Wie verwalte ich meinen eigenen internen Mail-Server ?

SEINEN EIGENEN MAIL-SERVER VERWALTEN

Ein permanenter DSL- oder Kabel-Anschluss erlaubt die Aufschaltung eines Mail-Servers ; er ist rund um die Uhr da, um eingehende Mails zu empfangen und ist jederzeit für einen Versand nach aussen bereit. Der Vorteil des permanenten Anschlusses hat aber auch seine Schattenseite, indem er besonders anfällig auf Attacken von aussen ist, und ein schlecht geschützter Mail-Server wird vorzugsweise zum Opfer von Spam.

Entscheiden Sie sich für Ihren eigenen Mail-Server, kann VTX als Ihr Secondary Mail-Server agieren.
Dazu muss bloss im DNS-Server (auf den der Domainname zeigt), die IP-Adresse Ihres Mail-Servers an erster Stelle (Primary MX) und die des VTX-Servers an zweiter Stelle (Secondary MX) eingetragen werden.

Zur Beachtung : Der VTX-Server kann nicht als ausgehender Mail-Server verwendet werden, und wir haben Anti-Spamming-Grundsätze auf unseren Servern aktiviert.

WAS IST SPAM ?

Spam ist im Internet vergleichbar mit unerwünschter Werbung in Ihrem Briefkasten. Während man an diesem einen kleinen entsprechenden Kleber anbringen kann, gibt es diese Möglichkeit für sein elektronisches Gegenstück nicht. Zudem muss keine reelle Person vorbeikommen, um den Briefkasten zu « beglücken », und die Gefahr des Überquellens ist gross, wie fast alle von uns es schon erlebt haben.

Im Internet wird Etikette strikt angewendet, und jede noch so gut gemeinte Werbebotschaft wird als Spam bezeichnet. Dabei handelt es sich um eine Vorsichtsmassnahme, die eine Überlasting des Netzwerkes durch Millionen Werbe-Mails verhindern soll.

WIE WIRD GESPAMMT ?

Die Beantwortung dieser Frage lässt einen besser erahnen, wie jede und jeder sich gegen solche Machenschaften schützen kann.

Eine Einzelperson oder eine Firma hat etwas zu verkaufen oder anzubieten. Dabei müssen vorerst geeignete Mail-Adressen gesammelt werden, indem z.B. Diskussions-Foren und Mailing-Listen « ausgesaugt » werden oder ein Verzeichnis von « Mailto » auf Web-Seiten erstellt wird ; meistens verfügen die Spammer nicht über genügend Kompetenz ; somit ist es am einfachsten, Adresslisten zu kaufen. Es besteht ein blühender Markt von Listen mit Millionen Adressen.

Die nächste Etappe ist der Versand der Botschaft. Das Verschicken von Tausenden von Mails ist ein kostenträchtiges Unterfangen ; es werden eine umfangreiche Ausrüstung, aber auch grosse Bandbreiten vorausgesetzt. Warum sich also nicht bei Andern bedienen, die ihr Gerät offen lassen ? Die Idee ist so einfach und genial, dass sie immer mehr angewandt wird. Um ein solches Gerät ausfindig zu machen, genügt es, die Adressen der Mail-Server zu durchforsten und zu versuchen, eine Mail an das Verzeichnis dieser Geräte zu versenden. Das erste Gerät, das «mitmacht», wird umgehend durch ein Mail getäuscht, mit dem man den Versand einiger Tausend Exemplare verlangt. Diese Operationen werden vorwiegend nachts durchgeführt, wenn der Server nicht überwacht ist (es wäre ja schade, davon nur ein paar wenige Minuten profitieren zu können ...).

Die « glücklichen » Empfänger dieser Botschaft können deren wirkliche Quelle nicht ausmachen, sehen jedoch sehr gut, von welchem (nicht geschützten) Server die Mail zu ihnen geleitet wurde. Der fragliche Server wird als unsicher eingestuft, und damit beginnt ein informelles Prozedere der « Verbannung » aus der Internet-Gemeinschaft.

Gewinner sind nur die Versender der Millionen Mails, denn Hunderte von Personen werden bei jedem verlockenden Angebot anbeissen.

AUF DER ANDERN SEITE : LAUTER VERLIERER

Seitens der « Opfer », die solche Mails erhalten, geht Zeit verloren, und dieser Ärger kann schnell in ein Gefühl von Belästigung umschlagen.

Seitens des Servers sind die Konsequenzen sofort viel schlimmer : ein gespammter Server, der ungeschützt bleibt, wird immer und immer wieder missbraucht. Damit kommt man in einen Teufelskreis : die zugeteilte Bandbreite reicht nicht mehr aus, die Ausrüstung muss erweitert werden, von den Datenverkehrs-Kosten gar nicht zu sprechen. Zudem muss sich jemand a posteriori mit diesen Problemen befassen und die Beschwerden von Betroffenen beantworten. Dann müssen Schritte zur Boykott-Aufhebung (« Black List ») unternommen werden. Ein steiniger Weg, den man durch eine sogar einfache Vorbeugung gar nicht erst gehen müsste.

Wie schütze ich mich gegen Spamming ?

WIE SCHÜTZE ICH MEINEN ACCOUNT ?

Es gibt kein Wundermittel ; das einfachste ist, seine E-Mail-Adresse nicht in alle Winde zu verstreuen. Wenn Sie Spam mit dem Vermerk « Dies ist kein Spam – Sie können sich einfach durch Retournierung eines "Unsubscribe"-Mails an die Adresse gogo@money.com abmelden » erhalten und so antworten, ist dies der beste Beweis für die Gültigkeit Ihrer Adresse. Beacbten Sie, dass in der Mehrzahl der Fälle die wirkliche Absender-Adresse natürlich unbekannt bleibt.

WIE SCHÜTZE ICH MEINEN SERVER ?

Man muss sich erst einmal vergegenwärtigen, dass potentiell jede Site zur Spam-Quelle werden kann. Eine Regel will, dass die Adresse Postmaster@site.xxx obligatorisch ist für jede Site mit Maildienst. In stillschweigender Übereinkunft wird vermehrt die Adresse abuse@site.xxx erstellt, die für die Unterbreitung von Beschwerden verwendet wird. Allein die Tatsache, diese Adresse anzuerkennen und zu akzeptieren, legt schon ein Zeugnis guten Willens ab : Ihre Korrespondenten wissen, dass Sie sich der Problematik bewusst sind.

Die wichtigste Vorsichtsmassnahme ist, eine Message Relay (Mail-Relais) zu verhindern. Denn die Grundeinstellung der meisten Server lässt sie Mitteilungen ungeachtet der Herkunft weiterleiten. So können Spammer diese Leichtgläubigkeit ausnützen, um Ihre Ressourcen «anzuzapfen» und ihre Millionen von Mails zu verschicken.

Das Prinzip ist denkbar einfach : eine Botschaft von ausserhalb des Server-Lokalnetzes darf an keine auswärtige Adresse geliefert werden.

Ein anderes Prinzip kann angewendet werden : nur ein ausgewiesener Benutzer darf eine Mitteilung versenden.

Hiernach finden Sie einige Links zu Sites, die Ihnen beim Schutz Ihres Systems behilflich sein können.

WO BLEIBT DA DIE POLIZEI ?

Es gibt just einige relativ seriöse und « schrecklich » wirksame Organisationen, wie z.B. http://maps.vix.com.
Dabei handelt es sich um gemeinnützige Organisationen, deren einziges Ziel es ist, die durch das Spamming angerichteten Schäden wiedergutzumachen. Sie verfügen dabei über einen ganzen Rattenschwanz von Tests, um festzustellen, ob eine Site als Message Relay offen ist. Mangels direkter Druckmittel erstellen sie ein Verzeichnis von schlecht konfigurierten oder absichtlich im Spam-Bereich tätigen Sites. Solche «Black-lists » kommen somit in freien Umlauf, und es ist jedem freigestellt, darauf zu vertrauen und seinen Server so zu programmieren, dass er Mails von solchen « angeschwärzten » Sites ganz einfach zurückweist, im Bestreben, seine eigenen Benutzer zu schützen.

Es ist gut, zu wissen, dass diese Sites sich nicht nur als « Richter » verstehen, sondern auch eine umfassende Dokumentations-Quelle mit Wissenswertem zum Schutz jeden Server-Typs darstellen, und wir ermuntern Sie, solche Sites aufzusuchen.

EIN BISSCHEN VOKABULAR

Der Ausdruck « Spam » kommt aus einem Sketch der « Monty Python », worin eine Gruppe Wikinger immer lauter ein Loblied auf « Spam » singt, das eine CornedBeef-Marke verkörpert (http://www.spam.com/).

Für Liebhaber von Kürzeln haben wir hier eine kleine Klassifizierung der unerwünschten Mails in mehrere Kategorien :

UBE (Unsollicited Bulk E-mail) : Massenversand von unerwünschten E-Mails, also Spam ; UBE ist dabei ein generisches Kürzel, unabhängig vom Inhalt (Verkauf, Werbung, Kette, Propaganda, usw.) ;

UCE (Unsollicited Commercial E-mail) : reine Verkaufs-Mails ; nicht jedes UCE-Mail wird zwingend an mehrere Empfänger adressiert, somit ist jedes UCE nicht unbedingt mit Spam gleichzusetzen ;

MMF (Make Money Fast) : les chaînes (interdites en France et aux USA entre autres pays), les recettes miraclespour devenir riche rapidement et sans effort, etc.

MLM (Multi-Level Marketing) : Hier geht es um eine Variante der vorgängig erwähnten Kategorie, also alle Pyramiden-Schemen (analog zu Ketten-Versand).

NÜTZLICHE LINKS

http://de.wikipedia.org/wiki/Spam	DIE Referenz
http://www.cauce.org	Coalition Against Unsollicited Commercial E-mail (englisch)
http://spam.abuse.net/	(englisch)