HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

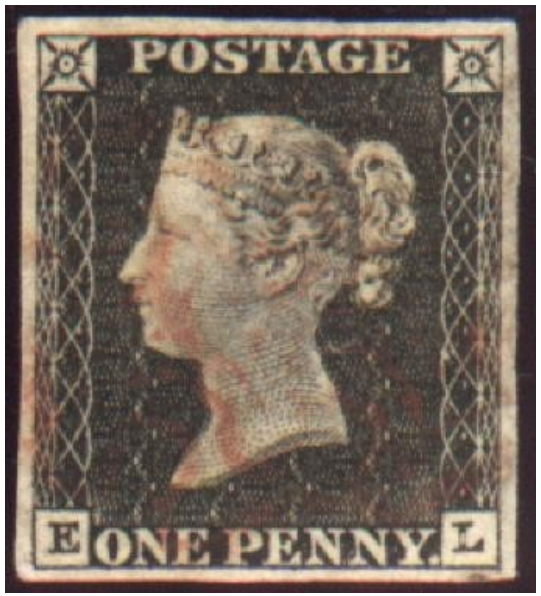
Gleich geht’s los...

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Irrungen der Geschichte: Die Briefmarke gegen Spam

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

PennyBlack: Der Blick in die Geschichte



- Das Problem:
  SPAM kostet nichts.
  - 100 Millionen Mails für < 100 US-$ sind „nichts“!
- Die Lösung (a la Microsoft):
  Mails müssen etwas kosten.
  - „PennyBlack“, die E-Mail-Briefmarke
  - Kosten durch Resourcenverbrauch (CPU), Aufgabe („Captcha“) oder $$$
  - MS erklärte sich großzügig bereit, das Inkasso zu übernehmen
- Rest der Welt wollte sich das SPAM-Problem nicht lösen lassen.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

SPF:
Sender Policy Framework

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

SPF – das Sender Policy Framework: Die Idee dahinter

- Das Problem:
  Spammer können Absender beliebig fälschen.
  - SMTP sieht keine Verifizierung eines Absenders vor.
  - MX-Records im DNS regeln nur Empfangs-, nie aber Versendeserver
    - Behauptungen, der MX-Record würde Outbound definieren, sind absoluter Quatsch.
- Die Lösung:
  Versendeserver einer Domain festlegen
  - So könnte geprüft werden, wer Mails mit einem best. Absender versenden darf
  - Könnte Absenderfälschungen wirksam eindämmen – ärgert Spammer.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

SPF:
Die technische Umsetzung

- Versendeserver müssen im DNS geregelt sein
  - Eigene DNS-Records nur langwierig einzuführen
  - TXT-Feld im DNS ungenutzt, kann „mißbraucht“ werden
  - Eigene SPF-Records jetzt seit RFC 4408 (bind 9.4) vorgesehen
  - langsame Verbreitung neuer DNS-Software

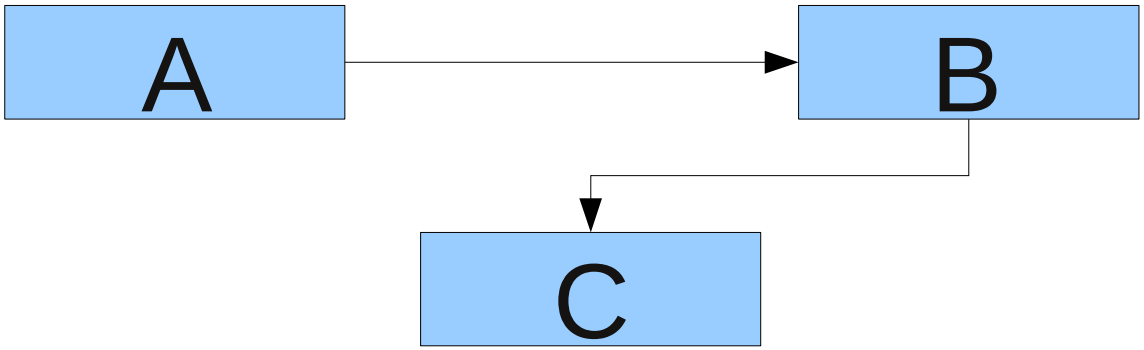
HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

SPF:
So sieht das aus.

- SPF-Records, ein Beispiel:
  heinlein-support.de. IN TXT "v=spf1 ip4:213.203.238.0/25 ip4:195.10.208.0/24 mx include:jpberlin.de ?all"
  - v=spf1 – SPF-Record Version 1
  - ip4:xxx.xxx.xxx.xxx/xx – Netzbereich ipv4 (analog: ip6:)
  - mx – Die Server, die auch als MX-Records inbound definiert sind
  - include:domain.tld – SPF-Record einer anderen Domain (des Providers)
  - a:host.domain.tld – der genannte Hostname
  - ?all – Über alle *nicht* genannten Server wird *keine* Aussage getroffen
    - (Alternativ: „-all“ -- alle anderen Server dürfen nicht, +all – alle anderen dürfen)

SPF:
Aber warum dann „-all“?

- Problem 1: Weiterleitungen

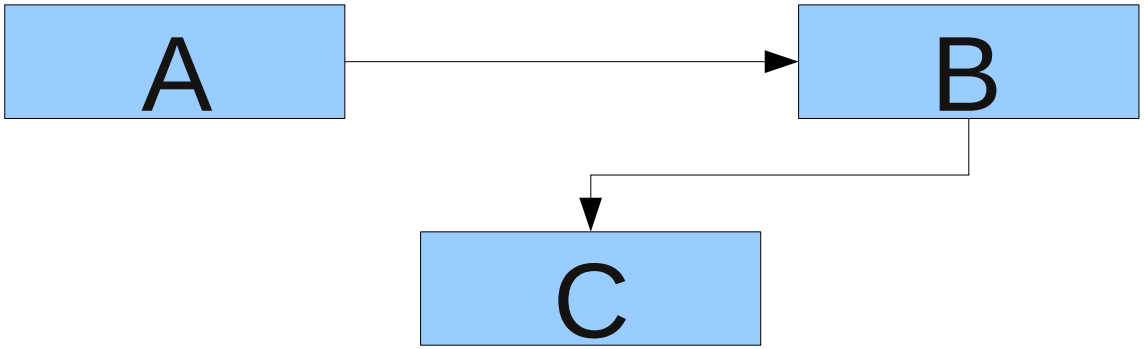


- Mails @A versandt von Server B bei „-all“ laut SPF nicht erlaubt.
  - Nutzer haben aber millionenfach Weiterleitungen!
  - SPF: „Nutzer @C muß eben @B whitelisten.“

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

SPF:
Aber warum dann „-all“?

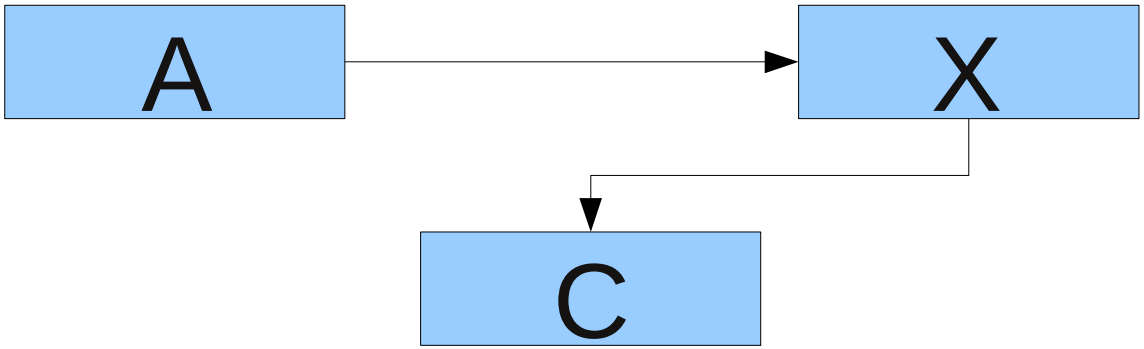
- Problem 2: Mailinglisten



- @A schreibt an Mailingliste @B
- @C empfängt legal Mails @A über Server @B
  - Läßt sich noch dadurch lösen, daß Absender = Mailingliste
  - Wünschenswert?!?

SPF:
Aber warum dann „-all“?

- Problem 3: Communities, Webforen, Grußkarten, Heise-Ticker



- Empfang der A-Mails von Server X laut SPF nicht erlaubt.
  - Müßte eh Envelope-Absender = Postmaster@Forum sein
  - Macht aber jetzt schon fast niemand richtig!

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Sender Rewriting Scheme (SRS): Die Lösung des Weiterleitungsproblems?

- Weiterleitungsmechanismus: Sender Rewriting Scheme (SRS)
  - Aus user@domain1 wird domain1=user@domain2
  - Es gelten die SPF-Records von domain2
- Problem: Spammer B kann weiterhin Adressen fälschen!
  - Crypto-Hash HHH und Timestamp sollen schützen:
    SRS0=HHH=TT=domain1=user@domain2

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Sender Rewriting Scheme (SRS): Es funktioniert nicht.

- Mailserver müßten das überhaupt erstmal implementieren
  - Wie lange dauert das, wenn heute noch Exchange 4.0 von 1998 aktiv ist?
- Geht nur, wenn alle mitmachen
  - Implementiert ein Weiterleitungsserver kein SRS; so bricht er die Kette
  - Alle Mails der Nutzer mit „-all“ werden geblockt
- Was passiert bei mehrfachen Weiterleitungen?
- Was passiert bei Antworten?
  - Und: 1990 – 1998: Gatewayadressierungen brachten nur Ärger, Ärger, Ärger
- Aber: Nutzer sehen sowieso Mailheader, nicht Envelope

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

SPF:
Ist das jetzt Spamschutz?

- SPF authentifiziert erstmal nur Absender
- Wirkt nur mittelbar als Spamschutz
  - Spammer müßten vorzugsweise eigene Domains mit eigenen SPFs nutzen
  - Eigene Domains sind spottbillig und schnell zu kriegen, ggf. sogar kostenlos
  - Gefälschte Owner-Daten bei Domains kein Problem

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

SPF:
Was macht SpamAssassin daraus?

- SPF wird gebrochen:
  - Könnte gefälschte Adresse sein
  - Könnte aber auch Weiterleitung/Liste/Forum sein
  - Kein hartes Ablehnungskriterium – kann aber einfließen!
  - SpamAssassin: score SPF_FAIL 2.600 0.992 1.669 0.693
- SPF wird eingehalten:
  - Soll Mail privilegiert / gewhitelisted werden?
  - Spammer könnte eigene Domain mit eigenem SPF nutzen!
  - Kein Whitelisting-Kriterium!
  - SpamAssassin: score SPF_PASS -0.001

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

SPF:
Die Quintessenz

- Die Definition eines eigenen SPF-Records ist einfach und schadet nichts...
  - Schema laut Vortrag, Hilfe auf http://www.openspf.org
  - Aber immer „?all“ angeben!
- ...bringt aber auch nicht wirklich etwas
  - Aber einige nutzen SPF_PASS fälschlicherweise als „starkes“ Kritierium, das kann man sich ja zu nutze machen, wenn es funktioniert.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

DKIM:
Domain Key Identified Mail
RFC 4871
(früher: Yahoo Domain Keys)

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

DKIM – Domain Key Identified Mail: Die Idee dahinter

- Selbe Grundidee:
  Absender nicht authentifiziert, Versendeserver beliebig
- DKIM-Lösung:
  Auch Daten im Mailheader müssen authentifiziert werden
  - Nutzer sieht und antwortet u.a. an From: aus Mailheader!
- Kryptographische Signierung relevanter Headereinträgen und des Bodies der E-Mail
  - Zugleich angenehme Nebeneffekte: Fälschungssicherheit!

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

DKIM:
Die technische Umsetzung

- Mailserver einer Domain haben Schlüssel
  - Sie signieren Mails (Body + ausgewählte Header-Zeilen)
- Public-Key der Domain über DNS-TXT abfragbar
- Andere Server können Key fetchen und Mails prüfen
  - Über sog. Selektoren können mehrere Keys parallel benutzt werden
  - Wichtig für Key-Expire oder externe Dienstleister

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Welche Header fließen in die DKIM-Signatur ein?

- Diese Header sollten von DKIM erfaßt werden:
  - From (erforderlich in allen Signaturen)
  - Sender, Reply-To
  - Subject
  - Date, Message-ID
  - To, Cc
  - MIME-Version
  - Content-Type, Content-Transfer-Encoding,Content-ID, Content-Description
  - Resent-Date, Resent-From, Resent-Sender, Resent-To, Resent-Cc, Resent-Message-ID
  - In-Reply-To, References
  - List-Id, List-Help, List-Unsubscribe, List-Subscribe, List-Post, List-Owner, List-Archive
- Diese Header haben in DKIM nichts zu suchen:
  - Return-Path
  - Comments, Keywords
  - Bcc, Resent-Bcc
  - DKIM-Signature
  - Authentication-Results

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

So sieht eine DKIM-Signatur in der Praxis aus

- DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/simple; d=xing.com; h=date:message-id:content-type:mime-version:subject:reply-to:from:received:received:received:x-virus-scanned;s=main;t=1286749000;bh=1eEgKOQyOuKTyyPhvs1P6EUnp68IMRZNk6og84vd1+I=;b=HfWryPy6Us45G6SPVZNSjIuZbMzM/iQgMIhdB5c/fPRwNng+wUaIG2sHRmP0toqqge5yAQ7dvdfWZ4QnpsJYDaiO3PUF1F1t0BbSYl/R4ld/0QFmzwwvAEpqWHHWSenj4j8rT8w9Qkakt5cSn0IoMseelsMd5lgbD8YlVDIeflQ=

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

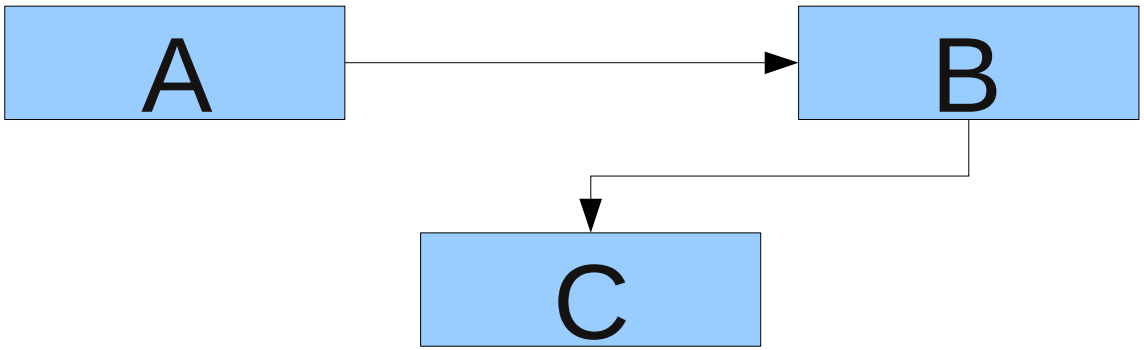
Was sagt uns das über nicht-signierte E-Mails?

- Author Domain Signing Praxis (ADSP)
  - Definiert in RFC 5016
- Einfache Methode, mit der der Absender sagen kann, welche Signatur-Politik seine Domain haben soll.
  - Soll Header-Spoofing vermeiden
- Ebenfalls einfache Definition in DNS-TXT-Feld „_adsp“:
  - _adsp._domainkey.example.com IN TXT „dkim=all“
  - Unsignierte Mails dieser Domain invalide

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

DKIM:
Wo ist der Unterschied zu SPF?

- DKIM und SPF im Vergleich:
  Mails können beliebig weitergeleitet werden!



- Server C findet Absender und Signatur von A!
  - DKIM sichert, daß Mail mal über A versandt wurde, auch wenn sie von B kommt!

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

DKIM: Weiterleitungen und Mailinglisten?

- Wenig Probleme bei Mailinglisten und Communities
  - Keine Adreß-Umschreibungen nötig
  - Keine Anpassungen der MTAs, einfache DKIM-Filter etc. reichen
- Aber: Kaputte Software zerstört ggf. DKIM-Header
  - Insb. Zeichensatzkonvertierung zerstört die Prüfsummen
  - Problem ist lösbar => Software fixen => Kommt Zeit, kommt Update
  - Mailinglisten sollten eingehende DKIM-Header ggf. einfach löschen und selbst neu signieren

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Was bringt DKIM?

- Doch gleicher Fragestellung nach dem Nutzen wie bei SPF!
  - Positives Whitelisting?
    Spammer können eigene Domains nutzen
  - Negatives Blacklisting?
    Würde sehr viele normale Mails treffen, es werden nie alle mitmachen.
- DKIM ist eine Technik, um darauf aufbauend Nutzen zu ziehen
  - Grundlage bspw. für Reputationsprojekte, die validierte Absender brauchen

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

DKIM: Wie nutzt man das?

- Früher: DKIM-Proxy:
  - http://dkimproxy.sourceforge.net/
- Besser: Amavis
  - Ab Version 2.6.0 (Juni 2008) native DKIM-Unterstützung auch ohne SpamAssassin
  - Amavis kann ausgehende E-Mails prüfen – aber auch signieren!
  - Wohl beste Lösung, wenn Amavis eh im Einsatz ist

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

DKIM: Mini-Howto für Amavisd-new

- Schlüssel erzeugen:
  - Amavisd genrsa /var/spool/amavis/dkim/key.pem
- amavisd.conf anpassen:
  - $enable_dkim_verification = 1; # enable DKIM signatures verification
    $enable_dkim_signing = 1; # load DKIM signing code,
    dkim_key('example.com', 'abc', '/var/spool/amavis/dkim/key.pem');
  - Domain muß in local_domains_maps enthalten sein!
- Key im DNS veröffentlichen
  - amavisd showkeys
    abc._domainkey.example.com. 3600 TXT ("v=DKIM1; p="
    "MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDQcNuAysGQ4YxBhgPl6u"
    "JutgxhazJDOEw0zeNNbor9nPhDllMwT9WHPBCxQEpE4NvwDFmhaBh0/jdjYEl/kZ"
    "11u5bsMWo/8cf4RYgrEbklc0f9HJ+pyx4eNq9BTgWn8mDFc2Y36cmz5K2tBrpPT0"
    "ElR7qsLo5bIKjBAFkQIDAQAB")
- Testen:
  - amavisd testkeys
    TESTING: abc._domainkey.example.com => pass
- Mails senden und testen

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Achja. Dann war da noch... Microsoft

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Achja...
Microsoft

- Nach dem PennyBlack-Mißerfolg kam die MS Caller-ID
- Abgekupfertes SPF einmal durch den Fleischwolf gedreht:
  - Nutzt Subdomain „_ep“: „_ep.domain.de“
    Achja: Ein führendes „_“ im Namen ist eigentlich gar nicht erlaubt...
  - Nutzt XML statt Leerzeichen um Information zu codieren
    Achja: MS hat ein Patent auf XML in DNS-Records
    Achja: Normale MTAs haben mit XML gar nix am Hut / keinen XML-Parser
- Caller-ID scheiterte, da nicht patentverletzungsfrei machbar

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Warum einfach wenn es auch kompliziert geht.

- So sieht das aus: „host -t TXT _ep.hotmail.com“ ergibt:

```
_ep.hotmail.com descriptive text "
<ep xmlns='http://ms.net/1' testing='true'>
  <out>
    <m>
      <indirect>list1._ep.hotmail.com</indirect>
      <indirect>list2._ep.hotmail.com</indirect>
      <indirect>list3._ep.hotmail.com</indirect>
    </m>
  </out>
</ep>"
```

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Achja: Microsoft

- Trat SPF-Konsortium bei um Gutes zu tun
- Erfand Sender-ID-Framework: SIDF = SPF + Caller-ID
  - Sichert ähnlich wie DKIM auch Mailheader
  - Wirkt aber nicht, da im Endeffekt nur „Resent-Sender:“ stimmen muß, was aber so gut wie kein Client anzeigt. Sender/From ist dann egal und unüberprüft.
- IETF-Arbeit an SIDF 2004 eingestellt, weil keine freie Lizenz
- MS versucht SIDF durch msn/hotmail durchzusetzen
  - Mails ohne SIDF sollen pauschal als SPAM betrachtet werden
  - AOL wurde gezwungen SIDF einzusetzen, obwohl AOL zu DKIM-Fraktion gehört
- MS wirkt mit Verbreitungszahlen von SPF für angeblich hohe Verbreitung von Sender-ID (gegen den Willen der SPF'ler)

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Zu unrecht gescholten: Greylisting

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Greylisting: Mythen und Falschinformationen

- Das Prinzip:
  E-Mails unbekannter Absender werden zunächst mit temporären Fehler (4xx) abgewiesen
  - Temporäre Fehler sind „normal“: too many connections, dns error, not enough space left on device und und und
- Später wird gleiche Mail vom gleichen Client dann akzeptiert

- Client soll zeigen, daß er ein queuender Mailserver ist
  - Botnetze queuen in aller Regel nicht => fire & forget im Massenversand
- Greylisting hilft gegen Botnetz-Mails: Spam und Viren

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Mythos 1:
Aber dann werden ja alle Mails verzögert.

- Gute Greylisting-Implementationen lernen vollautomatisch alle die Subnetze, aus denen wiederholt Triple bestätigt wurden
  - Kein unnötiger „Test“ wenn bekannt ist, daß der Client ein Mailserver ist
- Nach kurzer Trainingsphase von wenigen Tagen: 98% aller erwünschten e-Mails erhalten keinerlei Verzögerung!
  - Mailserver aller relevanten Provider und Geschäftspartner sind schnell angelernt
  - Nur Mails unbekannter neuer Absender werden verzögert => i.d.R. egal
  - Zeitkritische Empfangspostfächer ganz selektiv vom Greylisting befreien (support@/helpdesk@, bestellung@, hotline@ etc. etc.)

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Mythos 2:
Dann müßten Spammer doch nur queuen

- Ja, richtig, sie könnten natürlich queuen. Aber:
  - Erneute Zustellversuche senken den effektiven Durchsatz eines Botnetzes
  - Warum riskieren erneute Zustellversuche zu vergeuden, wenn anderswo Mails sofort zugestellt werden können?
  - Spammer haben genügend weitere Mailadressen.
  - Wer Mail bekommt ist Spammer egal. Hauptsache große Versandmenge.
  - Heutige Spamwellen oft ganz massiv unter 2-3 Stunden Gesamtzeit!
- Die Zeit arbeitet für uns:
  - Besitzer des vireninfizierten PCs bemerkt Infektion (PC nicht mehr nutzbar)
  - Zwangstrennung am Home-DSL (1h Verzögerung = 1/24 Chance auf neue IP!)
  - IP des PCs landet schnell auf Blacklisten

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Mythos 3: Greylisting ist aufwändig

- Genau das Gegenteil ist richtig.
  - Greylisting ist der „billigste“ einfachste, unkomplizierteste Spam-Schutz, den es derzeit gibt.
  - Es werden zwei Mailadressen,eine IP und ein Timestamp in einer DB gespeichert!
- Faktor 1000 mehr Last würden Mails angenommen und nur durch Content-Filterung geprüft werden!

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Mythos 4: Manche Provider senden nicht erneut

- Gerade große ISPs (web.de, gmail.com, yahoo.com) geben massenweise temporäre Fehler aus
  - Wer damit nicht umgehen kann, kann 50% seiner Mails nicht sicher zustellen
- Temporäre Fehler 4xx sind fest im RFC 2822 (SMTP) definiert
  - 4xx-Codes sind auch ohne Greylisting Alltag

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Mythos 4: Manche Provider senden nicht erneut

- Wie auch immer: Problem des Absenders
  - Kein bekannter MTA, sondern unbekannte buggy Wald- und Wiesen-Software
  - Absender scheint es seit Jahren egal zu sein, daß er relevant viele Mails nicht zustellen kann. Warum sollte ich mir dann das zu Herzen nehmen?
- Ich muß für meine Empfänger den schnelle, sicheren, zuverlässigen und staufreien Empfang normaler E-Mails von normalen Mailservern sicherstellen

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Mythos 5: Zentrale/synchrone Greylisting-DBs nötig

- Häufige (aber falsche) Behauptung: Zentrale oder synchrone DB für alle Mailrelays notwenig, sonst viele Verzögerungen
  - Bei 4xx auf Mailrelay wandert Client **sofort** zu Mailrelay 2 (...3...4).
  - Alle Mailrelays lernen zeitgleich „unbestätigtes Triple“
  - Erneuter Zustellversuch nach wenigen Minuten bestätigt auf einem der Relays das Triple => Mail geht also ganz normal durch
  - Nächste E-Mail bestätigt auf anderem Server offenes Triple
- Aber: Sehr viele Mailrelays (>4) und sehr seltenen E-Mails (alle paar Tage): ggf. langsameres „Lernen“ weil offene Triple expiren => Nicht praktisch relevant.
  - Also: Jedem Mailrelay eigene robuste (Berkley)-DB auf Dateiebene
  - Kein MySQL als Single-Point-of-Failure implementieren

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Was wäre die Welt ohne Greylisting?

- Ohne Greylisting:
  Mailstau bei jeder neuen Spamwelle!
  - Teure Content-Filterung => hoher Serveraufwand
  - SPAM steigt weiterhin exponentiell an
  - Wie will man da zukünftig skalieren?!

- Mit Greylisting:
  Beste Garantie für sofortige Mailzustellung!
  - Nur schnelle Checks trennen die Spreu vom Weizen
  - Nur wenn die Server „sauber“ gehalten werden, können echte Mails schnell verarbeitet werden!

- Gerade die kleine Verzögerung bei unwichtigen/neuen Mails garantiert die schnelle Zustellung.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Greylisting erhöht die Sicherheit

- Fast alle Viren werden über Viren-Botnetze verschickt
- Greylisting verschafft uns Zeit...
  - Virenwellen werden immer kürzer und massiver. Nach 2h ist oft alles vorbei.
  - Problem: Zeit bis zum Signaturenupdate meines Virenkillers
  - Greylisting erhöht meine Chance, aktuellere Virenpattern zu haben!
- Firmen treiben oft immensen Aufwand zum Schutz vor Viren. Greylisting ist ein billiger, einfacher, sehr erfolgreicher Spamschutz der die Lücke bis zum Virenkiller-Update überbrückt – und wird doch oft ignoriert!

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Und was bedeutet das nun alles?

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

- SPF und DKIM sind eigentlich kein Spamschutz, sondern nur der Versuch der Absender-Verifizierung
- Ausgehend SPF und DKIM schadet nicht – kann nur nützen
  - SPF: Sehr einfach. Nur kleine Änderung in DNS-Zone.
  - DKIM: Software nötig / mehr Aufwand. Mit Amavis sehr einfach.
- Eingehend SPF und DKIM nur „soft“ prüfen – wie SpamAssassin. Harte Checks sind empfehlenswert.

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

- Greylisting wird seit 2004 totgesagt
  - Fast immer auf Basis falscher Behauptungen/Annahmen
- Greylisting funktioniert seit 2004 nach wie vor hervorragend
  - Gezielt und nur gegen Botnetz-Spam
- Greylisting wird auch noch lange hervorragend funktionieren
  - So oder so – es ist nur ein Check unter vielen.
- Greylisting ist in unter 2 Minuten eingerichtet. Machen!
  - „postgrey“ von David Schweikert (für Postfix)
  - Greylisting hat so gut wie keine Nebenwirkungen

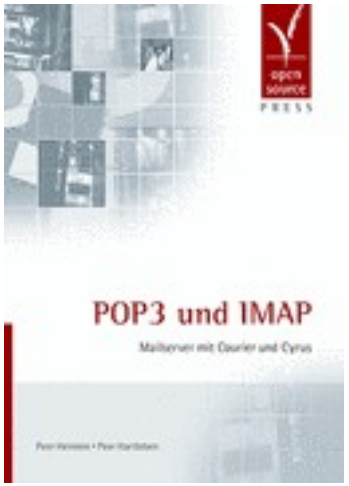
HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

- Es gibt keinen ultimativen Spamschutz
  - Es gibt kein ultimatives Medikament
  - Auch gute Medikamente rotten Krankheiten (so gut wie nie) aus
- Ergo: Kombination verschiedenster Techniken suchen
  - Greylisting
  - Policyd-weight (enthält RBL)
  - SpamAssassin
  - Persönliche Body-/Headerchecks
- Bitte nicht irgendwelchen Aussagen in irgendwelchen Foren trauen

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Wenn es um echtes Papier geht:

- „POP3 und IMAP“
  Mailserver mit Courier und Cyrus
  - Erläutert auch Detailwissen über IMAP und Mailstorage
  - Courier sehr einfach auf Dovecot übertragbar,
    Prinzipien und nötiges Wissen sind identisch



- Das Postfix-Buch
  Sichere Mailserver mit Postfix
  - Der Klassiker mit rund 750 Seiten
  - Beinhaltet auch Spamschutz und Rechtsgrundlagen
  - Seit Juni 2008 in vollständig überarbeiteter 3. Auflage

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Soweit, sogut.

Fragen?

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Und nun...

- **Vielen Dank für's Zuhören...**
- **Schönen Nachmittag noch...**
- **Und viel Spaß an der Tastatur.**
- **Bis bald.**

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Heinlein Support hilft auch bei allen Fragen rund um E-Mails:

- AKADEMIE
  - Von Profis für Profis: Wir vermitteln die oberen 10% Wissen. Geballtes Wissen und umfangreiche Praxiserfahrung aus erster Hand.
- SUPPORT
  - Wir sind das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im Heinlein CompetenceCall Notfälle, auf Wunsch auch in SLAs mit 24/7-Verfügbarkeiten.
- HOSTING
  - Wenn Hosting kein Massengeschäft sein darf: Individuelles Business-Hosting mit perfekter Maintenance durch unsere Linux-Profis. Sicherheit und Verfügbarkeit werden bei uns groß geschrieben.