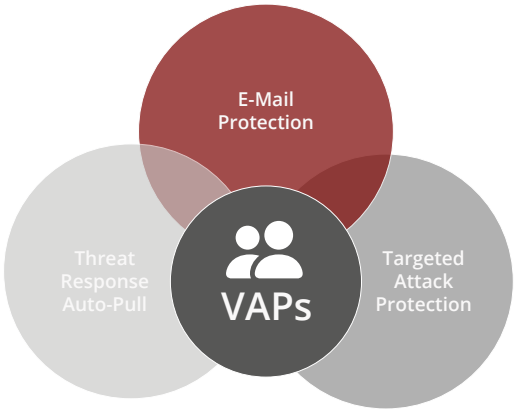
DTS

DTS
E-Mail Security

E-Mail Security

E-Mails sind als Kommunikationsmittel unverzichtbar. Im betrieblichen Umfeld sind sie ein elementarer Bestandteil der meisten Geschäftsprozesse. Auf Grund der Architektur ist das Medium E-Mail allerdings anfällig für Cyberangriffe aller Art und damit u. a. für Sabotage, Wirtschaftsspionage oder Datendiebstahl. Wenn man bedenkt, dass pro Tag mehr als 300 Milliarden E-Mails versendet werden, wird das Ausmaß der Gefahr deutlich. Nicht umsonst beginnen über 90 % aller Angriffe auf Unternehmen mit einer E-Mail. Das Ziel der Angreifer hat sich dabei verschoben. Natürlich sind Sicherheitslücken und fehlerhafte Konfigurationen der Infrastruktur beliebte Ziele. Im Mittelpunkt steht aber der Mensch bzw. Mitarbeitende, der „ausgenutzt" wird, um schadhafte Programme auszuführen, oder z. B. Überweisungen zu tätigen und Zugangsdaten einzugeben. Identitäten und Informationen geben dem Angreifer einen massiven Mehrwert für weitere gezielte Angriffe. Schnell wird klar, eine hohe Priorisierung der E-Mail-Sicherheit ist essenziell. Gemeinsam mit unserem langjährigen Partner Proofpoint ermöglichen wir Ihnen die weltweit führende Lösung zur Abwehr von zielgerichteten E-Mail-Angriffen.

- Vollständige Abwehr von gezielten E-Mail Angriffen & bösartigen Anhängen sowie Inhalten
- Identifizierung von bekannten & unbekannten Bedrohungen
- Höchste Viren- & Spam-Erkennungsrate
- Schutz vor Impostor/BEC-Angriffen
- Dynamische Reputationsanalyse
- Targeted Attack Protection als Schutz gegen neuartige Gefahren
- Automatisierte E-Mail-Quarantänisierung mittels Threat Response Auto-Pull
- DTS Managed Services



Drei grundsätzliche Bausteine ermöglichen einen ganzheitlichen E-Mail-Schutz für Ihr Unternehmen und Ihre Very Attacked People (VAP):

Proofpoint E-Mail Protection
Proofpoint E-Mail Protection hilft Ihnen ein- und ausgehende E-Mails mit einer benutzerfreundlichen Lösung zu sichern und zu kontrollieren. Sie können Ihre Mitarbeitenden, Daten sowie Ihr gesamtes Unternehmen vollständig vor den heutigen Bedrohungen absichern, egal ob Impostor E-Mails, Phishing, Malware, Spam oder Bulk-Mails. Die Dynamic Reputation, eine dynamische Reputationsanalyse, ist ein von Proofpoint entwickelter Dienst zur Prüfung der Absender-Reputation. Hier werden kontinuierlich globale IP-Adressen bewertet, um festzustellen, ob E-Mail-Verbindungen akzeptiert, abgelehnt oder reduziert werden sollten.

Basierend auf der patentierten Proofpoint MLX-Technologie für maschinelles Lernen untersucht und filtert die Lösung Millionen möglicher Spam-Attribute in jeder E-Mail, einschließlich der Kopfzeilen und der Struktur von E-Mails, enthaltenen Bildern, der Reputation des Absenders sowie unstrukturierter Inhalte im Nachrichtentext. Diese Spam Detection verhindert zuverlässig Spam-E-Mails und anhangsbasierten Spam, inkl. PDF- und Bild-Spam. Außerdem werden gleichzeitig neuartige Spam-Angriffe automatisch gefiltert, sobald sie auftreten. Der cloudbasierte Dynamic Update Service von Proofpoint hält die Spam Detection jederzeit auf dem aktuellen Stand und gewährleistet maximale Erkennung.

Impostor E-Mails, das sogenannte Business E-Mail Compromise, sind besonders beliebt. Die E-Mail Protection erkennt und klassifiziert auch solche zielgerichteten, betrügerischen E-Mails dank der Kombination von Authentifizierung (DMARC), vordefinierten Regeln und dynamischer Klassifizierung. Die Technologie bewertet aktiv die Reputation des Senders für umfassenden Schutz ohne zusätzlichen Administrationsaufwand.

Mit der Virus Protection ist zudem ein lokaler Anti-Virus Scanner enthalten, der auf dem Proofpoint-Gateway läuft und alle in den E-Mails bzw. Anhängen enthaltenen bekannten Bedrohungen herausfiltert. Der zusätzliche Zero-Hour Anti-Virus ist eine eigens von Proofpoint entwickelte Anti-Virus Engine, die unabhängig von Anti-Viren Signaturen arbeitet und somit einen zusätzlichen Schutz Ihres E-Mailverkehrs vor Phishing Attacken bietet.

Als Echtzeit-E-Mail-Inhaltsfilter ermöglicht Ihnen die E-Mail-Firewall Compliance-Richtlinien für Nachrichteninhalte und Anhänge zu definieren und durchzusetzen. Das statische Filterregelwerk können Sie auf Ihre Bedürfnisse abstimmen und auf diese Weise z. B. die zulässige Nachrichtengrößen oder Anhänge angeben.

Außerdem bietet die Smart Search Funktion eine erweiterte E-Mail-Nachrichtenverfolgung in Echtzeit mit forensischer und protokollierter Analyse, zwecks Troubleshooting. Die Protokollanalysen zur Nachrichtenverfolgung werden schnell über alle Proofpoint-Systeme hinweg konsolidiert und für eine schnelle Suche indexiert. Die Analyseinformationen werden zudem kontinuierlich aktualisiert, so dass innerhalb von Minuten detaillierte Analysen zu jeder E-Mail-Nachricht über die benutzerfreundliche Oberfläche verfolgt werden können.

Targeted Attack Protection (TAP)
Mit TAP sind Sie den Angriffen stets einen Schritt voraus. Der innovative Ansatz erkennt, analysiert und blockiert hochentwickelte Bedrohungen bevor sie Ihren Posteingang erreichen. Das beinhaltet nicht nur Ransomware und Gefahren, die über schädliche Anhänge und URLs übertragen werden, sondern Zero-Day-Bedrohungen, polymorphe Malware, manipulierte Dokumente sowie Phishing. TAP erkennt auch Risiken in Cloud-Anwendungen und korreliert E-Mail-Angriffe mit Anmeldedaten-Diebstahl oder anderen Attacken.

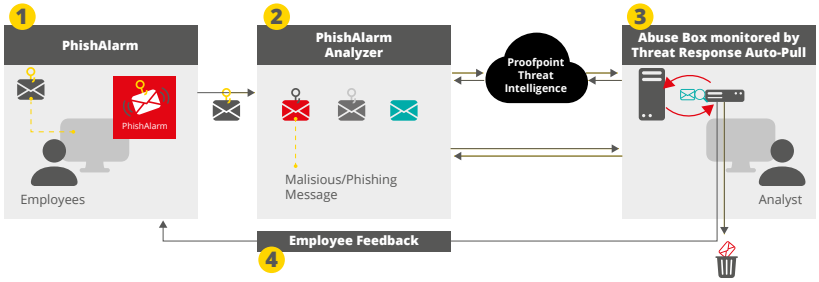
Die Attachment Defense von TAP dient hierbei der Erkennung und dem Schutz vor Malware, die in PDF-, Microsoft Office- und Flash-Dateianhängen enthalten ist. Während der Nachrichtenverarbeitung ermittelt der Proofpoint Protection Server, ob zu einer Nachricht Anhänge vorhanden sind, für die die Attachment-Defense-Analyse unterstützt wird. Ist dies der Fall, wird für jeden Anhang ein SHA256-Hash berechnet. Bei E-Mails mit unbekannten Anhängen leitet die TAP Attachment De-

fense dann eine Kopie der Anhänge sowohl an die TAP-Sandbox als auch an Palo Alto Networks WildFire Cloud zur Urteilsfindung weiter. Die eigentliche E-Mail wird solange zurückgehalten bis ein Urteil über den Anhang vorliegt. Wenn eine der Sandboxen eine Bedrohung feststellt, wird die E-Mail gemäß dem Regelwerk behandelt. Sämtliche Informationen, sowohl von TAP als auch von WildFire, werden über das TAP-Dashboard gesammelt und organisiert.

Die URL Defense von TAP dient zusätzlich dazu, Klicks auf böswilligen Webseiten zu verfolgen und anschließend zu blockieren, ohne die Benutzerfreundlichkeit oder andere URL-Filtertechnologien zu beeinträchtigen. Während der Nachrichtenverarbeitung werden URLs transparent umgeschrieben (URL-Rewriting) und an den cloudbasierten Dienst von Proofpoint weitergeleitet. Die identifizierten URLs werden auch an die cloudbasierte Sandbox für eine vorausschauende Analyse übermittelt, die verdächtige URLs auf der Grundlage von E-Mail-Verkehrsmustern präventiv identifiziert. Aufgrund des URL-Rewritings findet eine zusätzliche Prüfung des Links zu dem Zeitpunkt statt, wenn ein Benutzer auf den Link klickt (Click-Time Defense). Hierbei spielt es keine Rolle auf welchem Endgerät der Link angeklickt wird, da die URL permanent auf das Proofpoint Gateway umgeleitet wird und somit einen Schutz für weitergeleitete E-Mails bietet.

Threat Response Auto-Pull (TRAP)
Wenn eine schädliche E-Mail erkannt wird, senden die Erkennungssysteme eine Warnung an das Threat Response System mit Informationen über die Nachricht. Threat Response verschiebt dann die Nachricht in Quarantäne. Jedoch wird es selbst mit der effektivsten Lösung immer Nachrichten geben, die es bis in den Posteingang eines Benutzers schaffen. Die Auto-Pull Funktion sucht daher nach weitergeleiteten Kopien der Nachricht sowie nach Verteilungslisten der Empfänger und der Nachricht in anderen Posteingängen auf demselben Server und verschiebt diese ebenfalls in eine Quarantäne mit beschränktem Zugang. Somit können mittels Automatisierung die Mitarbeitenden des Sicherheitsteams und des Helpdesks entlastet werden.

Closed Loop E-Mail Analysis and Response (CLEAR)
Ein geschulter Mitarbeiter kann Ihre letzte Verteidigungslinie gegen einen Cyberangriff sein. Mit Proofpoint CLEAR wird der Zyklus aus Berichten, Analysen und Behebungen potenziell schädlicher E-Mails von Tagen auf Minuten verkürzt. Dank der Anreicherung mit unseren führenden Cyber Security Lösungen für Bedrohungsdaten sowie Security Awareness Trainings kann CLEAR aktive Angriffe mit einem einzigen Mausklick blockieren. Und durch die automatische Reaktion auf schädliche Nachrichten spart Ihr Team wertvolle Zeit und Arbeitsaufwand. Mittels des Plug-ins PhishAlarm, welches in der E-Mail-Anwendung Ihrer Mitarbeitenden installiert wird, haben diese die Möglichkeit verdächtige E-Mails direkt zu melden. Die gemeldeten E-Mails werden zur Kontrolle in ein speziell dafür eingerichtetes Postfach verschoben und dort von PhishAlarm Analyzer und der Proofpoint Threat Intelligence auf diverse Parameter überprüft. So findet eine Vorqualifizierung statt, die dem E-Mail Administrator eine Überprüfung auf Schädlichkeit vereinfacht. Eindeutig schädliche E-Mails können dann automatisiert über Threat Response Auto-Pull aus allen Postfächern entfernt werden.



DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de