

Verschiedene öffentliche Datenbanken legen die Vermutung nahe, dass die IP Adresse [Nummer(n) aus der englischsprachigen email hier einfügen] ein offener Relay Mail Server (Mail-Weiterleitungsserver) oder ein offener Proxyserver sein könnte. Wir gehen davon aus, dass Sie einen Server haben, der eine solche IP Adresse benützt. Die vorliegende E-Mail enthält wichtige Hinweise, die Ihrer Online-Präsenz auf dem Internet dienen können.

Die vorliegende E-Mail wird im Rahmen der „Aktion zum Schutz Ihres Server“ verschickt. Hierbei handelt es sich um ein gemeinsames Projekt der amerikanischen Federal Trade Commission und anderer staatlicher Behörden rund um den Erdball, die sich mit dem Problem von unerwünscht zugeschickten E-Mails (spam) befassen. Wir bemühen uns, Ihnen zu zeigen, wie Sie Ihren Server schützen können, damit er nicht ein unwissentlicher Lieferant von Spam wird. Als erste Massnahme empfehlen wir, Ihren offenen Relay-Mail- oder Proxyserver zu schliessen.

Offene Relays und offene Proxies sind Server, die irgendeinem Computer auf der Welt erlauben, durch sie E-Mails zu anderen Internet-Mail-Adressaten zu leiten. Offene Relay- und Proxyserver werden oft von Personen missbraucht, welche das Internet mit Spam überschwemmen. Diese Missbräuche schaffen weltweit Probleme für Konsumenten, für die rechtsanwendenden Behörden und auch für Ihre Organisation. Beispielhaft sei auf folgende Szenarien verwiesen:

- Die Empfänger glauben, die Spam kämen von Ihrem System;
- Unbekannte Dritte können Ihren Server oder Ihre Internetdienstressourcen verwenden;
- Ihre Netzwerkverbindungen könnten wegen der Datenmenge verstopft werden;
- Ihre administrativen Kosten könnten steigen;
- oder Ihr Internet-Provider sieht sich veranlasst, Ihren Internetdienst zu schliessen.

Sicherungsmassnahmen für Ihren Server können helfen, Ihr System vor Missbräuchen zu schützen.

Wir bieten Ihnen zusätzliche Informationen über offene Relay- und Proxyserver und wie Sie Ihre Organisation vor Gefahren im Zusammenhang mit ungeschützten Server schützen können, einschliesslich Schritt-für-Schritt-Instruktionen. Am besten klicken Sie sich auf www.ftc.gov/secureyourserver ein. Hier finden Sie die entsprechenden Hinweise mit einer Liste von Behörden, die sich an diesem Projekt beteiligen. Für direkten Zugang zu den Instruktionen betreffend Schliessung Ihres offenen Relay- oder Proxyserver klicken Sie auf www.ftc.gov/bcp/online/pubs/buspubs/secureyourserver.htm.

Wenn Sie Fragen zu den Instruktionen oder zum vorliegenden Schreiben haben, wenden Sie sich bitte an secureyourserver@ftc.gov.