Tarpitting und Greylisting

Beim "Tarpitting" und "Greylisting" handelt es sich - sachgerechte Anwendung vorausgesetzt - um ausgesprochen trickreiche und nützliche Funktionen. Sie halten in Kombination mit weiteren Spamschutzverfahren bis zu 98% der eingehenden, unerwünschten (Werbe-)Botschaften vom eigenen Postfach fern und senken die Systemlast des Mailservers zugleich deutlich.
Hier erfahren Sie, wie das funktioniert.

Trick 1: Eile mit Weile - Tarpitting
Da wäre zunächst das "Tarpitting". Abgeleitet von "Tarpit", zu deutsch "Teergrube", versteht man darunter eine bewusst herbeigeführte, leichte Verzögerung der Annahme einer E-Mail durch den Mailserver. Wird einem Mailserver mit eingeschaltetem Tarpitting eine E-Mail zur Zustellung in ein Benutzerpostfach angeboten, wartet der Server eine bestimmte Zeit ab, bevor er die Nachricht tatsächlich annimmt. Spamversender wollen jedoch binnen kurzer Zeit eine möglichst große Zahl von Nachrichten versenden und akzeptieren die durch den annehmenden Server auferlegte Wartezeit nicht. Sie geben auf - und Ihnen bleibt die meist nutzlose E-Mail erspart. Die Postausgangsserver seriöser Versender müssen weit weniger Versandvolumen bewältigen und haben es weniger eilig: Die Mail Ihrer Geschäftspartner erreicht Sie weiterhin ungehindert. Von der serverseitigen Verzögerung bemerken Sie im Normalfall nichts.

Trick 2: Einmal ist keinmal - Greylisting
Mit dem "Greylisting" beschreitet man ebenfalls einen präventiven Weg der Spamvermeidung, allerdings mit einer Vorgehensweise, die zunächst einigermaßen rigoros anmutet. Während eine "Whitelist" alle Adressen beinhaltet, von denen man in jedem Fall E-Mails erhalten möchte, führt eine "Blacklist" jene Adressen auf, von denen man keinesfalls Nachrichten empfangen will. Beim "Greylisting" wird nun jede eingehende E-Mail vom Eingangsserver zunächst pauschal als unzustellbar zurückgewiesen, ganz so, als stünde sie auf der Blacklist. Die meisten "Spam-Schleudern" geben sich damit meist ebenfalls aus zeitlichen Gründen geschlagen und verzichten auf die Zustellung ihrer Nachrichten. Nicht so die Postausgangsserver seriöser Versender: Sie unternehmen in der Regel mindestens noch einen weiteren Versuch. Der mit Greylisting ausgestattete Mailserver erinnert sich an den ersten Vorgang und akzeptiert die E-Mail beim zweiten Mal so, als stünde deren Absender auf einer internen Whitelist. Ergebnis: Die erwünschte Nachricht erreicht ihren Empfänger unverzüglich. Auch hier ist eine Verzögerung nicht spürbar.

Im Prinzip schlägt man die Massenversender von Spam-Nachrichten mit ihren eigenen Waffen: Da diese riesigen Mengen an E-Mail versenden müssen, kümmern sie sich kaum um Verzögerungen und Fehler bei jeder einzelnen Übermittlung. Fehlschläge sind einkalkuliert, was der professionellen Spamabwehr vielversprechende Ansatzpunkte eröffnet. Tarpitting und Greylisting haben weiterhin den großen Vorteil, dass sie einen Großteil der unerwünschten Nachrichten präventiv abblocken, schon bevor sie die weiteren aktiven Spamfilter erreichen. Ressourcenintensive Listenabgleiche oder statistische Verfahren zur Inhaltsanalyse müssen nur noch von einem sehr kleinen Anteil der E-Mails durchlaufen werden. Dadurch können größere Mailvolumina mit kleineren und preiswerteren Serverrechnern verarbeitet werden. Selbstverständlich sind die mp-Mailserver mit beiden Funktionen ausgestattet und bieten so über 98% Erkennungsrate für Spam-Nachrichten. Kompetente Fachberatung und Konfigurationsunterstützung inklusive!

From:
https://help.m-privacy.de/ -

Permanent link:
https://help.m-privacy.de/doku.php/tightgate-mailserver:tarpit_greylist

Last update: **2020/09/25 07:58**