

Optimierte AntiSpam-Maßnahmen für IBH Internet-Server basierend auf Debian GNU/Linux

Die extreme Zunahme von unerwünschter EMail („Spam“) führt zu einer wesentlichen Belastung der EMail-Ressourcen in den Unternehmen. Außerdem entstehen indirekt Kosten durch den Diebstahl der Arbeitszeit, die benötigt wird, um unerwünschte EMail zu bearbeiten und zu löschen.

Rechtliche Aspekte

Innerhalb der EU gibt es auf Grundlage des Wettbewerbsrechts einheitliche Vorgaben zum Umgang mit unerwünschter Werbung per EMail. Abgesehen von eventuell anderen Regelungen im Ausland, ist die Realität jedoch, dass sich die meisten Spammer nicht an die Gesetze halten. Außerdem verschleiern sie ihre Identität und verwenden zum Spammen gehackte (manipulierte) Firmencomputer sowie in zunehmendem Umfang sogenannte „Botnetze“ aus infiltrierten Heim-PCs.

Darüber hinaus ist die rechtliche Definition von unerwünschter Werbung nicht identisch mit unserer allgemein üblichen Definition von Spam. Während weltweit bei den Internet-Benutzern jede Art unerwünschter EMail, die uns in unserem Persönlichkeitsrecht verletzt und/oder uns in unserer täglichen Arbeit behindert, als Spam verstanden wird, haben die Juristen Spam ausschließlich als unerwünschte kommerzielle EMail definiert. Auch die subjektive Bewertung von EMail kann sich unterscheiden. Während ein Empfänger den Newsletter als willkommene Informationsquelle betrachtet, mag ihn ein anderer Empfänger als Spam betrachten.

Bei der Optimierung der Spam-Bekämpfung geht es deshalb primär um die tausenden von EMail, die von unbekanntem Absendern, mit zweifelhaftem Inhalt, in der Regel mit verschleierter Identität, mit gefälschten EMail-Adressen und Pfaden oder von gehackten Computern verschickt werden, und die nach Möglichkeit gar nicht erst angenommen werden sollen. Die aktuelle Gesetzeslage bestimmt folgendes: Ein dem Mailserver anvertrautes Schriftstück („eine EMail“), dessen Empfang gegenüber dem Absender bestätigt wurde, muss ungeöffnet, also auch unkontrolliert, dem Empfänger zugestellt werden. Deshalb muss es im Unternehmen eine Betriebsvereinbarung geben, der vom Betriebsrat bzw. den Mitarbeitern zugestimmt wurde, und die eine private Nutzung der Telekommunikationseinrichtungen ausschließt.

Bei allen Anti-Virus- und Anti-Spam-Filtern, die nach dem Mailserver installiert sind, besteht das allgemeine Problem der Zustellung der EMail. Die gerichtliche Auffassung geht dahin, dass der Absender darauf vertrauen können muß, dass eine EMail dem Empfänger auch zugestellt wurde, wenn der Mailserver sie bereits übernommen hat. Nach Ansicht des OLG Karlsruhe ist eine EMail einem Server zur Weitervermittlung eindeutig anvertraut, wenn dieser die EMail ordnungsgemäß angenommen und quittiert hat. So lange der empfangende EMail-Server noch nicht das „250 OK“ gegeben hat, ist das Tatbestandsmerkmal „zur Übertragung anvertraut“ gemäß StGB § 206 Abs. 2 Nr. 2 noch nicht gegeben. Deshalb ist es sinnvoll, eine ganze Reihe praxisrelevanter Filtermaßnahmen schon vor diesem Zeitpunkt anzusetzen, da diese dann strafrechtlich nicht relevant sind. Eine Filterung und Blockierung der EMail mit Spam oder Schadcode vor Ihrer Annahme ist vor allem deshalb sinnvoll, weil dadurch beim betroffenen Unternehmen erhebliche Ressourcenbelastungen vermieden werden.

Optimale Spam-Abwehr mit IBH

Die hier von **IBH** vorgestellte **AntiSpam Lösung** erweitert den MTA (Mail Transfer Agent) auf Installationen des *IBH Internet Servers* (basierend auf Debian GNU/Linux) um zeitgemäße und rechtlich absicherbare Abwehrmechanismen gegen das ständig steigende Spam-Aufkommen im Internet. Sie geht davon aus, dass der IBH Internet Server entweder als *Perimeter Mail Relay* oder als finaler *Mailserver* eingesetzt wird. Da auf den *IBH Internet Servers* nur Sendmail bzw. Postfix zum Einsatz kommen, ist die Lösung auf diese beiden MTAs beschränkt. Für einen erweiterten Schutz gegen Malware kommt als MTA Postfix mit Amavis zum Einsatz, was dann durch eine Lizenz der AntiVirus-Software F-Prot (ebenfalls im Vertrieb von IBH) ideal ergänzt wird.

Die Grundphilosophie der Lösung ist die schnellstmögliche Ablehnung von hinreichend sicher erkanntem Spam, noch vor der vollständigen Annahme der EMail. Wenn eine sofortige Ablehnung nicht sinnvoll erscheint, wird die EMail mit entsprechenden Markierungen im Header versehen und weiter ausgeliefert. Als *wahrscheinlicher Spam* erkannte EMail wird dabei als Attachment weitergeleitet, damit sie im MUA (Mail User Agent) nicht angezeigt wird, aber trotzdem unmodifiziert verfügbar bleibt, falls die Einordnung fehlerhaft war.

Die Lösung besteht aus spezifischen Einstellungen am MTA sowie einigen Zusatzkomponenten, die den MTA erweitern. Auf der folgenden Seite folgt eine detailliertere Beschreibung der Maßnahmen sowie die Systemvoraussetzungen.



AntiSpam-Maßnahmen im SMTP-Dialog

Der wesentliche Ansatzpunkt für die sofortige Abweisung von mit höchster Wahrscheinlichkeit unerwünschter EMail ist der SMTP-Dialog. Hier wirkt eine Kombination von Maßnahmen zusammen:

- **SMTP-Hardening** - Befehle wie **EXPN** und **VERFY** werden deaktiviert, ESMTP-Features wie **PIPELINING** werden auf bekannte Gegenstellen eingeschränkt. Spamtool-typische Protokollverstöße werden durch eine kurze *Pause* erkannt und geblockt. Die Höchstzahl an *parallelen Empfängern* ist limitiert, wenn im Protokoll mehrfach *unbekannte Empfänger* auftauchen wird der Ablauf zusätzlich verzögert.
- **Rate Limiting** – Eine Kombination aus *globalem Rate Limit*, *per-Client Rate Limit* und *per-Client Connection Limit* reduziert den Eingang von neuen EMail auf ein angemessenes Maß und verhindert ein *DoS* auf die aufwendigeren Inhaltsfilter. Auch bei *hoher Systemlast* setzt der MTA die Mailannahme aus.
- **Greylisting** – EMail mit bisher unbekanntem Absender, Empfänger und einliefernder IP-Adresse werden *temporär abgelehnt*. Korrekte MTAs versuchen es später erneut, Spamtools typischerweise nicht. Das Verfahren kann die Einlieferung von EMail um eine *nicht vom Empfänger beeinflussbare* Zeit verzögern, ist also nicht in jedem Fall sinnvoll und daher optional. Die bei IBH gemessenen Erfolgsraten des Verfahrens (typisch >97% Ablehnungsquote) wiegen die Nachteile aber oft auf. *Whitelisting* von bekannten und erwünschten Absendern reduziert die Auswirkungen der Verzögerung.

Die Auslieferung an Gegenstellen, die ihrerseits Greylisting nutzen, wird durch *gestaffelte Warteschlangen* beschleunigt.

- **DNSBL** – Mit geeigneten *DNS Blacklists* werden IP-Adressen, die vom Listenbetreiber als Spamschleuder erkannt wurden, *an jeglicher Mailanlieferung gehindert*. Die Blacklists müssen geeignet gewählt sein, IBH empfiehlt momentan die Kombination aus *NiX Spam* (Heise) und *SBL-XBL* (Spamhaus).
- **Sender Validation** – Absenderadressen werden auf syntaktische und semantische Korrektheit geprüft.
- **Recipient Validation** – Die *sofortige Ablehnung von inkorrekten Empfängeradressen* ist ein essenzieller Bestandteil jeglicher Spamabwehr auf Perimeter Mail Relays. EMail zunächst anzunehmen, an den inneren Mailserver weiterzuleiten, dabei zu erfahren dass der Empfänger gar nicht existiert und dann einen *Non-Delivery Report* (Bounce) zu generieren ist nicht mehr zeitgemäß, da der Mechanismus inzwischen zur Erzeugung von *Bounce-Spam* missbraucht wird. Die Liste zulässiger Empfänger kann manuell gepflegt oder automatisch (z.B. per LDAP-Anfrage an ADS) erstellt werden. IBH hilft bei der Integration.

AntiSpam-Maßnahmen durch Content-Filter

Der SMTP-Dialog endet mit der eigentlichen Datenübertragung. Vor deren abschließender Bestätigung finden inhaltliche Prüfungen statt, die noch zur Ablehnung der EMail führen können:

- **Spamassassin** – Die bewährte Software zur Ermittlung der Spam-Wahrscheinlichkeit einer EMail wird hier bereits bei der Einlieferung benutzt. Übersteigt die Bewertung eine Grenze, ab der man *mit Sicherheit* von Spam ausgehen kann (15 Punkte), dann wird die Annahme verweigert. Ansonsten wird die EMail angenommen, sollte sie eine *zweifelhafte* Bewertung erhalten (ab 5 Punkte) markiert Spamassassin sie in geeigneter Weise für eine beliebige Weiterbehandlung im MUA. Bevorzugt wird dabei die *unveränderte Originalmail* zum *Anhang* einer neu generierten EMail, welche den Spamstatus erläutert. Der Nutzer kann so im Falle einer falsch-positiven Erkennung problemlos auf das Original zugreifen.

- **ClamAV** – Der freie Virenschanner ClamAV wird bereits bei der Einlieferung benutzt, um *einfach zu erkennende Malware* (Viren, Trojaner, Phishing etc) bereits vor der Annahme *abzuweisen*. Das ersetzt keine vollwertige AV-Lösung, stellt aber eine erste Verteidigungslinie zum frühestmöglichen Zeitpunkt dar.

- **optional AMaViS** – Die AMaViS-Schnittstelle ermöglicht die Ankopplung eines kommerziellen AntiVirus-Werkzeugs. IBH empfiehlt dafür den Einsatz der Software F-Prot von FRISK. F-Prot ist in einer Variante für Linux-Mailserver erhältlich und wird nach der Zahl der geschützten Mail-User lizenziert.

Systemvoraussetzungen

| |
|--|
| - IBH Internet-Server mit Betriebssystem Debian GNU/Linux (Etch/stable bzw. Lenny/testing) |
| - mind. Pentium 4 Prozessor (oder neuer) - mind. 512MB RAM (optimal: 1024MB) |
| - System agiert als Mailforwarder, auf das die MX-Einträge in der Maildomain verweisen |
| - <i>Alternativ:</i> direkt im IBH Rechenzentrum gehosteter Internet-Server |

Konditionen

| |
|--|
| 1.) Vorhandener Internet-Server mit gültiger Vereinbarung über IBH Linux Update-Service: 400,00 EUR/einmalig |
| 2.) Vorhandener Internet-Server ohne gültige Vereinbarung über IBH Linux Update-Service: wie 1.) zzgl. 90,00 EUR/Stunde nach Aufwand für Vorbereitung des Systems für AntiSpam-Lösung |
| 3.) Einweisung für die Eigenadministration durch den Kunden, Hinweise zu Optimierungsmöglichkeiten: 400,00 EUR/einmalig |

Das eigentliche, dahinterliegende Mailsystem muß die finale Zustellung der EMail über das SMTP-Protokoll bieten.

Alle genannten Preise verstehen sich netto zzgl. aktuell geltender Mehrwertsteuer.

Nehmen Sie Kontakt zu IBH auf!

Bei weiteren Fragen, für zusätzliche Detailinfos oder um ein kaufmännisches Angebot zu erhalten, rufen Sie uns bitte einfach an – 0351 477 77 20 – oder senden Sie uns eine EMail – sales@ibh.de. Weitere Informationen zum umfangreichen Leistungsportfolio der IBH IT-Service GmbH entnehmen Sie bitte der Webseite:

<http://www.ibh.de/>