Fünf Schritte zur Abwehr von BEC (Business Email Compromise)

- Erkennen und Stoppen von verschiedenen BEC-Angriffsformen, indem mehrere Angriffstaktiken abgedeckt werden
- Einblick in die Anwender, die am häufigsten angegriffen werden, und die Lieferanten, die das größte Risiko darstellen
- Schulungen für Ihre Anwender, damit sie E-Mail-Betrug erkennen und melden
- Schnellere Reaktion auf Bedrohungen und beschleunigte Behebung durch Automatisierung
- Höhere Sicherheit und operative Effektivität mit einer integrierten Ende-zu-Ende-Lösung

E-Mail-Betrug hat laut dem FBI im Jahr 2020 die größten finanziellen Verluste verursacht.[1] Der Schaden für Unternehmen lag bei fast 2 Milliarden US-Dollar, was 44 % aller gemeldeten Verluste entspricht. Gartner geht zudem davon aus, dass sich die Zahl der Angriffe mit Business Email Compromise (BEC, auch als Chefmasche bezeichnet) bis 2023 jedes Jahr verdoppelt und bei Unternehmen erhebliche finanzielle Verluste in Höhe von 5 Milliarden US-Dollar verursachen wird.[2]

BEC-Betrug beginnt häufig mit einer E-Mail, deren Absender sich als vertrauenswürdige Person ausgibt. Dazu ahmt der Angreifer entweder diese Person nach oder übernimmt deren Konto. Angreifer setzen dabei auf Social Engineering, um ihre Opfer zu täuschen oder mit Drohungen dazu zu bringen, Geld zu überweisen, vertrauliche Informationen weiterzugeben usw. Da bei BEC-Angriffen keine Schaddaten verwendet werden, sind sie für herkömmliche Gateways, die ausschließlich auf Reputation und Malware-Sandbox-Analysen setzen, nur schwer zu erkennen.

Gleichzeitig werden die Betrüger immer raffinierter und erweitern die Bandbreite an BEC-Varianten um Gutscheinkarten-Betrug, Umleitung von Gehaltszahlungen und Betrug mit Lieferantenrechnungen. Um diese wandlungsfähigen E-Mail-Betrugsversuche erfolgreich abwehren zu können, benötigen Sie eine ganzheitliche Lösung, die den Taktiken der BEC-Akteure mit mehreren Sicherheitskontrollen und Anwenderschulungen begegnet.

So kann Proofpoint BEC-Angriffe stoppen

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

- Erkennung und Blockierung von BEC-Bedrohungen, noch bevor sie Ihr Unternehmen erreichen
- Überblick über BEC-Risiken
- Schulung Ihrer Anwender, damit diese BEC erkennen und melden
- Automatisierte Bedrohungserkennung und -abwehr
- Schutz Ihrer Marke bei E-Mail-Betrugsversuchen

In dieser Kurzvorstellung wird erklärt, wie wir gängige BEC-Angriffe abwehren.

1 „Internet Crime Report“ (Bericht zu Internetkriminalität), FBI, 2021.
2 „Protecting Against Business Email Compromise“ (Schutz vor BEC), Gartner, 2020.

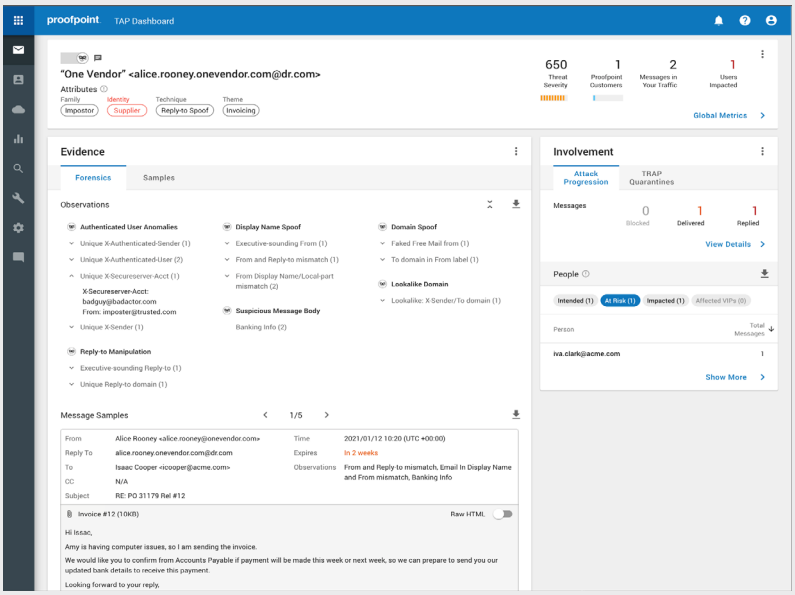

Abb. 1: Proofpoint identifiziert die Anwender, die am häufigsten mit Impostor-Bedrohungen angegriffen werden und bietet einen detaillierten Überblick über die BEC-Bedrohungen.

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

Unsere integrierte Bedrohungsschutz-Plattform verwendet **Advanced BEC Defense**. Unser BEC-Erkennungsmodul, das sich auf Machine Learning und künstliche Intelligenz stützt, erkennt dynamisch eine große Bandbreite an E-Mail-Betrugsmethoden und analysiert mehrere Nachrichtenattribute, zum Beispiel:

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

Das Modul analysiert außerdem den Nachrichteninhalt auf emotionale und sprachliche Besonderheiten sowie weitere Hinweise auf eine BEC-Bedrohung.

Advanced BEC Defense deckt alle BEC-Angriffstaktiken auf, einschließlich Display Name-Spoofing und Doppelgänger-Domänen. Zur Erkennung und Blockierung äußerst raffinierter Lieferkettenangriffe werden Nachrichten dynamisch auf zahlreiche Taktiken geprüft, die für Betrug mit Lieferantenrechnungen typisch sind, zum Beispiel:

- Änderungen der Reply-to-Adresse
- Verwendung schädlicher IP-Adressen
- Verwendung nachgeahmter Lieferantendomänen
- Wörter und Formulierungen, die für Lieferantenbetrug typisch sind

Die meisten E-Mail-Sicherheitsprodukte setzen lediglich auf statische Regelabgleiche oder begrenzte Kontextdaten, wodurch manuelle Optimierungen erforderlich sind. Unser Erkennungsmodul Advanced BEC Defense ist anders. Es basiert auf **NexusAI** und lernt in Echtzeit. Zudem ist es für Unternehmen aller Größen geeignet und deckt E-Mail, Cloud, Netzwerke und digitale Kanäle ab.

Wir bieten echtes Machine Learning, um den Bedrohungen immer einen Schritt voraus zu bleiben, und ermöglichen damit die dynamische Klassifizierung „guter“ und „schlechter“ E-Mails mit einem Minimum an False Positives. Das Modul reagiert auf Veränderungen der Angriffstaktiken, damit gefährliche Nachrichten gestoppt und legitime E-Mails zuverlässig zugestellt werden.

2. 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 sind am stärksten gefährdet?
- Welche Lieferanten stellen ein Risiko für unser Unternehmen dar?
- Was können wir tun, um die Risiken zu minimieren?

Wir liefern Informationen dazu, welche Anwender am häufigsten mit Impostor-E-Mails angegriffen werden und wer am wahrscheinlichsten auf solche Bedrohungen hereinfällt. Sie erhalten einen detaillierten Überblick über die BEC-Bedrohung, einschließlich der Themen der jeweiligen Impostor-Bedrohung (z. B. Gutscheinkarte, Köder, Betrug mit Lieferantenrechnung und Umleitung von Gehaltszahlungen, siehe Abb. 1). Dadurch kann Ihr Sicherheitsteam den Angriff besser verstehen und kommunizieren.

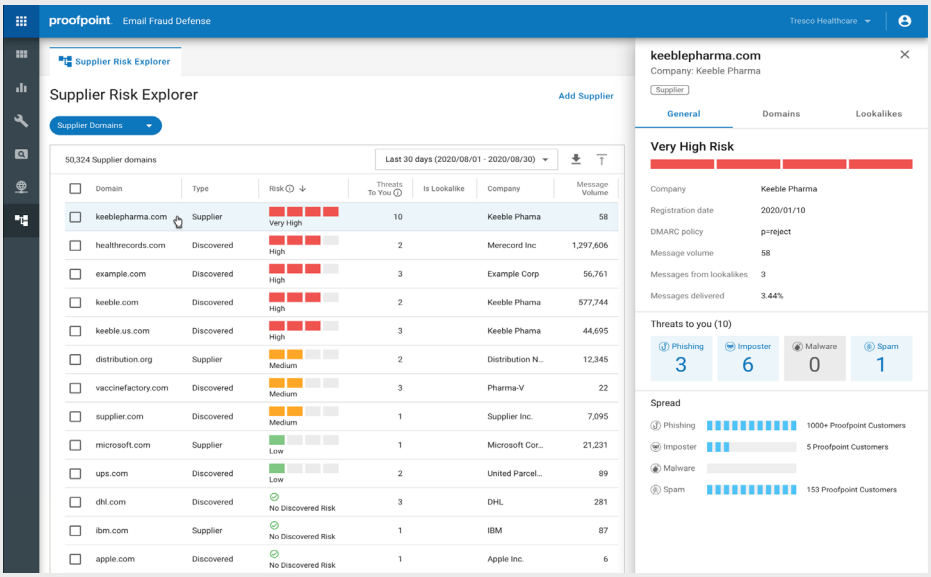

Abb. 2: Supplier Risk Explorer liefert einen Überblick über die Lieferantendomänen und Informationen dazu, welche Lieferanten für Ihr Unternehmen ein Risiko darstellen.

Darüber hinaus erhalten Sie einen Überblick darüber, welche Lieferanten für Ihr Unternehmen ein Risiko darstellen. **Nexus Supplier Risk Explorer** (siehe Abb. 2) bietet diese Vorteile:

- Automatische Identifizierung potenziell nachgeahmter und kompromittierter Lieferanten und Domänen, die an Ihre Anwender E-Mails senden
- Lieferantenzentrierter Blick auf BEC-Bedrohungen
- Informationen zum Nachrichtenaufkommen
- Informationen zu Bedrohungen, die in Lieferanten-Domänen erkannt wurden
- Informationen zu den Nachrichten, die über schädliche Doppelgänger-Domänen Ihrer Lieferanten verschickt wurden

Durch die Bewertung und Priorisierung der Risikostufe dieser Lieferanten-Domänen kann Ihr Sicherheitsteam seine Maßnahmen auf die für Ihr Unternehmen riskantesten Lieferanten konzentrieren.

3. Stärkung der Widerstandsfähigkeit Ihrer Anwender gegenüber BEC

BEC richtet sich gegen Menschen und versucht, diese zum Ausführen von Angriffen zu bringen, ohne dass diese es merken. 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.

Wir helfen Ihnen dabei, Ihre Anwender darin zu schulen, verdächtige Impostor-E-Mails zu identifizieren und zu melden. Wir vermitteln Ihren Endnutzern die Kenntnisse und Fähigkeiten, mit denen sie Ihr Unternehmen vor diesen personenzentrierten Bedrohungen schützen können. Die Erkenntnisse aus unserer integrierten Plattform ermöglichen den Aufbau eines Programms, das sich an Ihre Very Attacked People (besonders häufig angegriffene Personen, VAPs) oder Anwender richtet, die mit bekannt schädlichen Inhalten umgehen.

Zunächst können Sie feststellen, welche Anwender für BEC-Bedrohungen anfällig sind. Im nächsten Schritt überprüfen Sie mit simulierten, realitätsnahen BEC-Angriffen auf sichere Weise, wer in der Alltagsumgebung auf Impostor-Betrug reagiert. Diejenigen Mitarbeiter, die auf solche Angriffe hereinfallen, werden sofort auf ihren Fehler hingewiesen, und ihnen können im Anschluss automatisch die passenden Schulungsmodule zugewiesen werden.

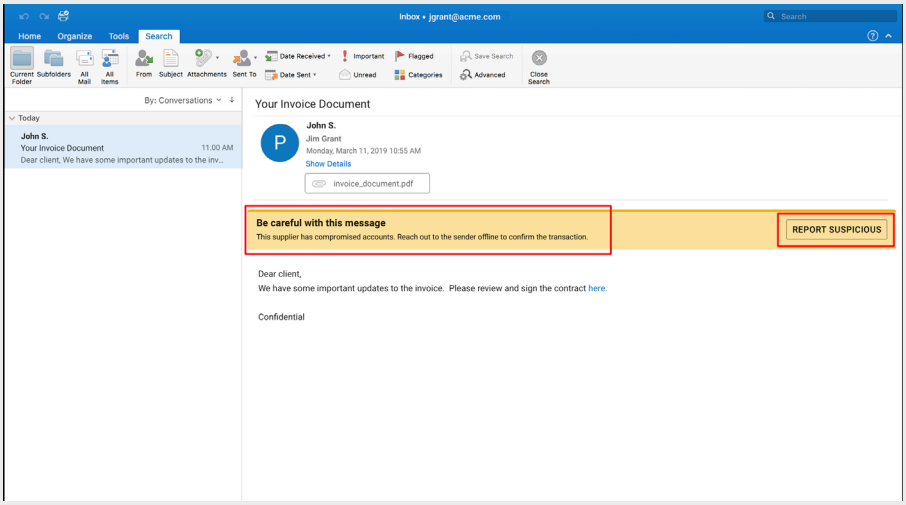

Abb. 3: Warnhinweise in E-Mails bieten Ihren Anwendern wichtige Informationen, damit sie bei nicht eindeutig legitimen E-Mails vorsichtiger agieren.

Die Schulungsmaterialien lassen sich vollständig anpassen, damit sie relevant sind und die internen Prozesse Ihres Unternehmens abdecken. So können Sie zum Beispiel Anwendern erklären, dass sie potenzielle Impostor-Bedrohungen an ein Abuse-Postfach senden und finanzbezogene Anfragen über einen unternehmensspezifischen Prozess verifizieren sollen.

Darüber hinaus erhalten Ihre Anwender Warnhinweise in E-Mails mit einer kurzen Beschreibung des Risikos, das die jeweilige E-Mail darstellt. Wir warnen Ihre Anwender zum Beispiel vor Nachrichten, die von einem externen Absender oder einer neu registrierten Domäne eingehen, damit sie bei nicht eindeutig legitimen E-Mails vorsichtiger agieren werden. Gleichzeitig wird damit auch die Gefahr von Kompromittierungen reduziert.

4. Automatische Reaktionen auf Bedrohungen

Die meisten Unternehmen haben Probleme durch zu kleine Sicherheitsteams, die von der Verwaltung unzähliger, nicht miteinander kommunizierender Sicherheitsanbieter und -produkte überfordert sind. Das erschwert die schnelle Suche, Untersuchung und Behebung von BEC-Bedrohungen im gesamten Unternehmen – und verlängert den Zeitraum, in dem das Unternehmen gefährdet bleibt.

Wir automatisieren die 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. Das gilt selbst für Nachrichten, die bereits weitergeleitet oder von anderen Endnutzern empfangen wurden. Darüber hinaus optimieren wir die Verwaltung des Abuse-Postfachs und ermöglichen die automatische Neutralisierung aktiver Bedrohungen innerhalb von Minuten, sodass die Belastung für das IT-Team verringert wird.

Anwender können verdächtige Nachrichten direkt über die Warnung melden, die auf das Risiko einer konkreten E-Mail hinweist. Alternativ können sie dazu das PhishAlarm®-Add-in nutzen. In beiden Fällen ist nur ein Klick nötig.

Die gemeldeten Nachrichten werden automatisch analysiert und ihr Kontext mit verschiedenen Bedrohungsdaten sowie Reputationssystemen angereichert. Durch die Funktionen zur BEC-Bedrohungssuche können Sie Ihre E-Mail-Umgebung schnell durchsuchen und feststellen, ob auch weitere Anwender diese Nachricht erhalten haben.

Wird die Nachricht als schädlich erkannt, dann wird sie – einschließlich aller Kopien und Weiterleitungen – automatisch unter Quarantäne gestellt, sodass Ihr Team nicht jeden einzelnen Vorfall manuell handhaben und untersuchen muss – und somit Zeit und Aufwand spart. Um den Kreis zu schließen, erhalten Ihre Anwender eine angepasste E-Mail mit der Information, dass die Nachricht als schädlich eingestuft wurde. Das fördert richtiges Verhalten und motiviert Ihre Mitarbeiter, ähnliche Nachrichten auch weiterhin zu melden.

5. 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. Auch wenn Marken-Spoofing keine direkten finanziellen Schäden für Ihr Unternehmen bedeutet, kann es die Reputation und das Vertrauen Ihrer Kunden schädigen und langfristig zu nativen Auswirkungen führen.

Proofpoint schützt Ihre Marke und den Ruf Ihres Unternehmens vor Schäden durch E-Mail-Betrugsversuche. Dazu verhindern wir, dass betrügerische E-Mails über Ihre vertrauenswürdigen Domänen verschickt werden. Außerdem authentifizieren wir alle zugestellten und von Ihrem Unternehmen versendeten E-Mails. Durch die vereinfachte DMARC-Implementierung mit geführten Workflows und Managed Services unterstützen wir Sie bei der korrekten Veröffentlichung von DMARC-Richtlinien zur E-Mail-Ablehnung. Das verhindert wirksam den Missbrauch Ihrer Domäne und blockiert alle Versuche, nicht autorisierte E-Mails aus Ihren vertrauenswürdigen Domänen zu versenden.

Außerdem erhalten Sie einen Überblick über alle E-Mails, die unter Verwendung Ihrer E-Mail-Domäne versendet werden, einschließlich vertrauenswürdiger externer Versender. Wir identifizieren Doppelgänger Ihrer Domänen und erkennen dynamisch neu registrierte Domänen, die bei E-Mail-Betrugsversuchen oder auf Phishing-Websites Ihre Marke imitieren. Sobald verdächtige Domänen aus einem geparkten Status auf aktiv oder „scharf geschaltet“ werden, erhalten Sie sofort eine Warnmeldung.

Zudem zeigen wir Ihnen, wie Angreifer Ihre Marke in digitalen Kanälen imitieren, einschließlich E-Mail, Webdomänen, sozialen Netzwerken und dem Darknet. Dank des Überblicks über alle Bereiche und unseres Virtual Takedown-Services können Sie schnell die Anfälligkeit von Kunden und Geschäftspartnern durch schädliche Doppelgänger-Domänen verringern.

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
- 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**.