DTS

DTS
E-Mail Security

E-Mail Security

Emails are indispensable as a means of communication. In the operational environment, they are a fundamental part of most business processes. Because of its architecture, however, the medium of email is vulnerable to cyber attacks of all kinds and thus to sabotage, industrial espionage and data theft, among other things. When you consider that more than 300 billion emails are sent every day, the scale of the threat becomes clear. It is hardly surprising that over 90% of all attacks on companies start with an email. The attackers' target has shifted over time. Of course, security vulnerabilities and faulty infrastructure configurations are popular targets. But the focus is now on people, employees who can be "exploited" to run malicious programs or, for example, to make bank transfers and enter access data. Identities and information give the attacker a massive advantage for further targeted attacks. It quickly becomes clear that email security is a high priority. Together with our long-term partner Proofpoint, we provide you with the world's leading solution for defending against targeted email attacks.

- Complete defense against targeted email attacks and malicious attachments and content
- Identification of known & unknown threats
- Highest virus & spam detection rate
- Protection against impostor/BEC attacks
- Dynamic reputation analysis
- Targeted attack protection as a safeguard against new types of threats
- Automated email quarantine using threat response auto-pull
- DTS managed services

Three basic building blocks enable comprehensive email protection for your organization and your very attacked people (VAPs):

Proofpoint Email Protection
Proofpoint Email Protection helps you secure and control inbound and outbound email with a user-friendly solution. You can fully protect your employees, your data and your entire organization from today's threats, including impostor emails, phishing, malware, spam and bulk emails. Dynamic reputation analysis is a sender reputation checking service developed by Proofpoint. Global IP addresses are continuously evaluated in this context to determine whether email connections should be accepted, rejected or reduced.

Based on Proofpoint's patented MLX machine learning technology, the solution examines and filters millions of possible spam attributes in each email, including email headers and structure, images, sender reputation and unstructured content in the message body. This spam detection reliably prevents spam emails and attachment-based spam, including PDF and image spam. At the same time, new types of spam attacks are automatically filtered out as soon as they occur. Proofpoint's cloud-based dynamic update service keeps spam detection up-to-date at all times, ensuring maximum detection.

Impostor emails, known as business email compromise, are particularly popular. The email protection also detects and classifies such targeted, fraudulent emails thanks to the combination of authentication (DMARC), predefined rules and dynamic classification. The technology actively assesses the sender's reputation for comprehensive protection with no additional administrative effort.

Also included with the virus protection is a local anti-virus scanner that runs on the Proofpoint gateway and filters out all known threats contained in emails and attachments. The additional Zero-Hour Anti-Virus is an anti-virus engine developed specifically by Proofpoint that works independently of anti-virus signatures to provide additional protection for your email traffic against phishing attacks.

As a real-time email content filter, the email firewall allows you to define and enforce compliance policies for message content and attachments. You can tailor the static filter rule set to your needs, specifying, for example, the message sizes or attachments allowed.

In addition, the smart search feature provides advanced real-time email message tracking with forensic logged analysis for troubleshooting purposes. Message tracking log analyses are quickly consolidated across all Proofpoint systems and indexed for fast searching. The analytical information is also continuously updated so that detailed analyses of any email message can be produced within minutes via the user-friendly interface.

Targeted Attack Protection (TAP)
With TAP you are always one step ahead of the attacks. The innovative approach detects, analyzes and blocks sophisticated threats before they reach your inbox. This includes not only ransomware and threats transmitted via malicious attachments and URLs, but zero-day threats, polymorphic malware, manipulated documents and phishing. TAP also detects risks in cloud applications and correlates email attacks with credential theft and other attacks.

TAP's Attachment Defense is designed to detect and protect against malware contained in PDF, Microsoft Office and Flash file attachments. During message processing, the Proofpoint Protection Server determines if there are attachments to a message for which attachment defense analysis is supported. If this is the case, a SHA256 hash is calculated for each attachment. For emails with unknown attachments, TAP Attachment Defense then forwards a copy of the attachments to both the TAP Sandbox and Palo Alto Networks WildFire Cloud for adjudication. The actual email is withheld until a verdict is reached on the attachment. If one of the sandboxes detects a threat, the email is handled according to the rules. All the information, from both TAP and WildFire, is collected and organized through the TAP dashboard.

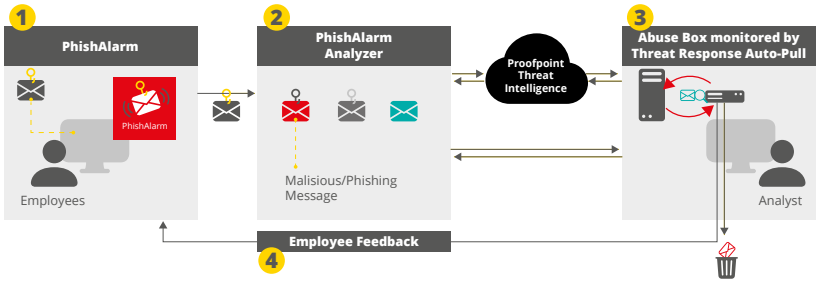
TAP URL Defense also serves to track and subsequently block clicks on malicious websites without compromising the user experience or other URL filtering technologies. During message processing, URLs are transparently rewritten (URL rewriting) and forwarded to Proofpoint's cloud-based service. The URLs identified are also submitted to the cloud-based sandbox for predictive analysis, which preemptively identifies suspicious URLs based on email traffic patterns. By means of URL rewriting, an additional check of the link takes place at the time when a user clicks on the link (click-time defense). It does not matter which device is used to click on the link, as the URL is permanently redirected to the Proofpoint gateway, providing protection for forwarded emails.

Threat Response Auto-Pull (TRAP)

When a malicious email is detected, the detection systems send an alert to the threat response system with information about the message. Threat Response then quarantines the message. Even with the most effective solution, however, there will always be messages that make it into a user's inbox. The auto-pull feature therefore looks for forwarded copies of the message, distribution lists of recipients and the message in other inboxes on the same server, and moves them to a restricted-access quarantine as well. This means that automation can be used to reduce the workload of the security team and the helpdesk.

Closed Loop Email Analysis and Response (CLEAR)

A trained employee can be your last line of defense against a cyber attack. Proofpoint CLEAR shortens the cycle of reporting, analysis and remediation of potentially malicious email from days to minutes. In combination with our leading cyber security threat intelligence solutions and security awareness training, CLEAR can block active attacks with a single click. And through automatic responses to malicious messages, your team saves valuable time and effort. With the PhishAlarm plug-in, which is installed in the email application of your employees, they are able to report suspicious emails directly. The reported emails are moved to a dedicated mailbox for inspection, where PhishAlarm Analyzer and Proofpoint Threat Intelligence check them for various parameters. In this way, a pre-qualification takes place, which makes it easier for the email administrator to check for threats. Clearly malicious emails can then be automatically removed from all mailboxes via Threat Response Auto-Pull.



DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de