proofpoint

TARGETED ATTACK PROTECTION (TAP)

SCHÜTZEN SIE IHR PERSONAL VOR ERWEITERTEN BEDROHUNGEN IN E-MAILS

Bedrohungsakteure nutzen die Tools aus, die Ihr Personal anwendet, um Ihre Endpunkte zu infiziern, Anmeldedaten zu stehlen und auf Ihre Daten zuzugreifen. Darum erreichen über 90 % aller gezielten Angriffe ihre Opfer über E-Mail.

Traditionelle Cybersicherheitslösungen nutzen veraltete Methoden, wie Reputation und Signaturen, die nicht mehr ausreichen, um bösartige E-Mail zu erkennen und zu stoppen. Malware-Techniken haben sich rapide weiterentwickelt und um damit Schritt halten zu können, muss die Technologie zum Schutz vor diesen Bedrohungen ebenfalls voranschreiten.

Proofpoint Targeted Attack Protection (TAP) hilft Ihnen, erweiterte Bedrohungen zu erkennen, einzudämmen und zu lösen, die Ihre Mitarbeiter durch E-Mail anvisieren. Wir erkennen bekannte Bedrohungen und neue, noch nie zuvor gesehene Angriffe, die bösartige Anhänge und URLs verwenden,um Malware auf einem Gerät zu installieren oder den Benutzer dazu zu verleiten, Passwörter und andere empfindliche Daten bekanntzugeben. TAP ist unübertroffen beim Stoppen gezielter Angriffe, die polymorphe Malware, infizierte Dokumente und Phishing-Techniken verwenden, um an empfindliche Informationen heranzukommen, empfindliche Informationen abzurufen oder Geld zu stehlen.

TAP ist die erste Verteidigungslinie an unserem E-Mail-Gateway. TAP besteht aus zwei Teilen:

Anhangs-Abwehr: TAP kann Nachrichten zurückhalten, bis die Analyse des Anhangs ein Urteil festlegt. Saubere Anhänge werden an den Posteingang geliefert, Bedrohungen werden unter Quarantäne gestellt.

URL-Abwehr: Nachrichten, die URLs enthalten, die bekanntermaßen schädlich sind, werden umgehend unter Quarantäne gestellt. TAP schreibt alle anderen URLs um, um das Anklicken zu verfolgen und zu blockieren. Wenn ein Benutzer auf die umgeschriebene URL klickt, wird er je nach Ergebnis der Inspektion von TAP an die Original-Webseitepage oder eine benutzerdefinierbare Sperrseite umgeleitet, die den Zugang zu schädlichen Sites blockiert.

STOPPEN VON BEDROHUNGEN, BEVOR SIE DEN POSTEINGANG ERREICHEN

TAP ist in die nächste Generation der Proofpoint E-Mail-Sicherheitsplattform eingebaut, die deutliche Transparenz in alle E-Mail-Kommunikationen bieten. Das bedeutet, dass TAP über mehr Kontext zur Extraktion von Bedrohungsintelligenz verfügt und die Angriffsoberfläche schnell entschärfen kann, indem schädliche Nachrichten blockiert und das Sicherheitsrisiko reduziert werden.

Andere erweiterte Bedrohungslösungen im Handel können den SMTP-Verkehr prüfen, um Bedrohungen über das Netzwerk zu erkennen. Diesem Ansatz mangelt es jedoch an Kontext, um zu verstehen, wer von der Bedrohung betroffen ist, und sie können keinen verschlüsselten Netzwerkverkehr prüfen.

WICHTIGE LEISTUNGEN

- **Bedrohungen stoppen, bevor sie im Posteingang landen**
- **Bekannte und unbekannte Bedrohungen in der E-Mail erkennen**
- **Mit durchgehendem Einblick reagieren**
- **Schnelle Bereitstellung und umfassender Schutz überall**

Daher bieten diese Lösungen nur eine beschränkte Sicht der E-Mail-Gefahrenlandschaft. Darüber hinaus können sie keine Zero-Day-Bedrohungen vor der Lieferung an den Posteingang stoppen, da sie nicht im E-Mail-Fluss integriert sind.

ERKENNUNG BEKANNTER UND UNBEKANNTER BEDROHUNGEN DURCH KOMPLEXE, ANPASSUNGSFÄHIGE TECHNIKEN

Die Gefahrenlandschaft ist ständigem Wandel unterworfen. Darum passen sich auch unsere erweiterten Bedrohungslösungen ständig an, um neue Angriffsmuster zu erkennen. TAP inspiziert die gesamte Angriffskette mit statischen und dynamischen Methoden. Wir analysieren potentielle Bedrohungen in mehreren Stufen anhand verschiedener Ansätze zur Untersuchung von Verhaltensmustern, Quellcodes und Protokollen. Da Vorbeugung besonders wichtig ist, sind unsere Lösungen so konzipiert, dass Bedrohungen so früh wie möglich in der Angriffskette erkannt werden. TAP verwendet einzigartige Funktionen, wie beispielsweise vorhersagende Analysen, um verdächtige URLs zu erkennen und zu isolieren, bevor der Benutzer darauf klicken kann.

Wir wissen, dass sich die Angriffsmuster zum Schutz vor Erkennung ändern. Und manche Bedrohungen, wie beispielsweise Phishing-Angriffe, hinterlassen keine erkennbaren Spuren. Unsere Technologien sind so aufgebaut, dass sie Bedrohungen nicht nur erkennen, sondern auch daraus lernen. Wir können die Muster, Taktiken, Verhalten und Tools jeden Angriffs beobachten, damit der nächste Angriff einfacher zu erfassen ist.

REAKTION MIT DURCHGEHENDEM EINBLICK UND ÜBERLEGENER SICHERHEITSINTELLIGENZ

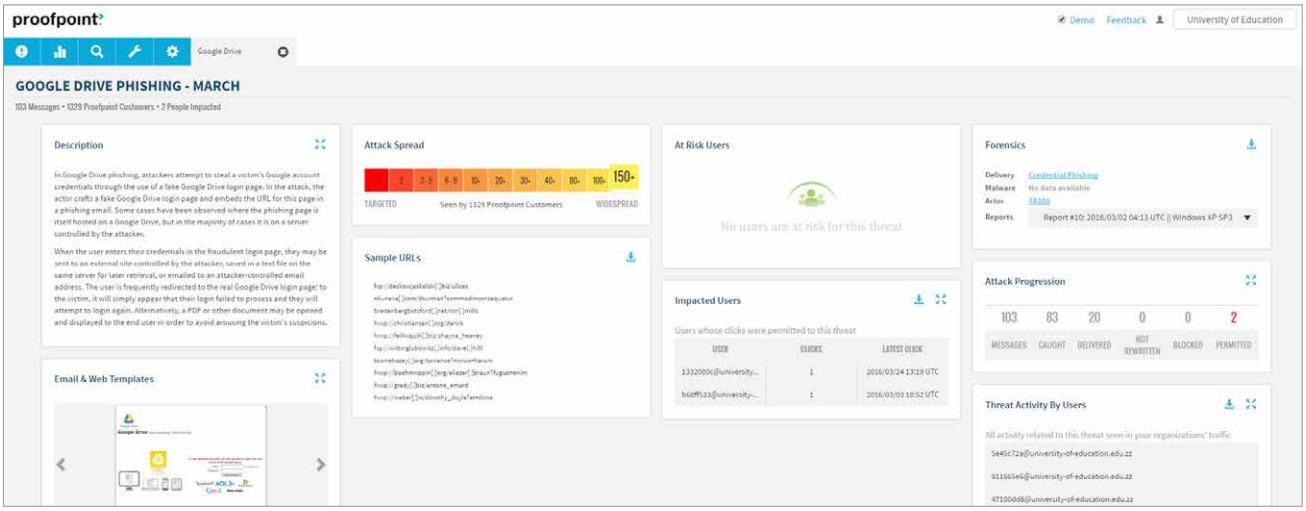
Proofpoint ist das einzige Cybersicherheits-Unternehmen mit einer Bedrohungsintelligenz, die sich über E-Mail, Netzwerke, mobile Apps und Social Media erstreckt. Unser Angriffsdiagramm Community-basierter Intelligenz umfasst über 600 Milliarden Datenpunkte, die mit Angriffskampagnen verschiedener Branchen und geografischer Gebiete verbunden sind. Da wir die Mehrheit des schädlichen Verkehrs Kampagnen zuschreiben können, können Sie einfach zwischen umfangreichen Angriffen und Bedrohungen unterscheiden, die auf die Geschäftsführung und andere hochrangige Mitarbeiter abzielen.

Wir beziehen zudem die Einblicke der Proofpoint Emerging Threats (ET) Intelligence ein, der zeitgerechtesten und genauesten Quelle für Bedrohungsintelligenz auf dem Markt. Proofpoint ET Intelligence ist der Goldstandard für Bedrohungsforscher mit 100 % geprüfter Bedrohungsintelligenz, die über Domänen und IP-Adressen hinausreicht.

Proofpoint TAP umfasst ein webbasiertes, grafisches Dashboard, das Daten auf Bedrohungs-, Organisations- und Benutzerebene anbietet, damit Sie Warnungen priorisieren und reagieren können. Detaillierte forensische Informationen über individuelle Bedrohungen sowie Kampagnen werden Ihnen in Echtzeit bereitgestellt.

Wir beantworten wichtige Fragen, wie beispielsweise:

- Worin besteht die Bedrohung? Gehört sie zu einer Angriffskampagne?
- Wer wird angegriffen?
- Wie viele Nachrichten wurden blockiert?
- Welche Benutzer haben darauf geklickt?
- Wie lässt sich feststellen, ob ein Endpunkt infiziert wurde?



SCHNELLE BEREITSTELLUNG UND UMFASSENDER SCHUTZ FÜR UNMITTELBAREN WERT

Um Ihr Personal, Ihre Daten und Marken zu schützen, müssen moderne Abwehrmaßnahmen dort eingesetzt werden, wo Ihr Personal arbeitet und zwar im gleichen Tempo. Die TAP-Architektur sorgt für schnelle Bereitstellung und unmittelbaren Wertzuwachs. Sie können Hunderttausende von Benutzern in wenigen Tagen schützen, nicht in Wochen oder Monaten.

Unsere Lösung schützt Benutzer in jedem Netzwerk oder an jedem Gerät, unabhängig wo und wie sie ihre E-Mail abrufen. Proofpoint TAP lässt sich einfach als Add-on-Modul für die Proofpoint E-Mail-Sicherheitsplattform konfigurieren, die als Cloud-Service, virtuelle App oder Hardware-Anwendung bereitgestellt werden kann. Proofpoint verwendet die Cloud auch für tägliche Sofort-Updates unserer Software, damit neue Funktionen schnell übernommen werden und Ihnen helfen, Angreifern immer einen Schritt voraus zu sein.

ÜBER PROOFPOINT

Proofpoint Inc. (NASDAQ: PFPT), ein Unternehmen für Internetsicherheitslösungen der nächsten Generation, ermöglicht Organisationen, das Arbeitsumfeld ihrer Mitarbeiter vor fortschrittlichen Bedrohungen und Compliance-Risiken zu schützen. Proofpoint hilft Internetsicherheitsprofis dabei, ihre Anwender vor den hochentwickelten Angriffen zu schützen, die in E-Mails, mobilen Apps und in den sozialen Netzwerken gegen sie gerichtet werden. Es schützt die wichtigen Daten, die Menschen erstellen, und stattet Teams mit den richtigen Informationstools aus, die ihnen bei Problemen eine schnelle Reaktion ermöglichen. Führende Unternehmen aller Größenordnungen, darunter mehr als 50 % 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.