SMTP – Simple Mail Transfer Protocol

SMTP dient zum Austausch elektronischer Nachrichten im Internet. Es wird dabei vorrangig zum Versenden von E-Mails verwendet. Zum Abholen von Nachrichten kommen andere, spezialisierte Protokolle wie POP3 oder IMAP zum Einsatz. Der Standardport von SMTP ist der TCP Port 25, neuere Server benutzen auch zusätzlich den TCP Port 587, um für authentifizierte Benutzer Mails entgegenzunehmen.

SMTP ist ein textbasiertes Protokoll, der derzeit gültige RFC (Request for Comments) ist in RFC 2821 definiert.

Begriffe

MTA - Mail Transfer Agent: Transport zwischen MTAs (sendmail, postfix, exim, qmail, etc)
MUA - Mail User Agent: (Outlook, MS-Mail, Thunderbird, etc)
MDA - Mail Delivery Agent: Speicherung der Nachrichten in den Benutzerpostfächer am Mailserver (Procmail, Cyrus, Courier, Maildrop)
MRA - Mail Retrival Agent: Herunterladen der gespeicherten Nachrichten via POP

Einer der ersten MTAs, der SMTP implementiert hatte und weite Verbreitung erlangte, war sendmail (www.sendmail.org). Inzwischen gibt es über 100 Programme, die SMTP als Client oder Server unterstützen, darunter weit verbreitete SMTP-Server wie postfix, exim, qmail, usw.

SMTP begann als reines ASCII-Protokoll, so dass damit keine Binärdateien übertragen werden konnten. Erst Standards wie MIME (Multipurpose Internet Mail Extensions) schafften diese Möglichkeit durch ein Kodieren der Binärdateien in ASCII.

Erweiterungen des Protokolls waren Extended SMTP (ESMTP) 1995. Diese Erweiterung erlaubt, dass über ein modulares Konzept weitere Befehle (*SMTP-Verben*) definiert werden. Wenn der Sender sich beim Server nicht wie oben gezeigt mit `HELO`, sondern mit `EHLO` (*Extended HELO*) meldet, teilt der Server ihm im Gegenzug mit, welche Erweiterungen des Protokolls er unterstützt. Gängige Beispiele hierfür sind STARTTLS (Verschlüsselung – Transport Layer Security), 8BITMIME, DSN (Delivery Status Notifications) und AUTH (SMTP-Authentifizierung).

Während SMTP für die weltweite Zustellung zwischen beliebigen MTAs entwickelt wurde, ist LMTP für die Auslieferung der Mails innerhalb einer lokalen Organisation, d.h. für den Transport zwischen verschiedenen lokalen Serverkomponenten (MX-Server – Mailstore) wie etwa MTA und MDA gedacht.

SMTP ein robustes und zuverlässiges Protokoll, E-Mails gehen praktisch nicht verloren, bei Fehlern in der Zustellung wird der Absender informiert.

Eine typische SMTP-Sitzung zum Versenden einer E-Mail sieht folgendermaßen aus:

Client	Server	Erklärung
	`220 mail.example.com SMTP Foo Mailserver`	Server begrüßt den Client
`HELO client.example.org`		Client meldet sich an
	`250 Hello client.example.org, nice to meet you`	Server bestätigt Anmeldung. Wichtig ist, dass der Client jeweils auf die Antwort vom Server wartet.
`MAIL FROM:<bar@example.org>`		Absenderadresse
	`250 Sender OK`	
`RCPT TO:<foo@example.com>`		
	`250 Recipient OK`	
`DATA`		Client möchte jetzt die Mail mitteilen
	`354 End data with <CR><LF>.<CR><LF>`	

`From: <bar@example.org>`
`To: <foo@example.com>`
`Subject: Testmail`
`Date: Thu, 26 Oct 2006 13:10:50 +0200`
 	
`Testmail`
`.`
		Client schickt komplette Mail
		Die Mail muss mit einer Zeile,
		die nur einen Punkt enthält, abgeschlossen werden

	`250 Message accepted for delivery`	
`QUIT`		Client meldet sich ab
	`221 See you later`	

Das SMTP-Protokoll sieht zum Status der Kommunikation zwischen Mailserver und Mailclient folgende Fehlercodes vor:

- **1XX:** Mailserver hat die Anforderung akzeptiert, ist aber selbst noch nicht tätig geworden. Eine Bestätigungsmeldung ist erforderlich.
- **2XX:** Mailserver hat die Anforderung erfolgreich ohne Fehler ausgeführt.
- **3XX:** Mailserver hat die Anforderung verstanden, benötigt aber zur Verarbeitung weitere Informationen.
- **4XX:** Mailserver hat einen temporären Fehler festgestellt. Wenn die Anforderung ohne jegliche Änderung wiederholt wird, kann die Verarbeitung möglicherweise abgeschlossen werden.
- **5XX:** Mailserver hat einen fatalen Fehler festgestellt. Ihre Anforderung kann nicht verarbeitet werden.

MailHeader

```
Return-Path: <maluala_1970@Lagotronics.nl>
Received: from mx4.srv.eunet.at (mx4.srv.eunet.at [193.154.160.127])
        by imap04.si.eunet.at (Cyrus v2.2.12-Invoca-RPM-2.2.12-3.RHEL4.1) with LMTPA;
        Thu, 22 May 2008 07:05:39 +0200
X-Sieve: CMU Sieve 2.2
Received: from host151-128-static.22-87-b.business.telecomitalia.it (host151-128-static.22-87-
b.business.telecomitalia.it [87.22.128.151])
       by mx4.srv.eunet.at (8.14.1/8.14.1) with ESMTP id m4M55ZVd032413
       for <szojak@adis.at>; Thu, 22 May 2008 07:05:38 +0200
User-Agent: Microsoft-Entourage/12.1.0.080305
Date: Thu, 22 May 2008 07:05:38 +0200
Subject: Fantastic results guaranteed
From: Cutrara <maluala_1970@Lagotronics.nl>
To: "szojak@adis.at" <szojak@adis.at>
Message-ID: <117B10AE.1%maluala_1970@Lagotronics.nl>
Thread-Topic: Fantastic results guaranteed
Thread-Index: Aci72j16buBHOk3/Tui+0WeQlR455g==
Mime-version: 1.0
Content-type: multipart/alternative;
        boundary="B_2389618662_34279"
X-Spam-Checker-Version: MIMEDefang/SpamAssassin2.58
X-Spam-Flag: YES ; 5.719
X-Spam-Level: *****
X-Scanned-By: MIMEDefang 2.62 on 193.154.160.170
```

Die Nachricht mit der Message-ID “m4M55ZVd032413” wurde vom Host „87.22.128.151“ am 22. May 2008 um 07:05:38 abgeschickt, der für die Maildomain „adis.at“ zuständige Mailserver mx4.srv.eunet.at hat diese um 07:05:39 erhalten und diese per LMTP auf dem CyrusNode “imap04.si.eunet.at“ dem User in seine Mailbox gestellt. Die Nachricht wurde von der SpamSoftware als SPAM eingestuft.

Einträge im E-Mail-Header werden durch einen Zeilenumbruch (CRLF) voneinander getrennt. Der E-Mail-Header wird durch eine Leerzeile (CRLF CRLF) vom E-Mail-Body getrennt.

Date: Absendedatum und Uhrzeit. Der Zeitpunkt des Absendens der E-Mail.

From: Absender
Eine oder mehrere durch Kommas getrennte E-Mail-Adressen, die den oder die Absender einer E-Mail bezeichnen. Die meisten E-Mail-Clients unterstützen nur einen einzelnen Absender.

Sender: Technischer Absender
Ist der technische Absender ein anderer, als im From-Header bezeichnet, kann dieser im Sender-Header vermerkt werden. Das Sender-Feld darf nur eine einzelne E-Mail-Adresse enthalten. Beispiel: Die E-Mail-Adresse eines Sekretärs, der eine E-Mail nach Diktat des Chefs verschickt gehört ins Sender-Feld. Die E-Mail-Adresse des Chefs gehört ins From-Feld.

Reply-To: Antwortadresse
Eine oder mehrere durch Kommas getrennte E-Mail-Adressen, an die eine Antwort auf die E-Mail geschickt werden soll (falls unterschiedlich zum From-Feld).

To: Der Empfänger
Eine oder mehrere durch Kommas getrennte E-Mail-Adressen, an die die E-Mail primär gesendet wird.

CC: Carbon Copy, der (Kohlepapier-) Durchschlag
Eine oder mehrere durch Kommas getrennte E-Mail-Adressen, an die eine Kopie der E-Mail gesendet wird. Die Einträge im CC-Feld werden (im Gegensatz zum BCC-Feld) bei allen Empfängern angezeigt und sind somit bekannt.

BCC: Blind Carbon Copy, die Blindkopie (BK)
Das BCC-Feld enthält eine oder mehrere durch Kommas getrennte E-Mail-Adressen, an die eine Kopie der E-Mail gesendet wird, ohne dass dies jedoch für die anderen angegebenen Empfänger sichtbar ist („Blindkopie“). Das BCC-Feld wird nicht an die Empfänger übertragen, so ist für keinen der Empfänger erkennbar, an wen eine Kopie per BCC verschickt wurde.

Subject: Der Betreff
Es ist für den Empfänger eine wichtige Kurzinformation über den Inhalt der Mail und sollte daher nicht fehlen. In Anbetracht der steigenden Anzahl unerwünschter E-Mails wächst die Bedeutung des Betreff-Felds, denn oft lassen sich unerwünschte Nachrichten bereits am Betreff erkennen.

Weitere Header-Zeilen
Viele weitere Informationen werden, sowohl vom Mailprogramm des Absenders, als auch von den am Versand der Mail beteiligten Mailservern in den Mail-Header eingefügt. So lässt sich zum Beispiel in der Regel an den Received-Zeilen die Reihenfolge und Adresse aller am Versand beteiligten Mailserver ablesen. Weiterhin erscheinen Informationen über eine erfolgte Viren-Prüfung oder Spam-Filterung in den Header-Zeilen der E-Mail. Diese Felder beginnen mit „X-„ (X-Spam-Flag, X-Abuse, etc).

SPAM

UBE - Unsolicited Bulk E-Mail:
Es handelt sich dabei um E-Mails, die unangefordert an eine große Anzahl von Empfängern verschickt werden. Häufig handelt es sich dabei um E-Mail-Marketing-Aktionen – missionierende oder volksverhetzende E-Mails und Kettenbriefe.

UCE – Unsolicited Commercial E-Mail:
E-Mails mit kommerziellen Inhalten, die unangefordert an Empfänger (auch einzelne oder wenige) verschickt werden. Typische Beispiele für UCE sind dubiose oder besonders günstig erscheinende Angebote für Sex, Viagra, illegale Online-Glücksspiel-Casinos, gefälschte Uhren, Lebensverlängerung, Software, Markenprodukte, Finanzdienstleistungen oder Medikamente.

Kollateraler Spam:

E-Mails mit gefälschter Absender-Adresse (der Adresse des unbeteiligten Dritten) werden verschickt, das empfangende E-Mail-System nimmt diese E-Mail zunächst an und schickt daraufhin eine Unzustellbarkeitsnachricht, eine *Abwesenheitsnachricht* oder ähnliches an den vermeintlichen Absender.

AntiSpamstrategien

RBL-Listen

In den meisten Realtime Blackhole Lists werden die IP-Adressen von Rechnern gelistet, von denen in der Vergangenheit Spam versendet wurde. Die Abfrage wird per DNS durchgeführt ist einfach zu implementieren. 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 daher sorgfältig abwägen, welche RBLs er verwendet, um „falsche positive“ Ergebnisse zu vermeiden. Einige RBLs wie z.B. Spamcop können die Listeneinträge jedoch nach einer gewissen Zeit automatisch entfernen. Spamcop entfernt die Einträge nach kurzer Zeit, sobald keine Beschwerden mehr über den betroffenen Mailserver eingehen.

RCF-Checks (Greeting Pause, HELO)

Laut dem RFC muss der Absender auf die entsprechende Rückmeldung vom Mailserver warten. Viele Würmer und Viren haben diese Mechanismen jedoch nicht eingebaut und funktionieren nach dem „fire and forget – Prinzip“ und werden so in der ersten Phase des Verbindungsaufbaus schon vor dem Versenden der Nachricht gesperrt. Weiters kann überprüft werden, ob der HELO-String ein plausibler Hostname ist oder nicht. Der rurückgegebene Fehlercode ist immer 5xx.

Access Rates, Access Limits

Die Idee ist es die Resourcen des SMTP-Servers gerecht zu verteilen. IP-Adressen aus Übersee können beispielsweise weniger Ressourcen zur Verfügung bekommen als nationale. Hat ein SMTP-Server seine Ressourcen – wie Anzahl neuer Verbindungen pro Zeiteinheit schon verbraucht, so werden auch keine neuen Verbindungen mehr angenommen.

GreyListing

Wir ein SMTP-Server kontaktiert, damit dieser eine E-Mail in Empfang nimmt, so sind diesem Mailserver folgende drei Daten bekannt, bevor der Mail-Server die E-Mail annehmen muss:

1. IP-Adresse des absendenden Mailservers
2. E-Mail-Adresse des E-Mail-Senders
3. E-Mail-Adresse des E-Mail-Empfängers

Wurde eine E-Mail mit dieser Kombination von Adressen noch nie empfangen, dann wird der Zustellversuch durch den SMTP-Server abgeblockt mit einer Meldung, dass ein temporärer Fehler aufgetreten sei (4xx Return Code), der SMTP-Client die Zustellung also später noch einmal versuchen soll. Wird ein nächstes Mal versucht eine E-Mail mit der selben Kombination von Daten zuzustellen (was ein regulärer und RFC-konform konfigurierter SMTP-Server auf jeden Fall tun sollte), so wird diese E-Mail (nach einem konfigurierbaren Zeitintervall) akzeptiert.

Aktuelle Implementierung verwenden auch RBL-Listen fuer das GreyListing. So fallen beispielsweise alle IP-Adressen aus Dialin-Netzen automatisch in das Greylisting. Im Falle von false positives kommen Nachrichten somit verzögert an.

SPF-Sender Policy Framework

SPF legt in einem DNS-Eintrag fest, von welchen IP-Adressen oder Hosts eine Nachricht angenommen werden darf und was damit passieren soll:

```
$ host -t TXT gmx.de
gmx.de text "v=spf1 ip4:213.165.64.0/23 -all"
```

Die Firma GMX legt also fest, dass alle Server im Netzbereich von 213.165.64.0 bis 213.165.65.255 E-Mails von der Domäne `gmx.de` verschicken dürfen. Alle anderen Server sind laut diesem SPF-Record nicht für die Benutzung dieser Domäne in der Umschlag-Absenderadresse autorisiert.

Der Einsatz von SPF kann aber auch Probleme verursachen, wenn der Empfänger seine E-Mails an eine andere E-Mail-Adresse weiterschickt: Das empfangende System sieht in diesem Fall die Domain des Absenders in Verbindung mit der IP-Adresse des umleitenden Systems. Letzteres wird jedoch typischerweise nicht von den SPF-Regeln erfasst sein, sodass eine solche Mail bei einer SPF-Prüfung als unautorisiert eingestuft wird.

SpamBewertung

Dspam, SpamAssassin, Mimedefang

In der Praxis hat sich ein Mix obiger AntiSpamMechanismen bewährt

Als Ergänzung sei hier noch angeführt:

Telekommunikationsgesetz
ISPA – Spam Code of Conduct
RTR – Informationen betreffend unerwünschte Werbung mittels elektronischer Post