

PROOFPOINT THREAT RESPONSE AUTO-PULL

ZUGESTELLTE SCHÄDLICHE E-MAILS WERDEN AUTOMATISCH IN DIE QUARANTÄNE VERSCHOBEN

WICHTIGE VORTEILE

- Weniger Zeit bis zur Quarantäne und Eindämmung von E-Mail-Bedrohungen
- Weniger Expositionszeit bössartiger E-Mails
- Quarantänenachrichten werden an Verteilerlisten oder einzelne Personen weitergeleitet
- Empfang eines prüffähigen Verlaufs an Antwortaktionen, um die Rentabilität der bestehenden Infrastruktur zu fördern
- Geringere Abhängigkeit von kundenkodierter Software
- Empfang von E-Mail-Benachrichtigungen für Problemänderungen und Quarantänebestätigungen
- Einstellen flexibler Benachrichtigungen für die einfache Integration in Ticketingsysteme
- Automatische Überwachung und Prüfung missbrauchter Posteingänge auf Bedrohungen
- Wiederherstellung unter Quarantäne stehender Nachrichten durch die Option „Rückgängig machen“
- Bereinigung von Nachrichtengruppen mithilfe von CSV-Dateien oder SmartSearch-Ergebnissen

Proofpoint Threat Response™ ist die erste Bedrohungsmanagement-Plattform, die die Koordination und Automatisierung ausdehnt, damit schädliche E-Mails, die in die Posteingänge der Benutzer gelangt sind, widerrufen werden können. Threat Response Auto-Pull ist eine Einsteigerversion der Plattform, die schädliche E-Mails aus den Händen der Benutzer zieht und zusätzliche Geschäftslogik einsetzt, um evtl. weitergeleitete interne Kopien dieser Nachricht zu finden und zu löschen.

In vielen Organisationen ist die Behandlung von Sicherheitsvorfällen ein langsamer, arbeitsaufwendiger Vorgang. Es kann mitunter Tage oder Wochen dauern, bis E-Mail-Sicherheitsvorfälle angesprochen werden, und ihre Beseitigung kostet große Mühe. Der Umgang mit zugestellter E-Mail, die Malware, schädliche URLs oder Anmeldeinformationen-Phishing enthält, umfasst viele Schritte, darunter:

- Verbindung der E-Mail-Adresse mit einer internen Identität
- Suchen und Finden ausgewählter, schädlicher Nachrichten auf dem Server
- Entfernen schädlicher Nachrichten aus dem Posteingang des Benutzers oder anderen Ordnern
- Erkennen, welche schädlichen Nachrichten weitergeleitet wurden und das Verschieben dieser E-Mails in die Quarantäne

Das Wiederholen dieser Aufgaben für jeden E-Mail-Vorfall kann täglich viele Stunden dauern und ein bereits strapaziertes Sicherheits- und Nachrichtenteam überwältigen.

BEREINIGUNG ABGEFANGENER NACHRICHTEN

Bei der Bereinigung von schädlichen E-Mails handelt es sich oft um einen manuellen Prozess, der mit einer Warnung oder Beschwerde beginnt, dass eine schädliche E-Mail durchgelassen wurde.

Oberflächlich betrachtet, könnte die Bereinigung eines E-Mail-Vorfalles einfach aus einem Blick in den Posteingang und dem Löschen einer Nachricht bestehen – jedoch könnte sich das als kostspielige Prämisse herausstellen. Übliche Fehlschritte bei der Bereinigung beruhen auf einer groben Vereinfachung des Prozesses, bei dem der Nachrichtenumfang und alles, was über einen einfachen Fall hinausgeht, übersehen werden. Andere wichtige Überlegungen umfassen:

- Befindet sich die E-Mail nur im Posteingang oder wurde sie in einen anderen Ordner verschoben?
- Sollten Sie andere Ordner nach Kopien der Nachrichten absuchen?
- Wurde die Nachricht intern weitergeleitet? Falls ja, an wen und wie viele Kopien gibt es?
- Gibt es einen Prüfpfad oder Bericht aller Maßnahmen?

Es gibt noch andere Variablen, die eine erfolgreiche E-Mail-Bereinigung beeinflussen können, was zu DIY und hausgemachten E-Mail-Bereinigungsskripten geführt hat. Diese bergen ganz eigene Risiken.

GEFAHREN VON DIY UND KUNDENSPEZIFISCHEN CODES

Das Erstellen und Ausführen eines benutzerdefinierter Codes zum Bereinigen von E-Mails war die De-facto-Lösung für die Zustellung schädlicher E-Mails.

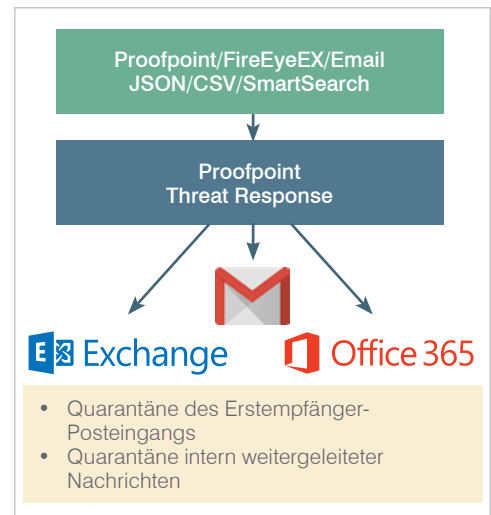
Daran ist prinzipiell nichts verkehrt, doch stellt der Aufbau und die Ausführung des kundendefinierten Codes eine Verpflichtung dar, die Entwicklungsfragen an die Standardsoftware mit sich bringt:

- Gibt es Spezifikationen oder führt der Kundencode nur eine Funktion aus und benötigt keine volle Spezifikation?
- Wie wird das Skript gepflegt? Gibt es einen Inhaber, der Probleme lösen kann? Was geschieht, wenn der Entwickler das Unternehmen verlässt?
- Wenn das Skript gegen Fremdprodukte wirkt, wer überwacht die Produktversionierung, das Testen, die Oberflächen- oder API-Änderungen der Fremdprodukte?

Außer diesen offensichtlichen technischen Anliegen verlangt die Geschäftsseite noch, dass der Kundencode Geschäftslogik- und Transparenzziele erfüllt.

Dazu gehört häufig:

- Überwachung der fortlaufenden Ausführung des Codes
- Messung und Verfolgung der Effektivität des Codes
- Gewähr, dass alle schädlichen Versionen der Nachricht, auch die weitergeleiteten, verarbeitet wurden.



ZIEHEN SIE THREAT RESPONSE AUTO-PULL IN BETRACHT

Threat Response Auto-Pull ist eine Einsteigerversion von Threat Response, die die E-Mail-Quarantänefunktion nach der Installation in Verbindung mit Proofpoint Targeted Attack Protection (TAP) und entweder O365 E-Mail oder Exchange lokal bereitstellt. TR Auto-Pull akzeptiert auch FireEye EX CSV-Dateien, SmartSearch und JSON-Warnungen.

Der Nutzungsfall ist einfach – wenn eine schädliche E-Mail erkannt wird, senden die Erkennungssysteme eine Warnung an Threat Response mit Informationen über diese Nachricht. Threat Response verschiebt die Nachricht anschließend von Exchange, Office 365 und/oder Gmail in die Quarantäne. Auto-Pull sucht darüber hinaus nach weitergeleiteten Kopien der Nachricht sowie nach Verteilungslisten der Empfänger der Nachricht in anderen Posteingängen auf demselben Server und verschiebt diese ebenfalls in eine Quarantäne mit beschränktem Zugang.

VORINSTALLIERTE INTEGRATIONEN

Threat Response Auto-Pull umfasst Adapter für den minutenschnellen Anschluss an Exchange-, Office 365-, Gmail-, CSV-, SmartSearch-, TAP-, FireEye EX- und JSON-Quellen, damit Sie keine zusätzlichen Systeme oder Verbindungselemente erwerben müssen. Administratoren benötigen nur die entsprechenden Anmeldeinformationen für Exchange und O365, um die E-Mail zurückzuziehen. Außerdem überwacht Threat Response Auto-Pull automatisch missbrauchte Posteingänge und Nachrichten, die dorthin gesendet werden, um sie mit Informationen aus Reputations-Datenbanken abzugleichen.

AUTO-PULL- ODER UMFASSENDES THREAT RESPONSE-PROGRAMM

Während Auto-Pull zwar E-Mail-Sicherheitsvorfälle anspricht, sollten Sicherheitsfachleute auch das umfassende Threat Response-Programm in Betracht ziehen, das über die E-Mail-Quarantäne hinausgeht und folgende erwägenswerte Funktionen umfasst:

- Die Sicherheitskoordination und Automation der Vorfallsreaktion
- Hinzufügen von Kontext und Intelligenz, um die Problemerkennung abzukürzen
- Sammlung und Prüfung von Endpunkt-Forensik gegen Sandbox-Forensik
- Annahme und Übernahme von Fremdintelligenz für alle Vorfälle
- Quarantäne und Eindämmung von Bedrohungen über Firewalls, Proxys und AD
- Echtzeitberichte über Kampagnen, Benutzer, Vorfälle, Bedrohungen und Ziele

ZUSAMMENFASSUNG

Threat Response Auto-Pull kann die proaktive, automatische Quarantäne und Eindämmung von schädlichen E-Mails bieten, die dem Posteingang zugestellt wurden, einschließlich intern weitergeleiteter Nachrichten. Sicherheitspersonal sollte über das umfassende Threat Response-Programm nachdenken, um Zeit, Effektivität und andere Funktionen zu erhalten, die über die Bearbeitung von E-Mail-Vorfällen hinausgehen.

„...es wurde mit TAP und AD bereitgestellt und integriert und begann innerhalb weniger Stunden mit der automatischen Löschung von Nachrichten.“

**Unbenannter Kunde,
Gesundheitswesen**

ÜBER PROOFPOINT

Proofpoint Inc. (NASDAQ: PFPT), ein Unternehmen für Internetsicherheitslösungen der nächsten Generation, ermöglicht Organisationen, das Arbeitsumfeld ihrer Mitarbeiter vor modernen Bedrohungen und Compliance-Risiken zu schützen. Proofpoint hilft Internetsicherheitsexperten dabei, ihre Anwender vor den hochentwickeltesten Angriffen zu schützen, die in E-Mails, mobilen Apps und in den sozialen Netzwerken gegen sie gerichtet werden. Das Unternehmen schützt die von den Mitarbeitern erstellten wichtigen Daten und stützt Teams mit den richtigen Informationstools aus, die ihnen bei Problemen eine schnelle Reaktion ermöglichen. Führende Unternehmen aller Größenordnungen, darunter mehr als 50 Prozent der Fortune 100-Unternehmen, vertrauen auf Proofpoint-Lösungen, die für die mobilen und von den sozialen Netzen geprägten Umgebungen der heutigen Zeit konzipiert sind. Zur Bekämpfung der modernen Bedrohungen stützen sich die Lösungen sowohl auf die Macht der Cloud als auch auf eine große datengesteuerte Analyseplattform.

©Proofpoint, Inc. Proofpoint ist eine Marke der Proofpoint, Inc. in den USA und anderen Ländern. Alle anderen aufgeführten Produkt- und Firmennamen sind Eigentum ihrer jeweiligen Inhaber.