Proofpoint Threat Response Auto-Pull

Automatisches Verschieben in die Quarantäne von bereits zugestellten, schädlichen E-Mails

WICHTIGE VORTEILE

- Schädliche E-Mails, die vorhandene E-Mail-Filter passiert haben, werden automatisch in die Quarantäne verschoben
- Exponentielle Zeitersparnis für Sicherheits- und Messaging-Teams bei der Orchestrierung und Beantwortung von E-Mail-Sicherheitsfragen
- Nutzt Proofpoint-Bedrohungsdaten zur Überprüfung von Nachrichten
- Automatische Überwachung des Abuse-Postfachs auf Bedrohungen
- Verschiebt auch schädliche Nachrichten in die Quarantäne, die an Personen oder Verteilerlisten weitergeleitet wurden
- Identifiziert Phishing-Kampagnen auch auf Basis unvollständiger Meldungen und spart Zeit aufgrund falsch gemeldeter Nachrichten

Mit Proofpoint Threat Response Auto-Pull (TRAP) können Ihre Messaging- und Sicherheitsadministratoren den Reaktionsprozess bei E-Mail-Zwischenfällen optimieren. Wenn eine schädliche E-Mail erkannt wird, analysiert TRAP die bereits zugestellten E-Mails auf Übereinstimmung und entfernt automatisch alle Nachrichten aus den Posteingängen der Nutzer. Zudem werden unerwünschte E-Mails, die bereits die Posteingänge erreicht haben, in die Quarantäne verschoben. Mit TRAP erhalten Sie eine leistungsstarke Lösung, die den Zeitaufwand für die Bereinigung von E-Mails für Ihre Sicherheits- und Messaging-Teams exponentiell verringert.

Mehr als 90 % aller Cyber-Angriffe beginnen mit dem Senden einer E-Mail. Das macht die E-Mail zum Angriffsvektor Nr. 1. Je professioneller Cyberkriminelle werden, umso größer wird die Gefahr, Opfer einer schädlichen E-Mail zu werden. Schädliche E-Mails können Phishing-Links enthalten, die nach der Zustellung „vergiftet“ werden, oder Verschleierungstechniken nutzen, die zu False-Negatives führen und damit die Zustellung ermöglichen. E-Mail-Sicherheitsteams haben häufig die Aufgabe, Nachrichten zu analysieren und nachträglich aus den Postfächern zu löschen, um das Bedrohungspotenzial zu reduzieren und mögliche Schäden zu vermeiden. Auch wenn das Verschieben einer E-Mail in die Quarantäne wenig Aufwand bedeutet und innerhalb weniger Minuten erledigt ist, summiert sich der Aufwand deutlich, wenn dieser Vorgang für zehn oder mehr Postfächer manuell durchzuführen ist.

Vektorübergreifender Bedrohungsdatenaustausch mit Proofpoint Nexus Threat Graph

Der Proofpoint Nexus Threat Graph bietet branchenführende Aggregation und Korrelation von Bedrohungsdaten zu E-Mails, Cloud, Netzwerken sowie sozialen Netzwerken und ermöglicht Echtzeit-Schutz und -Reaktionen mit Ihren Proofpoint-Produkten. Da Nexus Threat Graph zur Proofpoint-Plattform gehört, müssen Sie nichts installieren, bereitstellen oder verwalten. Ihre Vorteile als Teil dieses Netzwerks und durch die Nutzung aktuellster Informationen zur Bedrohungslandschaft:

- Echtzeit-Bedrohungsdaten von der Community, die aus mehr als 115.000 Kunden besteht
- Überblick über mehrere Vektoren wie E-Mails, Cloud, Netzwerk und soziale Netzwerke
- Mehr als 100 Bedrohungsakteure werden überwacht, um deren Motive und Taktiken zu verstehen und verbesserten Schutz zu bieten

TRAP nutzt die Nexus Threat Graph-Daten, um Zusammenhänge zwischen Empfängern und Anwenderidentitäten herzustellen. Auf diese Weise werden zugehörige Kampagnen offengelegt und sogar für den Angriff verwendete IP-Adressen und Domänen auf Reputations- und Bedrohungsdatenlisten aufgedeckt. TRAP kann anschließend automatisierte Aktionen abhängig von den angegriffenen Anwendern durchführen, d. h. basierend darauf, ob sie zu bestimmten Abteilungen oder Gruppen mit besonderen Berechtigungen gehören.

Wenn wir am Kundenstandort eine E-Mail erkennen, die schädliche Links, Anhänge oder verdächtige IP-Adressen enthält, geben wir diese Information an die gesamte Kundenbasis weiter, um sie zukünftig bereits vor der Übertragung zu schützen. Außerdem werden alle schädlichen E-Mails, die in den Posteingang zugestellt wurden, von uns entfernt oder unter Quarantäne gestellt.

Erkennung und Verringerung von Phishing-Risiken mit CLEAR

Ein geschulter Mitarbeiter kann Ihre letzte Verteidigungslinie gegen einen Cyberangriff sein. Mit Closed-Loop Email Analysis and Response (CLEAR) wird der Zyklus aus Berichten, Analysen und Behebungen potenziell schädlicher E-Mails von Tagen auf Minuten verkürzt. Dank der Anreicherung mit Proofpoint-Bedrohungsdaten kann CLEAR aktive Angriffe mit einem einzigen Mausklick stoppen. Und das automatische Verschieben schädlicher Nachrichten in die Quarantäne spart Ihrem Sicherheitsteam Zeit und Arbeitsaufwand.

CLEAR ist eine Komplettlösung und kombiniert die Funktionen von PhishAlarm, der Schaltfläche zur Meldung potenzieller Phishing-Mails, sowie PhishAlarm Analyzer zur Kategorisierung und Priorisierung der gemeldeten E-Mails mithilfe von Proofpoint-Bedrohungsdaten. Außerdem ist TRAP enthalten, das den Nachrichtenkontext anreichert und schädliche Nachrichten automatisch entfernt.

Gemeldete Nachrichten werden zur Überprüfung durch CLEAR an ein Abuse-Postfach gesendet und auf die gleiche Weise mit TRAP überwacht und verarbeitet. Anschließend kommen in einem weiteren Schritt Bedrohungsdaten von Proofpoint und Drittanbietern zum Einsatz, um festzustellen, ob die Inhalte der E-Mail mit schädlichen Markern übereinstimmen. Diese als schädlich eingestuften Nachrichten werden automatisch aus allen Posteingängen der Empfänger entfernt.

Out-of-Band-Verwaltung von E-Mails

TRAP nutzt CSV-Dateien und Proofpoint SmartSearch. Sie können SmartSearch-Ergebnisse und CSV-Dateien hochladen oder manuelle Zwischenfälle mit wichtigen Informationen nutzen, um eine oder tausende Nachrichten in die E-Mail-Quarantäne zu verschieben. Innerhalb weniger Augenblicke lassen sich sicherheitsrelevante Schadmails sowie gegen Richtlinien verstoßende E-Mails aus Postfächern entfernen. Sie erhalten eine Aktivitätenliste mit Informationen dazu, wer die E-Mails gelesen hat und ob der Rückruf erfolgreich war oder fehlgeschlagen ist.

Automatisches Verschieben weitergeleiteter Nachrichten in die Quarantäne

Um das Risiko vollständig zu beheben, müssen auch alle schädlichen und unerwünschten E-Mails in die Quarantäne verschoben werden, die an andere Personen, Abteilungen oder Verteilerlisten weitergeleitet wurden. Der Versuch, all diese E-Mails zu finden und manuell in die Quarantäne zu verschieben, bereitet jedoch vielen Administratoren Bauchschmerzen. TRAP trägt diesem Problem mit integrierter Geschäftslogik und Intelligence Rechnung. Die Lösung erkennt, wenn Nachrichten weitergeleitet oder an Verteilerlisten gesendet werden, und überprüft automatisch die Empfänger, um diese Nachrichten zu finden und zurückzuziehen. Dadurch sparen Sie viel Zeit und Nerven.

Verbesserte Triage-Untersuchungen

Mit TRAP können SOC-Analysten bei Zwischenfällen, die URLs beinhalten, genauere Triage-Untersuchungen durchführen. Dabei werden die URLs mithilfe der Proofpoint Browser Isolation-Technologie in einer sicheren Umgebung untersucht, damit die Analysten den Inhalt der URL einschätzen und gleichzeitig das Unternehmen vor Risiken schützen können.

WEITERE INFORMATIONEN

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