Proofpoint Targeted Attack Protection

Transparenz und Schutz vor hochentwickelten Bedrohungen

WICHTIGE VORTEILE

- Erkennt, analysiert und blockiert hochentwickelte Bedrohungen, noch bevor sie die Posteingänge der Anwender erreichen
- Einzigartige Einblicke zu Ihren Very Attacked People und zum Sicherheitsrisiko für Ihr Unternehmen
- Nutzung von Proofpoint-Bedrohungsdaten zur Abwehr von Bedrohungen; detaillierte Forensikdaten zu Angriffen
- Adaptive Sicherheitskontrollen mit URL-Isolierung und Security Awareness-Training
- Schutz vor URL- und webbasierten Angriffen, damit VAPs sicher unbekannte Websites aufrufen können, auf die in geschäftlichen E-Mails verwiesen wird (Bestandteil unserer Bundle-Angebote)

Mehr als 90 % der gezielten Angriffe auf Unternehmen beginnen mit einer E-Mail[1] und diese Bedrohungen entwickeln sich ständig weiter. Proofpoint Targeted Attack Protection (TAP) bietet einen innovativen Ansatz, der hochentwickelte Bedrohungen, die gegen Ihre Mitarbeiter gerichtet sind, erkennt, analysiert und blockiert. Zudem können Sie dank der einzigartigen Übersicht über diese Bedrohungen Ihre Gegenmaßnahmen optimieren.

TAP wehrt sowohl bekannte als auch komplett neue E-Mail-Angriffe ab. Die Lösung erkennt und blockiert polymorphe Malware, manipulierte Dokumente, Anmeldedaten-Phishing und weitere hochentwickelte Bedrohungen. Sie überwacht die Aktivitäten von Cloud-Anwendungen, um verdächtige Zugriffe, umfassende Dateiweitergaben, riskante Drittanbieter-Anwendungen uvm. aufzudecken. Zudem erhalten Sie die notwendigen Informationen, um Ihre am häufigsten angegriffenen Mitarbeiter identifizieren und schützen zu können.

Schutz vor BEC-, URL-, Anhang- und Cloud-basierten Bedrohungen

TAP greift auf statische sowie dynamische Techniken zurück, um jegliche neuen Angriffsmuster erkennen und abwehren zu können. Wir analysieren potenzielle Bedrohungen mit verschiedenen Ansätzen, die Verhalten, Code sowie verwendete Protokolle überprüfen. Auf diese Weise lassen sich Bedrohungen schon früh in der Angriffskette erkennen, so dass ein Schaden für das Unternehmen abgewendet werden kann.

TAP schützt vor Bedrohungen mit Business Email Compromise (BEC, auch als Chefmasche bezeichnet) und kompromittierten Lieferantenkonten. Diese Angriffsformen erfolgen häufig ohne Schaddaten, sodass für die Identifizierung hochentwickelte Erkennungstechniken erforderlich sind, die über Sandbox-Analysen hinausgehen. Unser Threat Intelligence-Modul Proofpoint Nexus Threat Graph unterstützt TAP. Es erfasst, analysiert und korreliert eine Billion Datenpunkte zu E-Mails, Cloud, Netzwerken, Endpunkten und sozialen Netzwerken. Das Erkennungsmodul Advanced BEC Defense wurde basierend auf umfangreichen Bedrohungsdaten erstellt und trainiert. Es lernt in Echtzeit, damit Sie bei Veränderungen in der Bedrohungslage schnell reagieren können.

Für die Untersuchung einer Vielzahl von Angriffen nutzen wir Sandbox-Analysen. Zu diesen Angriffen gehören solche mit schädlichen Anhängen und URLs, mit denen Malware installiert oder Benutzer zur Weitergabe von vertraulichen Informationen verleitet werden sollen. Unsere Untersuchungen werden zudem von Proofpoint-Analysten überwacht, um damit die Erkennung weiter zu verbessern und wertvolle Bedrohungsdaten zu erhalten.

Damit Sie bessere Erkenntnisse über Cloud-Angriffe erhalten, erkennt TAP auch Bedrohungen sowie Risiken in Cloud-Anwendungen und korreliert sie mit Anmeldedaten-Diebstahl oder anderen E-Mail-Attacken. Unsere Technologie erkennt nicht nur Bedrohungen, sie nutzt auch Machine Learning zur Erkennung der Muster, Verhaltensweisen und Techniken, die bei jedem Angriff eingesetzt werden. Mithilfe dieser Erkenntnisse lernt TAP stetig dazu und ist in der Lage sich anzupassen, um künftige Angriffe noch schneller zu entdecken.

1 Verizon: „Data Breach Investigations Report“ (Untersuchungsbericht zu Datenkompromittierungen), Juli 2019.

Advanced BEC Defense

Advanced BEC Defense schützt vor BEC-Angriffen sowie kompromittierten Lieferantenkonten und führt eine umfassende und detaillierte Analyse von Nachrichten dieser Aspekte durch:

- Header-Forensik
- IP-Adresse des Absenders
- Absender-/Empfänger-Beziehung
- Analyse der Reputation
- Detaillierte inhaltliche Analyse

Advanced BEC Defense bietet zudem einen detaillierteren Überblick über die Techniken der Angreifer, Beobachtungen zu Bedrohungen sowie Nachrichtenbeispiele. Dadurch verstehen Sie besser, wie Ihre Mitarbeiter gezielt angegriffen werden.

URL Defense

TAP URL Defense wehrt URL-basierte E-Mail-Bedrohungen wie Malware und Anmeldedaten-Phishing ab. Die Lösung bietet einzigartige prädiktive Analysen, die verdächtige URLs anhand von Mustern im E-Mail-Datenverkehr identifizieren und diese in einer Sandbox überprüfen. Alle URLs, die den Posteingang erreichen, werden transparent umgeschrieben, sodass die Anwender unabhängig vom verwendeten Endgerät oder Netzwerk geschützt bleiben. Bei jedem Klick auf eine URL wird in Echtzeit eine Sandbox-Analyse ausgeführt.

Attachment Defense

TAP Attachment Defense bietet Schutz vor bekannten sowie unbekannten Bedrohungen, die mittels Anhängen in E-Mails übertragen werden. Die Komponente bietet Schutz vor Bedrohungen, die in einer Vielzahl von Dateitypen, kennwortgeschützten Dokumenten, Anhängen mit eingebetteten URLs und ZIP-Dateien verborgen sind.

SaaS Defense

TAP SaaS Defense ist kompatibel mit Microsoft 365 oder Google Workspace (ehemals G Suite) und legt verdächtige Anmeldeaktivitäten offen. Dazu gehören ungewöhnliche Standorte für Anmeldungen sowie extrem häufige Anmeldeversuche und -fehler. Zudem gibt TAP SaaS Defense Warnungen aus, wenn zu viele Verbindungen von bekannt schädlichen IP-Adressen geöffnet werden. Sie erhalten einen Überblick über umfassende Datenweitergaben – sowohl an interne als auch externe Personen. Auf diese Weise sehen Sie, ob vertrauliche Daten innerhalb der letzten 30 Tage potenziell exfiltriert wurden. Außerdem schützt TAP SaaS Defense wichtige und besonders gefährdete Drittanbieter-Anwendungen, die in Ihrem Unternehmen eingesetzt werden.

Isolation for VAP*

TAP URL Isolation for VAP bietet Echtzeit-Phishing-Erkennung und schützt Ihre Very Attacked People (VAPs, besonders häufig angegriffene Personen) vor URL- und webbasierten Angriffen. Mithilfe unserer Lösung Browser Isolation können Ihre VAPs bedenkenlos URLs in geschäftlichen E-Mails aufrufen, da das Unternehmen zuverlässig geschützt ist.

Umfangreiche Einblicke zu Bedrohungen und Zielen

Proofpoint hat einen vollständigen Überblick über mehrere Bedrohungsvektoren, einschließlich E-Mail, Cloud, Netzwerk und soziale Netzwerke. Die Bedrohungsdaten basieren auf einem Kundenstamm mit mehr als 115.000 Kunden auf der ganzen Welt. Die Daten werden an Proofpoint Nexus Threat Graph übertragen, wo sie korreliert werden, um den Überblick über die Bedrohungslandschaft zu verbessern. Sie erhalten diese und weitere wichtige Erkenntnisse über das TAP Threat Insight-Dashboard, das Echtzeitinformationen zu Bedrohungen und Kampagnen detailliert aufzeigt. Mithilfe dieser Daten sehen Sie sowohl weit verbreitete als auch sehr zielgerichtete Angriffe. Bedrohungsdetails umfassen die betroffenen Anwender, Screenshots von Angriffen sowie umfangreiche Forensikdaten.

Very Attacked People

Mit dem Proofpoint Attack Index können Ihre Sicherheitsteams Ihre VAPs und damit die wichtigsten Ziele in Ihrem Unternehmen identifizieren. Dieser Index ist eine gewichtete zusammengefasste Bewertung aller Bedrohungen, die an eine Person in Ihrem Unternehmen gesendet werden. Er stuft Bedrohungen auf einer Skala von 0 bis 1.000 ein: Raffinesse des Bedrohungsakteurs, Genauigkeit und Fokus des Angriffs, Art des Angriffs und Angriffsvolumen insgesamt. Durch ein besseres Verständnis Ihrer VAPs können Sie die effektivste Methode zur Abwehr dieser Bedrohungen einsetzen.

Unternehmensweiter Attack Index

Der Attack Index kann auf Unternehmensebene angewendet und mit anderen Branchen verglichen werden, damit Sie das Risiko für Ihr Unternehmen quantifizieren können. Dieser Bericht verdeutlicht Ihrem CISO sowie dem Sicherheitsteam, wie Ihr Unternehmen im Vergleich zu ähnlichen Organisationen in anderen Branchen abschneidet. Sie erhalten auch Informationen über die Häufigkeit von Angriffen sowie die Arten von Bedrohungen. Dadurch können Sie die passenden Sicherheitskontrollen für Ihre individuelle Angriffssituation priorisieren.

* Nur für Kunden mit Lizenz für Bundle-Angebote verfügbar.

WEITERE INFORMATIONEN

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