular	UserLoggedIn
03/12 17:57:46	SaaS:Admin	Regular	ChangeUserLicense
03/12 17:57:46	SaaS:Admin	Regular	UpdateUser
03/12 17:06:57	SaaS:Admin	Regular	UpdateUser

Abbildung 29: Aktivität im Zusammenhang mit dem SaaS-Konto; zu sehen sind hier die geänderten Zugangsdaten

Zugriffsversuch aus einer ländlichen Gegend in Japan

Bei einem Finanzdienstleister in Europa wurde beobachtet, dass Office 365-Anmeldungen von einer ungewöhnlichen IP-Adresse in einer ländlichen Gegend in Japan aus erfolgten.

Zugriffe von entfernten Standorten sind zwar durchaus möglich, wenn ein Benutzer auf Reisen ist oder einen Proxy-Service nutzt, aber dies konnte auch ein deutlicher Hinweis auf kompromittierte Zugangsdaten und schädlichen Zugriff durch einen unbefugten Benutzer sein. Angesichts dessen, dass der Zugangspunkt ein ganz anderer war als die sonst üblichen IPs, kennzeichnete Darktrace die Aktivität als anormal und empfahl sofort weitere Untersuchungen.

Das Sicherheitsteam konnte das Office 365-Konto aus der Ferne sperren und die Zugangsdaten zurücksetzen und legte dem böswilligen Akteur damit das Handwerk. Wäre diese Aktivität nicht bemerkt worden, hätte der Bedrohungsakteur seine Zugriffsrechte nutzen können, um Malware in das Unternehmen einzuschleusen oder eine betrügerische Zahlung zu veranlassen.

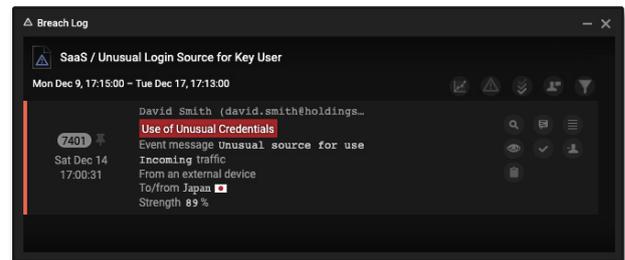


Abbildung 30: Die Anmeldung aus Japan wich von mehreren Modellen ab

Kompromittierung und Sabotage eines Office 365-Kontos

Bei einer internationalen Non-Profit-Organisation mit Büros in aller Welt erkannte Darktrace, dass in Office 365 ein Konto gekapert worden war, weil die statische „Impossible Travel“-Regel von Azure AD den Angriff nicht abgewehrt hatte. Die selbstlernende KI von Darktrace erkannte einen Anmeldevorgang von einer IP-Adresse aus, die ungewöhnlich für die betreffende Benutzerin und ihre Peer-Group war, und benachrichtigte sofort das Sicherheitsteam.

Darktrace wies darauf hin, dass für das Konto eine neue E-Mail-Verarbeitungsregel eingerichtet worden war, die eingehende E-Mails löscht. Dies war ein deutlicher Hinweis auf eine Kompromittierung und das Sicherheitsteam konnte das Konto sperren, bevor der Angreifer Schaden anrichten konnte.

Mit dieser neuen E-Mail-Verarbeitungsregel hätte der Angreifer E-Mail-Korrespondenz mit anderen Mitarbeitern im Unternehmen führen können, ohne dass der legitime Benutzer etwas davon mitbekommen hätte. Dies ist eine beliebte Strategie von Cyberkriminellen, um sich dauerhaften Zugriff zu verschaffen und sich im Unternehmen einzunisten, möglicherweise als Vorbereitung für einen großangelegten Angriff.

Durch Analyse der ungewöhnlichen IP-Adresse in Verbindung mit dem unüblichen Verhalten des scheinbaren Benutzers identifizierte Darktrace diese Aktivität als Kontokaperung und verhinderte damit größeren Schaden für das Unternehmen.

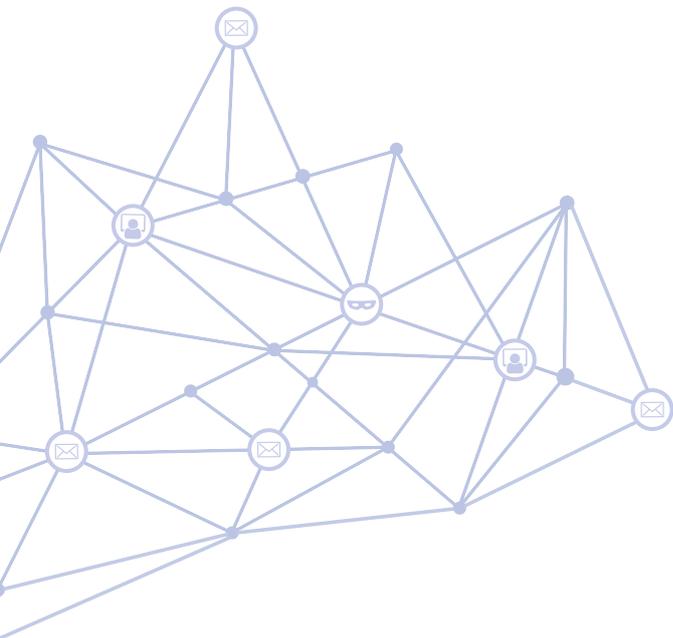
Automatisierter Brute-Force-Angriff

Darktrace stellte täglich über einen Zeitraum von einer Woche mehrere fehlgeschlagene Anmeldeversuche bei einem Office 365-Konto immer mit denselben Benutzernamen fest. Jede Anmeldeunde erfolgte an sechs Tagen immer genau um 18.04 Uhr. Dass Uhrzeit und Anzahl der Anmeldeversuche immer gleich waren, deutete auf einen automatisierten Brute-Force-Angriff hin, der so programmiert war, dass nach einer bestimmten Anzahl an Fehlversuchen Schluss war, um eine Kontosperrung zu vermeiden.

Darktrace stufte dieses Muster als äußerst anormal ein und benachrichtigte das Sicherheitsteam. Hätte Darktrace nicht die schwachen Indikatoren in Beziehung gesetzt und die subtilen Hinweise auf die sich entwickelnde Bedrohung erkannt, hätte dieser automatisierte Angriff noch Wochen oder Monate andauern können und der Angreifer hätte anhand anderer bereits gesammelter Informationen die Kennwörter der Benutzer erraten können.



Abbildung 31: Schaubild zur Veranschaulichung der wiederholten Anmeldeversuche





Über Darktrace

Darktrace ist das weltweit führende Unternehmen für Cyber-KI und Schöpfer der ‚Autonomous Response‘ Technologie. Darktraces selbstlernende KI basiert auf dem menschlichen Immunsystem und wird von über 3.000 Organisationen zum Schutz vor Bedrohungen für Cloud, E-Mail, IoT, Netzwerke und industrielle Systeme eingesetzt.

Das Unternehmen hat über 1.000 Mitarbeiter und Hauptsitze in San Francisco und Cambridge, Großbritannien. Alle 3 Sekunden wehrt Darktrace AI gegen eine Cyber-Bedrohung und verhindert, dass sie Schaden verursacht.

Kontakt

München +49 89 255 529 85

Nordamerika: +1 (415) 229 9100

Asien-Pazifik: +65 6804 5010

Lateinamerika: +55 11 97242 2011

info@darktrace.com | darktrace.com

[@darktrace](https://twitter.com/darktrace)