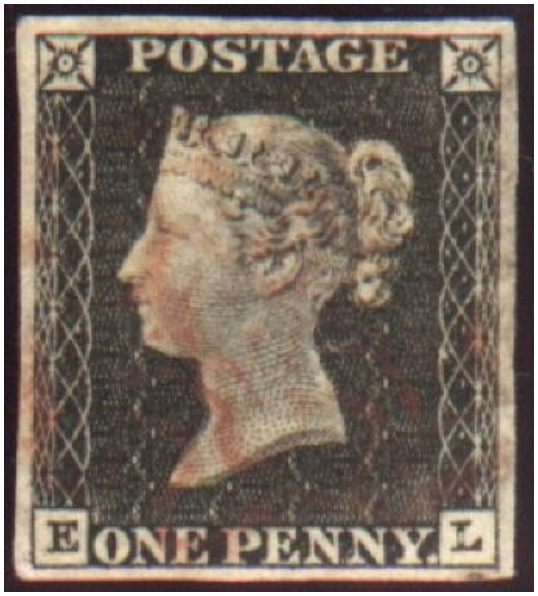
heinlein

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

SPF, DKIM und Greylisting
Noch aktuell im Spamschutz?

SPF, DKIM, Greylisting
[FrOSCon 2012]
Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Irrungen der Geschichte
Die Briefmarke gegen Spam: PennyBlack



- 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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

SPF:
Sender Policy Framework

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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 bestimmten Absender versenden darf
  - Könnte **Absenderfälschungen** wirksam eindämmen – ärgert Spammer.

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

SPF:
So sieht das aus.

- SPF-Records, ein Beispiel:

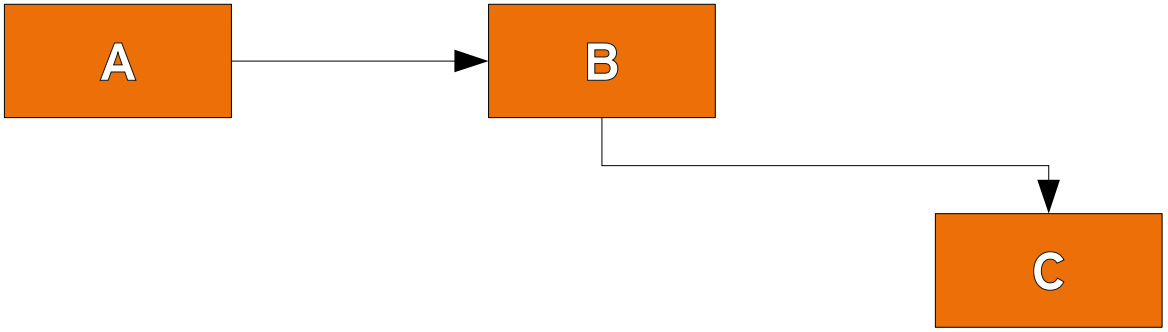
```
heinlein-support.de.  IN  TXT  "v=spf1 ip4:213.203.238.0/25
ip4:195.10.208.0/24 mx include:jpberlin.de ?all"
```

  - `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)
- http://www.openspf.org/SPF_Record_Syntax

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

SPF:
Aber warum dann „-all“?

- Problem 1: Weiterleitungen

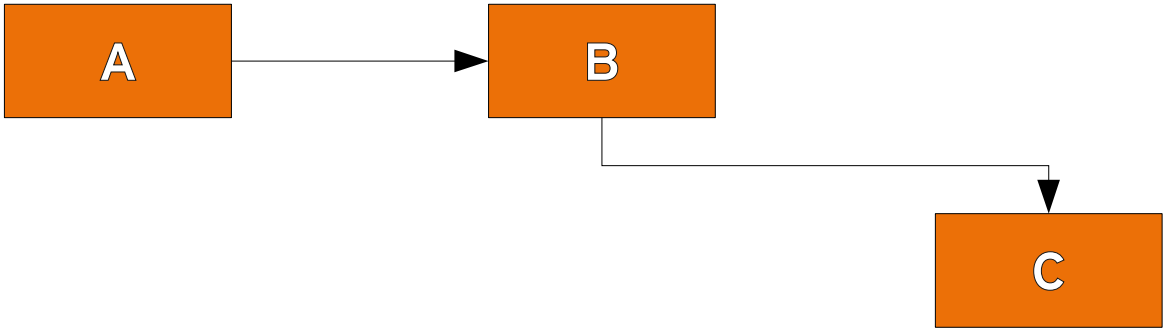


- Mails @A versandt von Server B bei „-all“ laut SPF nicht erlaubt.
  - Nutzer haben aber millionenfach Weiterleitungen!
  - SPF: „Nutzer @C muß eben @B whitelisten.“

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

SPF:
Aber warum dann „-all“?

- Problem 2: Mailinglisten

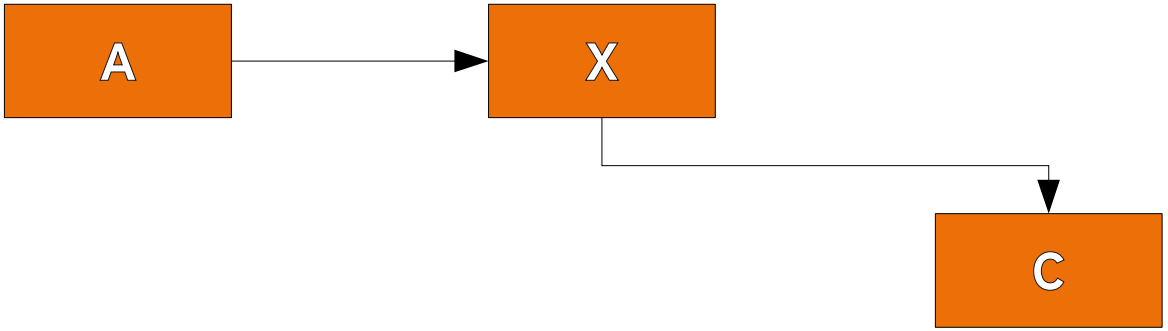


- @A schreibt an Mailingliste @B
- @C empfängt legal Mails @A über Server @B
  - Läßt sich noch dadurch lösen, daß Envelope-Absender = Mailingliste
  - Wünschenswert?!?

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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@X sein
  - Macht aber jetzt schon fast niemand richtig!

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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

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

SPF, DKIM, Greylisting
[FrOSCon 2012]
Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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.

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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!

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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+w
UaIG2sHRmP0toqqge5yAQ7dvdfWZ4QnpsJYDaiO3PUF1F1t0BbS
Yl/R4ld/0QFmzwwvAEpqWHHWSenj4j8rT8w9Qkakt5cSn0IoMse
elsMd5lgbD8YlVDIeflQ=
```

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

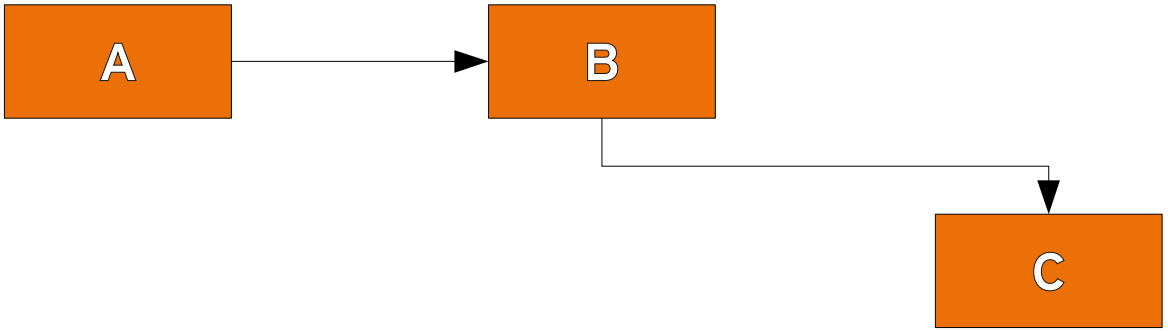
Was sagt uns das über nicht-signierte E-Mails?

- 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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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!

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Was bringt DKIM?

- Doch gleiche 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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Zu unrecht gescholten: Greylisting

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Greylisting
Das Funktionsprinzip

- 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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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 (postmaster@, support@, helpdesk@, bestellung@, hotline@ etc. etc.)

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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 Gesamtlaufzeit!
- 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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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.
- Würden Mails angenommen
  und nur durch Content-Filterung geprüft werden
  => Faktor 1000 mehr Last!

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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 schnellen, sicheren, zuverlässigen und staufreien Empfang normaler E-Mails von normalen Mailservern sicherstellen

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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 seltenene E-Mails (alle paar Tage): ggf. langsameres „Lernen“ weil offene Triple expiren => Nicht praktisch relevant.
  - Also: Jedem Mailrelay eigene robuste (Berkley)-DB auf Dateiebene
  - Keine zentrale MySQL als Single-Point-of-Failure implementieren

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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.

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

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!

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Greylisting und IPv6

- Greylisting ist – allen Unkenrufen zum Trotz – seit vielen Jahren der beste und nebenwirkungsfreieste Spamschutz, den es gibt.
  - Man muß es nur richtig einsetzen.
  - Ja, Spammer haben mit Greylisting massive Probleme
- Spammer, die mit IPv6 nun ständig Adressen wechseln, um RBLs auszutricksen, werden wegen den vielen neuen Adressen nicht mehr effektiv genug durch das Greylisting kommen.
  - Greylisting und RBL sind also wieder einmal ein Dreamteam, das sich gegenseitig absichert. Genial.

heinlein

SPF, DKIM, Greylisting
[FrOSCon 2012]
Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Anti-SPAM-Techniken und IPv6

SPF, DKIM, Greylisting
[FrOSCon 2012]
Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

RBLs und IPv6: Status Quo

- RBLs listen IP-Adressen, von denen aus Spam versandt worden ist
  - Genutzt werden Techniken, mit denen sonst DNS Reverse-Lookups gemacht werden
- Grundsätzlich geht das auch problemlos mit IPv6-Adressen

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

RBLs und IPv6: Der Haken

- Bei IPv6 erhält jeder Host potentiell viele Adressen.
  - Pro Kunde je nach Provider ein /56 oder ein /48 Netz.
  - Also SEHR viele Adressen zu verteilen.
- Problem: Spammer können für jede Spam-Mail eine neue IP-Adresse nehmen.
- Problem: Wie groß ist denn das Subnetz eines Hosts?
  - Es ist unklar, welcher Netzbereich komplett auf RBLs wandern darf!
  - Subnetz-Block zu klein: Spammer hat genug saubere Adressen.
  - Subnetz-Block zu groß: Unschuldige werden geblacklisted.

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

RBLs und IPv6

- RBLs helfen also prima gegen echte Mailrelays, über die Spam verschickt wird, denn die machen kein IP-Hopping
  - Gehackte Webseiten & Co
- RBLs helfen eventuell nur eingeschränkt gegen Botnetz-PC mit Spammer-Software drauf
  - Mal abwarten, ob/wie das genutzt wird.
- RBLs werden zukünftig eher zu WBLs, also Whitelists
  - Spamhaus hat WBL-Projekt bereits gestartet

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Policyd-weight: Nichts ist auch gut

- policyd-weight macht einen Plausibilitätscheck über die Angaben, die das einliefernde System im SMTP-Protokoll gemacht hat.
  - Besonders wird dabei Reverse-Lookup und HELO beachtet
- policyd-weight kann bei IPv6-Adressen nichts sinnvolles berechnen
  - Aber er stört sich aber auch nicht dran, liefert ein leeres Ergebnis ohne Auswirkung zurück an Postfix („DUNNO“).
- Schade, aber so funktioniert alles weiterhin.

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

SpamAssassin: Nichts besonderes

- Auch SpamAssassin hat mit IPv6 keine Probleme
  - RegExp-Pattern auf Viagra im Body gehen immernoch
  - Bayes-Filter gehen natürlich auch
  - Die von SpamAssassin geprüften RBLs gehen (prinzipiell) auch.
- Also alles schick.

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Und was bedeutet das nun alles?

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

- 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 nicht empfehlenswert.

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

- 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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

- 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

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Wer sind wir?

- wir bieten seit 20 Jahren Wissen und Erfahrung rund um Linux-Server und E-Mails
- IT-Consulting und 24/7 Linux-Support mit 21 Mitarbeitern
- Eigener Betrieb eines ISPs seit 1992
- Täglich tiefe Einblicke in die Herzen der IT aller Unternehmensgrößen

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

- Natürlich und gerne stehe ich Ihnen jederzeit mit Rat und Tat zur Verfügung und freue mich auf neue Kontakte.
  - Robert Sander
  - Mail: r.sander@heinlein-support.de
  - Telefon: 030/40 50 51 - 43

- Wenn's brennt:
  - Heinlein Support 24/7 Notfall-Hotline: 030/40 505 - 110

heinlein

SPF, DKIM, Greylisting
[FrOSCon 2012]
Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Ja, diese Folien stehen auch als PDF im Netz...
http://www.heinlein-support.de/vortrag

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Wir suchen:
Admins, Consultants, Trainer!

Wir bieten:
Spannende Projekte, Kundenlob, eigenständige Arbeit, keine Überstunden, Teamarbeit

...und natürlich: Linux, Linux, Linux...

http://www.heinlein-support.de/jobs

Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Und nun...

- Vielen Dank für's Zuhören...
- Schönen Tag noch...
- Und viel Erfolg an der Tastatur...

Bis bald.

heinlein

SPF, DKIM, Greylisting
[FrOSCon 2012]
Peer Heinlein <p.heinlein@heinlein-support.de>
Robert Sander <r.sander@heinlein-support.de>

Heinlein Support hilft bei allen Fragen rund um Linux-Server

HEINLEIN AKADEMIE

Von Profis für Profis: Wir vermitteln die oberen 10% Wissen: geballtes Wissen und umfangreiche Praxiserfahrung.

HEINLEIN HOSTING

Individuelles Business-Hosting mit perfekter Maintenance durch unsere Profis. Sicherheit und Verfügbarkeit stehen an erster Stelle.

HEINLEIN CONSULTING

Das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im CompetenceCall Notfälle, auch in SLAs mit 24/7-Verfügbarkeit.

HEINLEIN ELEMENTS

Hard- und Software-Appliances und speziell für den Serverbetrieb konzipierte Software rund ums Thema eMail.