Spam Check Service

URL

https://www.php-resource.de/script/PHP-Scripte/Webmastertools/Spam-Check-Service_17708

Produktbild

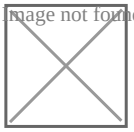

Image not found or type unknown

Beschreibung

- Willkommen

Dieser Service ist für jede Website gemacht. Hier ist es Ihnen möglich Ihren Server auf DNSBL einträge zu testen. Es geht ganz einfach links Ihre Domain eintragen und auf Check DNSBL klicken.

Sie bekommen direkt nach eintrag Ihr Sicherheitszertifikat per Mail zugesandt.Sie können Ihre Statistik nach 7 ,14 ,28,31 Tagen neu erstellen lassen.Desweiteren senden wir Ihnen auf wunsch die ergebnisse Automatisch via E-Mail zu.

Ab sofort ! Nun auch mit Besucherzähler (inkl. Passwortschutz) + Statistik + Herkunftsland der Besucher (auf der Statistik Seite) in deinem Zertifikat : DEMO

Was ist DNSBL In den den meisten RBLs werden IP-Adressen von Rechnern gelistet, von denen in der Vergangenheit Spam versendet wurde . einige Listen enthalten auch Quellen von Computerviren und anderer Malware. Heute handelt es sich bei diesen Rechnern meist um trojanisierte PCs oder seltener offene Mail-Relays, die von Spammern missbraucht wurden. Diese Listen können Mailserver oder Spam-Erkennungssoftware (z. B. Spamassassin) beim Eingang einer Mail nahezu in Echtzeit über das DNS-Protokoll auswerten und bei positivem Ergebnis die Annahme der Mail verweigern, die Annahme der Mail verzögern (Teergrube, Greylisting) oder die Mail so markieren, dass sie ohne großen Aufwand vom Empfänger gefiltert werden kann. Eine Liste mehrerer vertrauenswürdiger RBLs in Verbindung mit Greylisting hat sich als sehr effizient erwiesen (Stand Ende 2007). Die Abfrage einer DNSBL ist, wie der Name bereits vermuten lässt, aus technischer Sicht eine DNS-Abfrage. So ist meist keine zusätzliche Freigabe in der Firewall erforderlich.

VOR UND NACHTEILE DNSBL Der Vorteil von RBLs liegt vor allem darin, dass die Abfrage schnell ist und sich technisch einfach realisieren lässt. Bei geeignetem Einsatz ist die Verwendung sehr effizient und erzeugt selten Falsch-Positive Ergebnisse. Den größten Nachteil von RBLs zeigt am besten ein Beispiel: Verschickt ein Kunde Spam über den Mailserver seines Providers und die IP-Adresse des Mailservers wird deshalb gelistet, können Mails anderer Kunden, die denselben Mailserver verwenden, als Spam klassifiziert werden. Vergleichbare Probleme hat praktisch jeder Versender von Massen-Mails, selbst bei Confirmed Opt-In. Werden E-Mails aufgrund von RBL-Eintragen abgewiesen und werden mehrere RBLs in Folge verwendet, hat dies den Nachteil, dass sich der Anteil der Falsch-Positiven addiert. Aus diesem Grund sollten nur wenige, gut ausgewählte RBLs zum Abweisen von E-Mails verwendet werden. Um diese Problematik zu entschärfen, können die Ergebnisse der RBL-Abfragen zusammen mit weiteren Kriterien gewichtet werden. Das Ergebnis wird dann zur Spam-Klassifikation und ggf. zum Abweisen der Mail benutzt (so eingesetzt z.B. bei SpamAssassin). Bei einigen RBLs ist es schwer, teuer oder sogar unmöglich, eine IP-Adresse wieder entfernen zu lassen (delisting). In solchen Fällen schadet die RBL weniger den Spammern, als vielmehr den Besitzern von missbrauchten Rechnern. Der Administrator eines Mailservers muss

Details zur Anzeige