

Postfix, AMaViS und Co

- Christian Rößner
- Aufbau und Konzeption eines Mailserver-Setups unter den Gesichtspunkten starker Spam-Belastung und maximaler Sicherheit

Inhalt

- Was ist Spam, Ham, UCE und UBE?
- Verbreitungswege von Spam
- Das SMTP-Protokoll (vereinfacht dargestellt)
- Beispiel Mail-Header
- LDAP und MySQL

Sender-, Recipient Adressen

- Regeln für Email-Adressen:
 - Domain muss voll qualifiziert sein (FQDN)
 - Die Domain muss existieren (DNS)
- Unerlaubte Beispiele:
 - <foobar> - Kein Domain-Teil
 - <test@foobar> - Nicht FQDN
 - <test@foobar.fake> - Unbekannte Domain

Vorbetrachtung

- Mailservername
 - A und PTR müssen im DNS übereinstimmen
 - Muss im EHLO verwendet werden
- Relaying nur über SMTP-AUTH
- Mailserver darf nicht über dynamische Internetverbindung angeschlossen sein.

Postfix

- Postfix – ein reiner MTA
 - modularer Aufbau
 - Herzstück: `smtpd_recipient_restrictions`
 - Policy-Service Delegation
 - selektives Greylisting
 - Dynamic IP Maps

AMaViS

- AMaViS im Detail
 - Pre-Queue-Filter in Postfix
 - Policy-Banks
 - Spamassassin (SA)
 - Virens Scanner
 - Penpals

DNS und Spamtrap

- Eigener DNS
(auch für Realtime Blackhole Lists)
 - DNSBL – DNS Blacklists
 - RHSBL – Righthand-side Blacklists
- Spamtrap
 - Wie stellt man Spammern eine Falle?
Stichwort smtp-sink

Fehlentwicklungen

- SPF – Sender Policy Framework
- Microsoft Caller-ID/Sender-ID
- DKIM / Yahoo DomainKeys
 - evtl . Einsatz für Spam-Score in SA
- Veraltet: Teergruben / Tarpeting

Tools und Sonstiges

- Hilfswerkzeuge
 - swaks - Swiss Army Knife SMTP
 - sa-updater-wrap aktualisiert Score-Regeln
 - logwatch für Postfix und AMaViS
 - Monit überwacht essentielle Dienste
- Webmail – z.B. Squirrelmail
- Daten-Backup mit LVM-Snapshots

Literatur

- Postfix – Einrichtung, Betrieb und Wartung
ISBN 3-89864-350-6
dpunkt.verlag GmbH
von Ralf Hildebrandt, Patrick Ben Koetter
- Das Postfix-Buch – Sichere Mailserver
mit Linux
ISBN 978-3-937514-50-5
opensource press
von Peer Heinlein

Literatur

- OpenLDAP
ISBN 3-89842-762-5
Galileo computing
von Oliver Liebel, John Martin Ungar
- Mailingliste:
<postfix-users@listen.jpberlin.de>
- <http://www.postfix.org/>
- <http://www.ijs.si/software/amavisd/>