proofpoint.

PROOFPOINT CLOSED-LOOP EMAIL ANALYSIS AND RESPONSE

VERRINGERUNG DES PHISHING-RISIKOS MIT EINEM EINZIGEN KLICK

PRODUKTE

- PhishAlarm
- PhishAlarm Analyzer
- Threat Response Auto-Pull (TRAP)

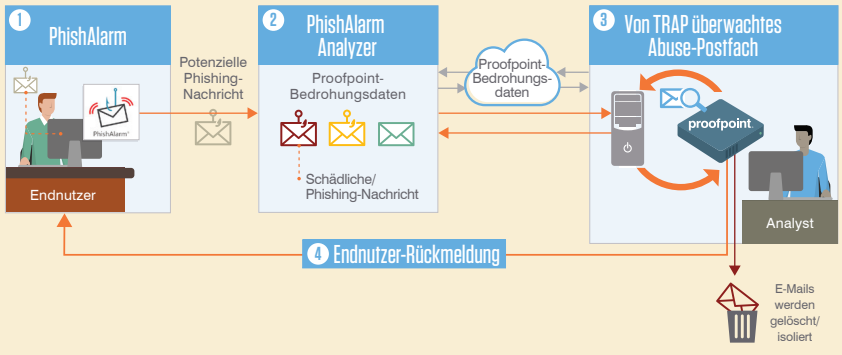
WICHTIGE VORTEILE

- Endnutzer können verdächtige Nachrichten mit einem einzigen Mausklick melden, automatisch analysieren und beheben lassen
- Zeitersparnis durch Automatisierung – schädliche Nachrichten werden aus dem Postfach des Absenders entfernt und zurückgezogen bzw. isolierte Nachrichten nachverfolgt
- Zur Optimierung des Behebungsprozesses werden standardmäßig exklusive Proofpoint-Bedrohungsdaten genutzt
- Detaillierte und auditfähige Dokumentation vorgenommener Aktionen

Geschulte und aufmerksame Mitarbeiter können Phishing-Versuche von legitimen E-Mails unterscheiden. Die empfohlenen Vorgehensweisen sehen meist vor, dass verdächtige Phishing-E-Mails erkannt und an das Sicherheitsteam oder ein Abuse-Postfach zum Melden schädlicher E-Mails weitergeleitet werden. Die Reaktionsteams sind jedoch häufig nicht ausreichend ausgestattet, um die gemeldeten Bedrohungen schnell zu priorisieren und zu beheben. Das Risiko einer längeren Gefährdung ist daher hoch und steigert wiederum das Gesamtrisiko für das Unternehmen. Wenn der Phishing-Versuch nicht entdeckt wird, verpassen die internen Sicherheitsteams eine Gelegenheit, potenzielle Kampagnen aufzudecken oder die Schutzmaßnahmen zu verbessern, noch bevor das Unternehmen von einer größeren Angriffswelle getroffen wird. Proofpoint Closed-Loop Email Analysis and Response (CLEAR) kann die Produktivitätsverluste und damit einhergehende finanzielle Einbußen durch laufende Angriffe verringern.

Mit einem einzigen Mausklick stellt CLEAR einen Überblick über aktive Angriffe bereit und ermöglicht die automatische intelligente Analyse sowie die Behebung potenzieller Phishing-Angriffe. CLEAR ist eine Komplettlösung und kombiniert die Funktionen der PhishAlarm-Schaltfläche zur E-Mail-Meldung, von PhishAlarm Analyzer, das Nachrichten anhand von Proofpoint-Bedrohungsdaten kategorisiert und priorisiert, sowie von Threat Response Auto-Pull (TRAP) für die Anreicherung von Nachrichtenkontext und automatische Behebung.

CLEAR WORKFLOW



MEHR MÖGLICHKEITEN MIT EINER EINZIGEN SCHALTFLÄCHE

Die PhishAlarm-Schaltfläche gibt Ihrem Sicherheitsteam einen besseren Überblick über eingehende Phishing-E-Mails, die von Ihren Mitarbeitern gemeldet werden.

Wenn PhishAlarm-Nutzer eine verdächtige E-Mail erhalten, klicken sie wie üblich auf die Schaltfläche „Report Phish“ (Phishing-Versuch melden). Wenn CLEAR implementiert ist, sendet PhishAlarm die E-Mail an PhishAlarm Analyzer. PhishAlarm Analyzer bewertet und kategorisiert gemeldete E-Mails auf intelligente Weise mithilfe der Proofpoint-Bedrohungsdaten. Dazu wird die E-Mail in einer Sandbox-Umgebung auf Bedrohungen untersucht. Der sich daraus ergebende Wert unterstützt die bessere Priorisierung und weitere Verarbeitung durch TRAP. Basierend darauf kann TRAP mithilfe von Sicherheitsautomatisierung sowie Koordinierung den Bedrohungskontext ergänzen und automatisch im gesamten Unternehmen weitere Vorkommen dieser schädlichen E-Mail entdecken.

SCHUTZ DURCH AUTOMATISIERUNG

TRAP überprüft das Abuse-Postfach ständig auf neue E-Mails und entfernt sowie isoliert sie nach dem Eingang.

Innerhalb von Sekunden analysiert TRAP diese Daten mithilfe mehrerer Bedrohungsdaten- und Reputationssysteme und kann auf diese Weise feststellen, ob eines dieser Elemente tatsächlich schädlich ist.

TRAP zeigt zudem den geografischen Standort der verdächtigen IP-Adressen an. Die Lösung korreliert automatisch verdächtige E-Mails mit aktuellen Angriffskampagnen und erstellt damit ohne zusätzlichen Aufwand eine Übersicht über potenzielle Bedrohungen. Dank dieser Erkenntnisse kann Ihr Team schnell reagieren und so Ihre Anwender sowie Daten schützen.

TRAP nutzt standardmäßig die branchenweit besten Reputations- und Bedrohungsdaten-Feeds. Außerdem verfügt die Lösung bereits über eine Geschäftslogik für E-Mails, sodass sie Nachrichten schnell erkennen und entfernen kann, die Anmeldedaten-Phishing, Malware-Links und schädliche Anhänge enthalten.

Weiterhin sind standardmäßig Funktionen zur Behandlung von Sicherheitsvorfällen sowie Berichterstellung enthalten. Ihre Sicherheitsteams müssen keinen Code schreiben und nach der Ersteinrichtung keine weiteren Integrationen vornehmen. Stattdessen haben sie folgende Möglichkeiten:

- Einen Vorfall erstellen
- E-Mail-Header analysieren
- Absender-IP-Adressen überprüfen
- Absenderdomäne überprüfen
- Absenderreputation untersuchen
- Links analysieren, die zu Anmeldedaten-Phishing oder Malware führen
- Anhänge auf Bedrohungen, Malware oder andere aktive Inhalte analysieren
- Das Erstellen und Pflegen von YARA-Regeln und manuellen Skripten überflüssig machen

TRAP erstellt eine Bedrohungsbewertung, ermittelt den geografischen Standort und verknüpft Informationen aus E-Mails, sodass Analysten schnell eine Übersicht der potenziellen Bedrohung erhalten.

VERRINGERUNG DES RISIKOS SCHÄDLICHER E-MAILS

E-Mail-Administratoren können schädliche E-Mails manuell oder automatisch aus den Absenderpostfächern entfernen. TRAP verfolgt weitergeleitete E-Mails und erweitert Empfängerlisten, damit weitergeleitete Nachrichten auch dann zurückgezogen werden können, wenn diese an Verteilerlisten weitergeleitet wurden. In diesem Fall entfernt und isoliert TRAP die E-Mails. Alle an das Abuse-Postfach gesendeten schädlichen E-Mails werden aus den Postfächern Ihrer Anwender entfernt, sodass die Risiken verringert werden.

Unabhängig davon, wie viele E-Mails Ihr Abuse-Postfach umfasst, können Sie mit CLEAR schon heute Ihr Phishing-Risiko senken.

GESCHLOSSENER KREIS DER E-MAIL-BERICHTE

Endnutzer erhalten Rückmeldungen zu allen gemeldeten Nachrichten, ganz gleich, ob diese tatsächlich schädlich waren, als Massen-E-Mails eingestuft wurden oder sich als harmlos erwiesen haben. Damit wird der Kreis der E-Mail-Berichte geschlossen. Auf diese Weise werden die Endnutzer motiviert, Nachrichten zu melden, und verbessern so die Sicherheit Ihres Unternehmens. Wenn Nachrichten als Massen-E-Mails oder harmlos eingestuft werden, kann TRAP die Sicherheitsteams von der weiteren Untersuchung entlasten, und die Vorfälle werden automatisch geschlossen. Dies schließt den Kreislauf für unschädliche E-Mails.

WEITERE INFORMATIONEN

Weitere Informationen erhalten Sie unter proofpoint.com/de oder von Ihrem örtlichen Proofpoint-Vertriebsrepräsentanten.

Hinweis: Für die oben beschriebene Automatisierung sind PhishAlarm, PhishAlarm Analyzer und TRAP erforderlich.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) ist ein führendes Cybersicherheitsunternehmen. Im Fokus steht für Proofpoint dabei der Schutz der Mitarbeiter. Denn diese bedeuten für ein Unternehmen zugleich das größte Kapital aber auch das größte Risiko. Mit einer integrierten Suite von Cloud-basierten Cybersecurity-Lösungen unterstützt Proofpoint Unternehmen auf der ganzen Welt dabei, gezielte Bedrohungen zu stoppen, ihre Daten zu schützen und IT-Anwender in den Unternehmen für Risiken von Cyberangriffen zu sensibilisieren. Führende Unternehmen aller Größen, darunter mehr als die Hälfte der Fortune-1000-Unternehmen, verlassen sich auf Proofpoint, um ihre wichtigsten Sicherheits- und Compliance-Risiken bei der Nutzung von E-Mails, der Cloud, Social Media und dem Internet zu minimieren. www.proofpoint.com/de