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 Unternehmens
- Nutzung von Proofpoint-Bedrohungsdaten zur Abwehr von Bedrohungen; detaillierte Forensikdaten zu Angriffen
- Adaptive Sicherheitskontrollen mit URL-Isolierung und Security Awareness-Training

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 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.

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 in 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: „Cost of a Data Breach Investigations Report“ (Untersuchungsbericht zu den Kosten von Datenkompromittierungen), Juli 2019.

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 (Office 365) sowie Google 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 zu 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 exfiltiert wurden. Außerdem schützt TAP SaaS Defense wichtige und besonders gefährdete Drittanbieter-Anwendungen, die in Ihrem Unternehmen eingesetzt werden.

UMFANGREICHE EINBLICKE ZU BEDROHUNGEN UND ZIELEN

Proofpoint bietet Bedrohungsdaten, die E-Mails, Cloud, Netzwerke, Mobilgeräte-Apps und soziale Netzwerke abdecken. Unser Bedrohungsdiagramm, das auf den Bedrohungsdaten aus unserer Community basiert, umfasst mehr als eine Billion Datenpunkte. Es korreliert Informationen zu Angriffskampagnen gegen unterschiedliche Branchen und geografische Regionen. Sie erhalten diese und weitere wichtige Informationen über das TAP Threat Insight-Dashboard übersichtlich dargestellt und können die Erkenntnisse daraus ganz unkompliziert nutzen. Dieses Dashboard bietet in Echtzeit detaillierte Informationen zu Bedrohungen sowie zu Angriffskampagnen. 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 (VAPs)

Um die Personen schützen zu können, die in Ihrem Unternehmen am häufigsten angegriffen werden, müssen Ihre Sicherheitsteams diese Mitarbeiter kennen. Der Proofpoint Attack Index erleichtert das Identifizieren dieser Very Attacked People (VAPs™). Dieser Index ist eine gewichtete zusammengefasste Bewertung aller Bedrohungen, die an eine Person in Ihrem Unternehmen gesendet werden. Er stuft Bedrohungen anhand von vier Faktoren 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 Angriffsindex

Der Angriffsindex 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.

WEITERE INFORMATIONEN

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