Fünf Schritte zur Abwehr von Business Email Compromise

Wichtige Vorteile

- Erkennen und Stoppen von verschiedenen BEC-Angriffsformen, indem mehrere Angriffstaktiken abgedeckt werden
- Überblick über die am häufigsten angegriffenen Anwender und die Drittanbieter mit dem größten Angriffsrisiko
- Benachrichtigung bei Lieferanten mit potenziell kompromittierten Konten
- Schulungen für Ihre Anwender, damit sie E-Mail-Betrug erkennen und melden
- Schnellere Reaktion auf Bedrohungen und beschleunigte Behebung durch Automatisierung
- Verbesserte Sicherheit und operative Effektivität durch eine integrierte Ende-zu-Ende-Lösung

Business Email Compromise (BEC) ist eine der Hauptursachen für finanzielle Verluste. Laut dem *Internet Crime Report* (Bericht zu Internetkriminalität) des FBI liegen die jährlichen Schäden durch BEC bei mehr als 2,7 Milliarden US-Dollar – was 80 Mal höher ist als die Verluste durch Ransomware.[1]

Bei BEC-Angriffen werden häufig vertrauenswürdige Absender imitiert und die Empfänger mit seriös aussehenden E-Mails getäuscht. Anschließend missbrauchen die Angreifer die Vertrauensstellung des scheinbaren Absenders, um die Empfänger beispielsweise zu Banküberweisungen oder anderen Zahlungen zu verleiten. Solche Methoden lassen sich nur schwer kontern, da hier keine Schaddaten zum Einsatz kommen. Einige Angreifer gehen jedoch noch weiter und nutzen für ihre BEC-Attacken kompromittierte seriöse Lieferantenkonten.

Der Schutz Ihres Unternehmens vor BEC erfordert eine Kombination aus Technologie und Schulungen: Sie benötigen einen wirklich ganzheitlichen Ansatz, um die E-Mail-Kompromittierungskette effektiv zu unterbrechen. Proofpoint kann Ihnen helfen.

Wir sind der einzige und bisher einzige Anbieter einer umfassenden und integrierten Bedrohungsschutz-Plattform, die Folgendes bietet:

- Erkennung und Blockierung von BEC-Bedrohungen, noch bevor sie die Posteingänge erreichen
- Schulung Ihrer Anwender, damit diese BEC erkennen und melden
- Vollständiger Überblick über Risiken durch Lieferanten und kompromittierte Drittanbieter-Konten
- Automatisierte Bedrohungserkennung und -abwehr
- Schutz Ihrer Marke bei E-Mail-Betrugsversuchen

Diese Kurzvorstellung liefert eine ausführliche Beschreibung unseres Ansatzes.

1 *Internet Crime Report* (Bericht zu Internetkriminalität), FBI, 2022.

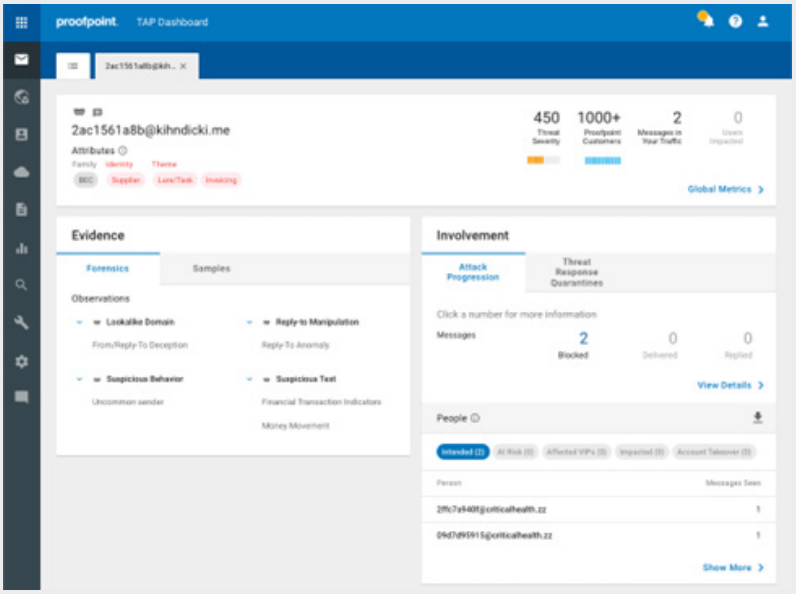

Abb. 1: Proofpoint identifiziert die Anwender, die am häufigsten mit BEC-Methoden angegriffen werden, und bietet einen detaillierten Überblick über diese Bedrohungen (einschließlich Themen, verwendeten Taktiken uvm.).

Erkennung und Blockierung von Impostor-Bedrohungen, noch bevor sie Ihr Unternehmen erreichen

Unsere integrierte Plattform setzt auf die Proofpoint-Lösung Advanced BEC Defense, die unser neuestes, KI-gestütztes BEC-Erkennungsmodul Supernova verwendet. Diese hochmoderne Technologie erkennt 17 Mal mehr Bedrohungen und ermöglicht uns die Aufdeckung eines breiten Spektrums an E-Mail-Betrugsangriffen.

Proofpoint Advanced BEC Defense führt umfassende Analysen verschiedener Nachrichtenattribute durch, zum Beispiel:

- E-Mail-Header
- IP-Adresse des Absenders
- Absender-/Empfänger-Beziehung
- Reputation des Absenders

Proofpoint Advanced BEC Defense führt semantische LLM-Analysen (Large-Language Module) des Nachrichtentexts durch und sucht nach emotionalen und sprachlichen Besonderheiten. Dadurch lässt sich erkennen, ob es sich bei einer Nachricht um eine BEC-Bedrohung handelt. Außerdem überwacht das verhaltensbasierte Machine-Learning-Modul auch Aktivitäten auf Hinweise für schädliches Verhalten bzw. Bedrohungssignaturen, um Muster zu erkennen und auf diese Weise in Echtzeit Anomalien aufzuspüren.

Die Überwachung beantwortet unter anderem folgende Fragen:

- Versendet ein Absender ungewöhnlich viele E-Mails?
- Stammen die E-Mails von einer ungewöhnlichen IP-Adresse?
- Hatten die Anwender des Unternehmens bereits mit dem Absender Kontakt?

Diese Informationen erweitern die Erkennungsmöglichkeiten um die Identifizierung raffinierter E-Mail-Bedrohungen wie Ransomware, Anmeldedaten-Phishing und kompromittierte Drittanbieter-Konten sowie Display Name-Spoofing und Doppelgänger-Domains. Die Lösung blockiert sogar äußerst raffinierte Supply-Chain-Angriffe, da Nachrichten dynamisch auf Taktiken geprüft werden, die für Betrug mit Lieferantenrechnungen typisch sind. Mithilfe von Machine Learning lernt Proofpoint Advanced BEC Defense in Echtzeit, um möglichst geringe False-Positive-Raten zu erreichen.

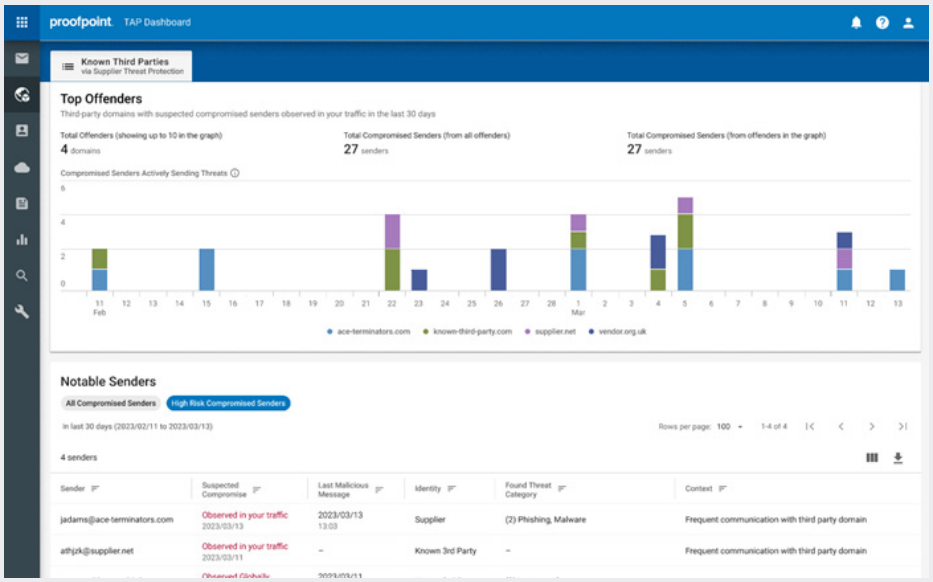

Abb. 2: Das Add-on Supplier Threat Protection erkennt kompromittierte Drittanbieter-Konten, mit denen Ihr Unternehmen interagiert.

Überblick über Ihre BEC-Risiken

Damit Sie Ihre BEC-Risiken besser verstehen, kommunizieren und minimieren können, unterstützen wir Sie dabei, gegenüber Ihren Führungskräften folgende Fragen zu beantworten:

- Welche BEC-Risiken bestehen in unserem Unternehmen?
- Welche Anwender werden am häufigsten angegriffen?
- Bei welchen unserer vertrauenswürdigen Geschäftspartner wurden möglicherweise Konten kompromittiert?
- Wie können wir Risiken quantifizieren und beheben?

Proofpoint liefert Informationen dazu, welche Anwender am häufigsten angegriffen werden und wer am wahrscheinlichsten auf Impostor-Bedrohungen hereinfällt. Dabei erhalten Sie einen detaillierten Überblick über die BEC-Bedrohung, einschließlich der Themen der jeweiligen Impostor-Bedrohung (z. B. Gutscheinkarte, Betrug mit Lieferantenrechnung und Umleitung von Gehaltszahlungen, siehe Abb. 1). Anschließend können Sie gefährdete Anwender mit adaptiven Sicherheitskontrollen zusätzlich schützen sowie Risiken besser an die Unternehmensführung kommunizieren.

Proofpoint erweitert Ihren Schutz mithilfe von Transparenz und Einblicken in Risiken durch Lieferanten, sodass Sie damit verbundene Bedrohungen wie folgt unter Kontrolle bekommen können:

- Proaktives Identifizieren möglicherweise imitierter und kompromittierter Lieferantenkonten
- Lieferantenzentrierter und priorisierter Überblick über BEC-Bedrohungen
- Identifizieren und Verhindern von Bedrohungen, die von Lieferanten-Domains sowie böswilligen Doppelgängern dieser Domains ausgehen

Wir analysieren und priorisieren die Risikostufe dieser Lieferanten-Domains und benachrichtigen Sie über potenziell kompromittierte Konten, sodass Ihr Sicherheitsteam seine Maßnahmen auf die für Ihr Unternehmen riskantesten Lieferanten konzentrieren kann.

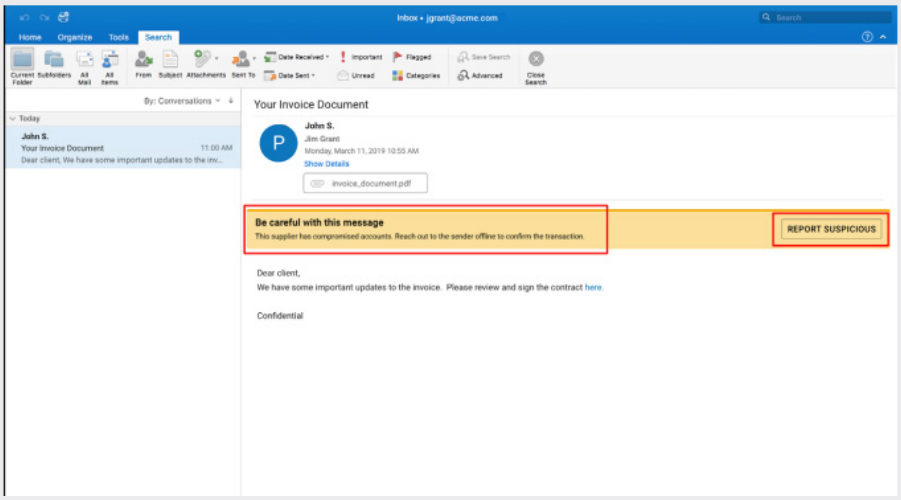

Abb. 3: Warnhinweise in E-Mails bieten Ihren Anwendern wichtige Informationen, damit sie bei nicht eindeutig legitimen E-Mails vorsichtiger agieren.

Stärkung der Resilienz Ihrer Anwender gegenüber BEC

BEC-Angriffe richten sich gegen Menschen und versuchen, diese zum Ausführen von Angriffen zu bringen, ohne dass sie argwöhnisch werden. Da diese Impostor-Angriffe auf Social Engineering und Identitätstäuschung setzen, bilden Ihre Anwender häufig die letzte Verteidigungslinie. Daher sind zur Minimierung von BEC-Risiken sowohl Technologie als auch Schulungen erforderlich.

Mit unserer Proofpoint PhishAlarm-Schaltfläche können Sie Ihren Anwendern ein wichtiges Hilfsmittel zum Melden möglicher Impostor-E-Mails in die Hand geben. Außerdem zeigen wir bei potenziell verdächtigen Nachrichten in der E-Mail Warnhinweise an, damit die Anwender informiertere Entscheidungen treffen können. Schulen Sie Ihre Anwender zu den neuesten Angriffsmethoden bei BEC-Attacken und weisen Sie den am häufigsten angegriffenen Nutzern gezielte Schulungen zu, damit BEC-Angriffe bei ihnen keine Chance haben.

Automatische Reaktionen auf Bedrohungen

Viele Unternehmen kämpfen in ihren IT-Sicherheits-abteilungen mit Fachkräftemangel, was die Suche, Untersuchung und Behebung von BEC-Bedrohungen im gesamten Unternehmen erschwert. Deshalb automatisieren wir den gesamten Prozess der Erkennung und Behebung von Bedrohungen. Mit unserer TRAP-Funktion (Threat Response Auto-Pull) können Sie alle verdächtigen oder unerwünschten E-Mails automatisiert oder mit nur einem Klick unter Quarantäne stellen. Die Automatikfunktionen berücksichtigen auch E-Mails, die von anderen Anwendern weitergeleitet oder empfangen wurden, sowie von anderen Proofpoint-Kunden erhaltene Nachrichten. Dadurch profitieren alle Seiten von den zusätzlichen Bedrohungsdaten.

Darüber hinaus optimieren wir die Verwaltung des Abuse-Postfachs. Von Nutzern gemeldete E-Mails werden automatisch analysiert und als gefährlich erkannte Nachrichten können isoliert oder unschädlich gemacht werden, sodass die Reaktion auf Bedrohungen beschleunigt und manuelle Abläufe minimiert werden.

Schutz Ihrer Marke bei E-Mail-Betrugsversuchen

Bei Marken-Spoofing richten die Angreifer sich direkt gegen Ihre Kunden und Geschäftspartner und versuchen, über Ihren Firmennamen und Ihre Marke an Geld zu gelangen. Proofpoint schützt Ihre Marke vor Schäden durch BEC-Angriffe. Dazu verhindern wir, dass betrügerische E-Mails über Ihre vertrauenswürdigen Domains verschickt werden. Wir authentifizieren alle zugestellten und von Ihrem Unternehmen versendeten E-Mails. Unsere geführten Workflows und Managed Services vereinfachen die Implementierung von DMARC. Das verhindert wirksam den Missbrauch Ihrer Domain und blockiert alle Versuche, nicht autorisierte E-Mails aus Ihren vertrauenswürdigen Domains zu versenden.

Außerdem erhalten Sie einen Überblick über alle E-Mails, die unter Verwendung Ihrer Domain versendet werden, einschließlich solcher von vertrauenswürdigen externen Versendern. Wir identifizieren Doppelgänger Ihrer Domains und erkennen dynamisch neu registrierte Domains, die bei E-Mail-Betrugsversuchen Ihre Marke imitieren. Dank unseres Virtual Takedown-Services können Sie schnell Maßnahmen ergreifen, um diese Websites stilllegen zu lassen.

Zusammenfassung

E-Mail-Betrug verursacht die größten finanziellen Verluste. Die Betrüger werden immer raffinierter und entwickeln dabei ihre BEC-Taktiken weiter bis hin zu komplexem Lieferantenbetrug. Proofpoint ist der erste und einzige Anbieter mit einer integrierten Ende-zu-Ende-Lösung, die neue Bedrohungen effektiv abwehren kann.

Unsere BEC-Lösung bietet folgende Vorteile:

- Erkennung und Blockierung verschiedener BEC-Angriffstaktiken
- Überblick über die menschliche Angriffsfläche sowie detaillierte Informationen zu BEC-Bedrohungen
- Identifizierung der Lieferanten, die ein Risiko darstellen und deren Konten kompromittiert sein könnten
- Schulung Ihrer Anwender, damit sie nicht auf BEC-Angriffe hereinfallen
- Automatisierte Untersuchung und Behebung von Zwischenfällen
- Schutz Ihrer Marke bei E-Mail-Betrugsversuchen

Mit Proofpoint können Sie BEC-Bedrohungen schnell, einfach und effektiv abwehren.

WEITERE INFORMATIONEN

Weitere Informationen finden Sie unter **proofpoint.com/de**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. ist ein führendes Unternehmen für Cybersicherheit und Compliance. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter, denn diese bedeuten für ein Unternehmen sowohl das größte Kapital als auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und ihre IT-Anwender für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter 75 Prozent der Fortune-100-Unternehmen, setzen auf die personenzentrierten Sicherheits- und Compliance-Lösungen von Proofpoint, um ihre größten Risiken in den Bereichen E-Mail, Cloud, soziale Netzwerke und Web zu minimieren. Weitere Informationen finden Sie unter **www.proofpoint.de**.

proofpoint.

0201-012-04-02 11/23