IT-Sicherheit

- Sicherheit vernetzter Systeme -

Kapitel 15: Anti-Spam Maßnahmen

Inhalt (1)

1. Spam aus Betreibersicht
2. Spam Statistik
3. Spam Quellen
4. Abwehrmaßnahmen im Münchner Wissenschaftsnetz (MWN)
   - Mail aus dem MWN ins Internet
     - Bot-Net „Infektionen“ verhindern
     - Bot-Net Überwachung; Identifikation von Clients im MWN
     - Statistische Verkehrsanalysen
     - Authentifizierung der Sender
     - Kennzeichnung von Netzen aus denen keine Mail verschickt werden sollte
   - Mail aus dem Internet ins MWN
     - Phase I: „(Spam) Mail zurückweisen“
     - Phase II: Inhaltliche Bewertung und Markierung

- Dank an: E. Bötsch, M. Diehn, B. Schmidt, M. Storz

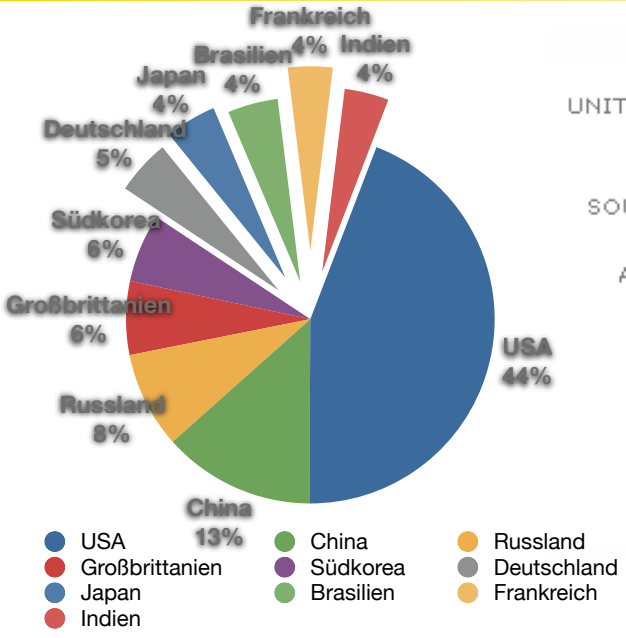
SPAM aus Sicht der Betreiber von Mail-Servern

- (seit ca. 2003/2004) Viren verschicken sich selbst und SPAM:
  - Problem: Mailadressen werden z.T. generiert
  - SPAM/Viren-Mail nicht zustellbar wenn Adresse ungültig
  - Mailserver antwortet mit Mitteilung an den Absender (ebenfalls gefälscht)
  - Mailserver versucht über längeren Zeitraum diese Mitteilung zuzustellen
  - Folge: Hohe Last auf den Mail-Servern
- Abwehrmaßnahmen, Grundidee:
  - Formale Verfahren (z.B. Protokoll-konformes Verhalten)
  - Statistische Analysen
  - Überprüfungen des sendenden Mailservers
  - Frühzeitige Verifizierung der Empfängeradressen
  - Keine Inhaltliche Analyse
- Ziel: Ressourcen-schonende Abwehr von Spam

Spam Statistiken

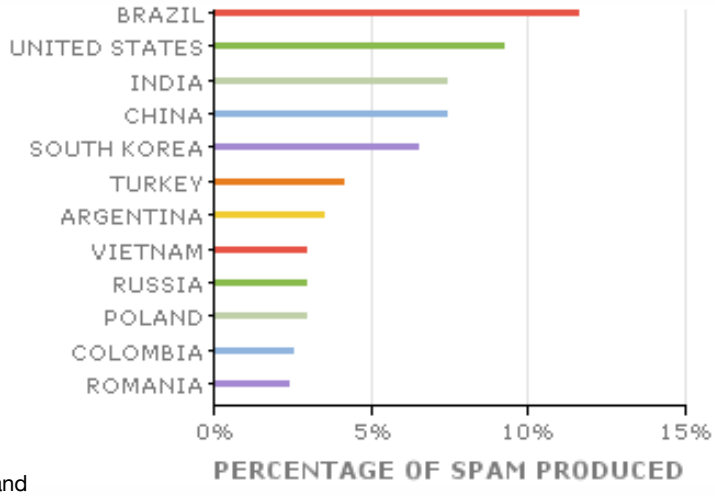
- Gesicherte Aussagen schwierig
- Unterschiedlichste Arten von Statistiken:
  - Unternehmensstatistiken
  - Statistiken von Herstellern von Sicherheitslösungen
  - Statistiken von Blacklist-Betreibern
- Unterschiedlichster Fokus
  - Regional
  - Bot-Net
- Gute Sammlung unterschiedlichster Statistiken:
  - http://spamlinks.net/stats.htm

Spam-Quellen: Länder



Top Ten Spammer; prozentuale Verteilung

www.spamhaus.org (06.01.09)

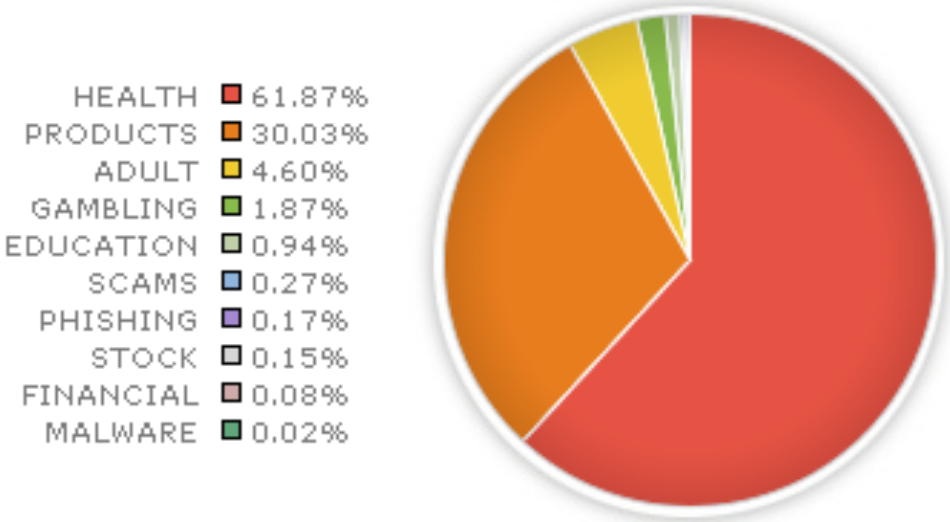


Dirty Dozend Spammer; im Verhältnis zum gesamten Spam-Aufkommen einer Woche

www.marshal.com (29.12.08-4.1.09)

Spam Statistik: Inhaltliche Klassifikation

- Quelle: www.marshal.com (29.12.08-4.1.09)



TOP Spammer (www.spamhaus.org)

1		**Canadian Pharmacy** A long time running pharmacy spam operation. Uses botnet spam techniques to send tens-of-millions of spams per day. Probably uses many affiliates all over the world to spam but is probably based in Eastern Europe and hosts sites on botnets and on Chines	**United States**
2		**Leo Kuvayev / BadCow** Russian/American spammer. Does "OEM CD" pirated software spam, copy-cat pharmaceuticals, porn spam, porn payment collection, etc. Spams using virus-created botnets and seems to be involved in virus distribution. Partnered with Vlad - aka "Mr. Green"	**Russian Federation**
3		**HerbalKing** Massive affilitiate spam program for snakeoil Body Part Enhancement scams. Also does replica luxury goods, pharma and porn. Spams via botnets, bulletproof hosting offshore and even sometimes uses fast flux hosting.	**India**
4		**Vincent Chan / yoric.net** Vincent Chan and his Chinese partners have been sending spam for years. They mainly do pharmacy, and are able to send out huge amounts daily. The use a vast amount of compromised machines, for sending, hosting and proxy hijacking.	**Hong Kong**

Stand: 08.01.09

Wichtigste Spam-Quellen

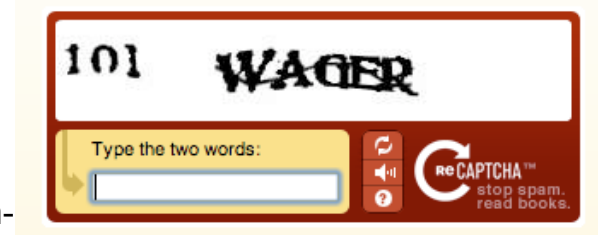
- Bot-Netze / Viren
- Wegwerf-Accounts bei Freemailern
- Weitergeleiteter Spam
  - Nutzer legt in nicht gesicherter Domäne ein .forward an
  - Gesicherte Domäne wird mir weitergeleiteter Spam belastet
- Backscatter-Spam

Spam-Quellen: Bot-Netze / „Viren“

- Start 2003: Wurmfamilien wie Sobig bauen Botnet auf
- Frühe (Spam-) Botnetze:
  - Optimiert möglichst viele Mails in kurzer Zeit zu generieren
  - keine vollständige SMTP-Engine implementiert
  - z.T. zentrale Komponenten erforderlich (Bot-Server)
  - Fire and forget Prinzip (nutzbar im Greylisting; später in diesem Kapitel)
- Neuere Template basierte Botnetze
  - Implementieren z.T. vollständige SMTP Engine
  - Spam-Templates
  - Liste von Adressen
  - arbeitet völlig autonom; keine zentralen Komponenten erforderlich

Spam-Quellen: Wegwerf-Accounts

- Freemailer bieten Möglichkeit über Web-Inferface Mail zu versenden
- Automatisiertes Anlegen von Mail-Accounts war möglich
- Spammer legt grosse Zahl von Accounts an und sendet SPAM
- Gegenmaßnahme: CAPTCHA (**C**ompletely **A**utomated **P**ublic **T**uring Test to tell **C**omputers and **H**umans **A**part)
  - Turing Test: kann Mensch unterscheiden ob er mit Mensch oder Computer kommuniziert
  - CAPTCHA: Computer unterscheidet Computer oder Mensch
  - Bsp (recapchta.net)
- Problem: erste Bots mit CAPTCHA-Erkennungsroutinen
  - 2006: phpBB-Bot registriert sich bei CAPTCHA gesichertem Bulletin-Board



Spam-Quelle: Backscatter

- Indirekter Spam durch „Rückstreuung“
- Spammer verwendet gültige Adressen als Sender-Adresse
- Automatismen generieren automatische Antwort
  - Unzustellbarkeitsnachricht (Empfänger existiert nicht)
  - Vacation-Mail
  - Empfänger erzeugt automatisiert Empfangsbestätigung
  - Weiterleitung; aber Ziel-Server nimmt diese nicht an
  - Mailing-Listen für die keine Schreibberechtigung besteht
  - Anti-Spam System berichtet über Blockade der Mail
  - Virenscanner findet Virus und informiert Sender
- Antwort (ggf. mit Spam-Inhalt) geht an unbeteiligten Dritten

Inhalt (1)

1. Spam aus Betreibersicht
2. Spam Statistik
3. Spam Quellen
4. Abwehrmaßnahmen im Münchner Wissenschaftsnetz (MWN)
   - Mail aus dem MWN ins Internet
     - Bot-Net „Infektionen“ verhindern
     - Bot-Net Überwachung; Identifikation von Clients im MWN
     - Statistische Verkehrsanalysen
     - Authentifizierung der Sender
     - Kennzeichnung von Netzen aus denen keine Mail verschickt werden sollte
   - Mail aus dem Internet ins MWN
     - Phase I: „(Spam) Mail zurückweisen“
     - Phase II: Inhaltliche Bewertung und Markierung

- Dank an: E. Bötsch, M. Diehn, B. Schmidt, M. Storz

Spam aus dem MWN ins Internet

- LRZ verantwortlich für den Betrieb der Netzinfrastruktur bis zur „Datendose“
- Verantwortung über Endsysteme liegt bei Instituten
- Vorgaben über Betriebssysteme o.ä. sind nicht möglich
- Große Hegerogenität bei den betriebenen Systemen
- Viele Gäste im Netz
- Deutlich andere Struktur als in „normalen“ Unternehmen

➡ Bestimmter Anteil infizierter Systeme lässt sich nicht vermeiden

➡ Damit auch potentielle Quellen für Spam im MWN

- Ziel: Spam soweit als möglich verhindern

potentielle eigene Spam-Quellen: Schutzmaßnahmen

- Meldung oder Beschwerde von Extern
  - Kommt sehr selten vor; Prozess zur Abuse-Bearbeitung
- Schutz vor Infektionen mit Viren oder Bot-Clients
  - LRZ betreibt eigenen Windows Update Server (WSUS)
  - Bayernweite Lizenz für Viren-Scanner; kostenlos nutzbar für:
    - Wissenschaftler
    - Mitarbeiter der Universitäten und Forschungseinrichtungen
    - Studenten
    - Nutzung für **private** Zwecke explizit erlaubt
  - Betrieb eines eigenen Update Servers für Signaturen
  - Awareness Kampagnen und Information
- Bot-Net Überwachung
  - Detektion von Bot-Net Clients
  - Sperrung entsprechender Rechner
  - Information an Nutzer oder Netzverantwortlich

eigene Spam-Quellen blocken: Verkehrsanalysen

- Statistische Analyse des TCP/IP Verkehrs
- Unterschiedliche Netzbereiche und Mechanismen
  - Private Netze, Studentenwohnheime etc.
    - dynamische Verkehrsbeschränkung (Strafpunkte)
    - ggf. automatische Sperre der Rechner
    - ➡ Nat-O-Mat (später in der Vorlesung)
  - Zentraler Internet-Übergang
    - Internetanschluss: 10 Gbit/s
    - Übergang ins deutsche Forschungsnetz (betrieben vom DFN Verein)
    - Accounting Mechanismen zur Bestimmung der Anzahl von Mail-Verbindungen
    - Verschiedene Schwellwerte
    - Derzeit keine automatischen Reaktionen
    - Alarming, (menschliche) Überprüfung und Reaktion
    - Ausnahmelisten für bekannte Mail-Server im MWN

Verkehrsanalyse: Schwellwerte

- Monitoring Intervalle: 5 Minuten und 1 Stunde
- Schwellwerte und Reaktion:
  - Statistik Log: 5 Verb. / 5 Min. 30 Verb. / 1 h
  - Soft Limit: 20 Verb. / 5 Min. 80 Verb. / 1 h (Mail an Benutzer)
  - Hard Limit: 300 Verb. / 5 Min 1000 Verb. / 1h (Sperre und Mail)
- Gründe für hohes Mail-Aufkommen
  1. Großer Mail Server
  2. Legitimer Rechner generiert viele Mail (z.B. Monitoring, Stau von Nachrichten, Software läuft Amok)
  3. Versand von Rundbriefen oder Newslettern
  4. Infektion mit Malware und / oder Kompromittierung des Rechners
- ➡ Whitelisting um False Positives zu vermeiden

Mail-Monitoring: Zahlen

- Schwellwerte (Wdh.)
  - Statistik Log: 5 Verb. / 5 Min. 30 Verb. / 1 h
  - Soft Limit: 20 Verb. / 5 Min. 80 Verb. / 1 h
  - Hard Limit: 300 Verb. / 5 Min 1000 Verb. / 1 h
- Durchschnittliches Mailaufkommen über alle Rechner
  - 1,91 Mails / 5 Minuten
  - 4,96 Mails / 1 h
- Mailaufkommen großer Server
  - bis zu 2.000 Mails / 5 Min
  - bis zu 10.000 Mails / 1 h
- Welches Mailaufkommen schafft ein inifzierter Rechner der „Aldi-Klasse“?
  - bis zu 3.500 Mails / 5 Min.
  - bis zu 18.000 Mails / 1 h

eigene Spamquellen: Gegenmaßnahmen

- Nutzer-Authentisierung bei Mail-Versand
  - Nutzer muss sich vor Mail-Versand beim Server authentisieren
    - z.B. mit Benutzernahme und Passwort
  - RFC 2476
  - Port 587 anstatt Port 25
  - Kommunikation z.B. über SSL geschützt
- Markierung eigener Netze aus denen keine Mail kommen sollte
  - Typischerweise gedacht für Dial-Up Netze
  - Eintrag in Blacklisten; z.B. PBL (Policy Block List) von Spamhaus
- Information für Betroffene: Ordentliche Pflege der RIR DB
  - Regional Internet Registry (RIR), z.B. Réseaux IP Européens Network Coordination Centre (RIPE NCC) zuständig für Europa
  - Datenbank mit Informationen über Netz und Betreiber
  - Damit Zuordnung IP-Adresse zu ISP
  - Abfrage mit: whois -h whois.ripe.net <IP-Adresse>

Sender Policy Framework (SPF)

- Erschwert das Fälschen der Absenderadresse
- Schützt damit vor Backscatter Spam
- Zusätzlicher DNS Ressource Record TXT für SPF
  - Enthält Adressen aller Systeme der Domain die Mail versenden dürfen (Sender Policy)
  - Empfangsserver kann prüfen ob sendender Rechner berechtigt ist
  - Absender-Fälscher müsste über berechtigten Mail-Server versenden
- Beispiel:
  - Abfrage nach RR vom Typ TXT für die Google Mail Domain:
    `host -t txt gmail.com`
  - `v=spf1 ip4:216.239.32.0/19 ip4:64.233.160.0/19 ip4:66.249.80.0/20 ip4:72.14.192.0/18 .....`
- Probleme:
  - Spammer verwendet Domain mit gesetztem SPF Record
  - Bot-Net Client aus korrekt konfigurierter Domain versendet Spam

Inhalt (1)

4. Abwehrmaßnahmen im Münchner Wissenschaftsnetz (MWN)
   - Mail aus dem MWN ins Internet
     - .....
   - Überblick über das Simple Mail Transfer Protokoll
   - Mail Infrastruktur im LRZ
   - Mail aus dem Internet ins MWN
     - Phase I: „(Spam) Mail zurückweisen“
     - Phase II: Inhaltliche Bewertung und Markierung
   - Betriebserfahrungen und Statistiken

- Dank an: E. Bötsch, M. Diehn, B. Schmidt, M. Storz

Simple Mail Transfer Protocol: Überblick

- Textbasiertes Protokoll; Protokollablauf

Client	Server	Erklärung
Verbindungsaufbau Port 25		
	220 mail.domain.de	Begrüßung
HELO client.domain.de		Client meldet sich an
	250 Hello client.domain.de	Server bestätigt
MAIL FROM: <user@test.de>		Absenderadresse (Envelope)
	250 Sender OK	
RCPT TO: <empfang@bla.de>		Empfängeradresse (Envelope)
	250 Recipient OK	
DATA		Client möchte Mail senden
	354 Enter mail, end with "." on a line by itself	Server akzeptiert

Simple Mail Transfer Protocol: Überblick

- Protokollablauf Fortsetzung

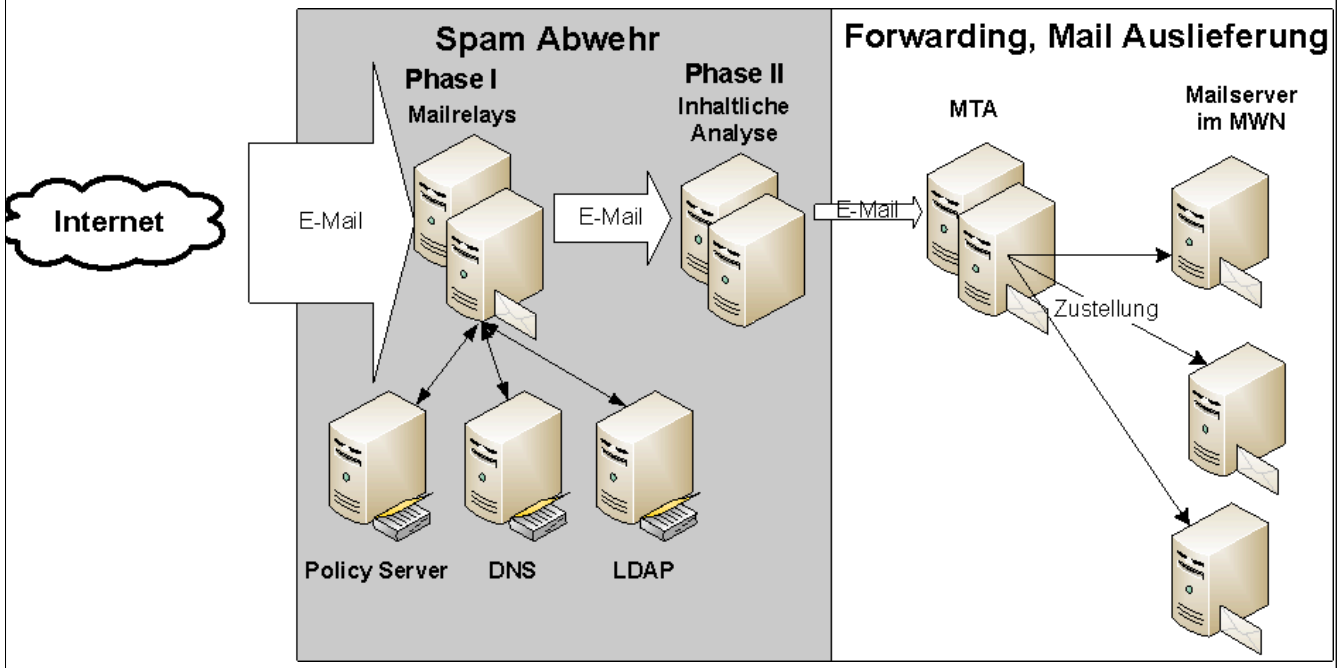
Client	Server	Erklärung
FROM: fake@fake.de TO: <gast@gast.de> Subject: Testmail Und hier kommen dann die Daten. ;-) .		Client gibt Maildaten an; Hinweis: Envelope Adressen müssen nicht mit Adressen in der Mail übereinstimmen
	250 Message accepted for delivery	
quit		Client meldet sich ab
	221 Connection closed	Server bestätigt

SMTP: ungesichertes Protokoll

- SMTP Informationen sind nicht integegritätsgeschützt
- Adressen lassen sich leicht fälschen

- DEMO

Mail-Infrastruktur im MWN



- Phase I: Entscheidung ob Mail angenommen oder abgelehnt wird; erst in Phase II wird Protokollprimitiv „DATA“ akzeptiert

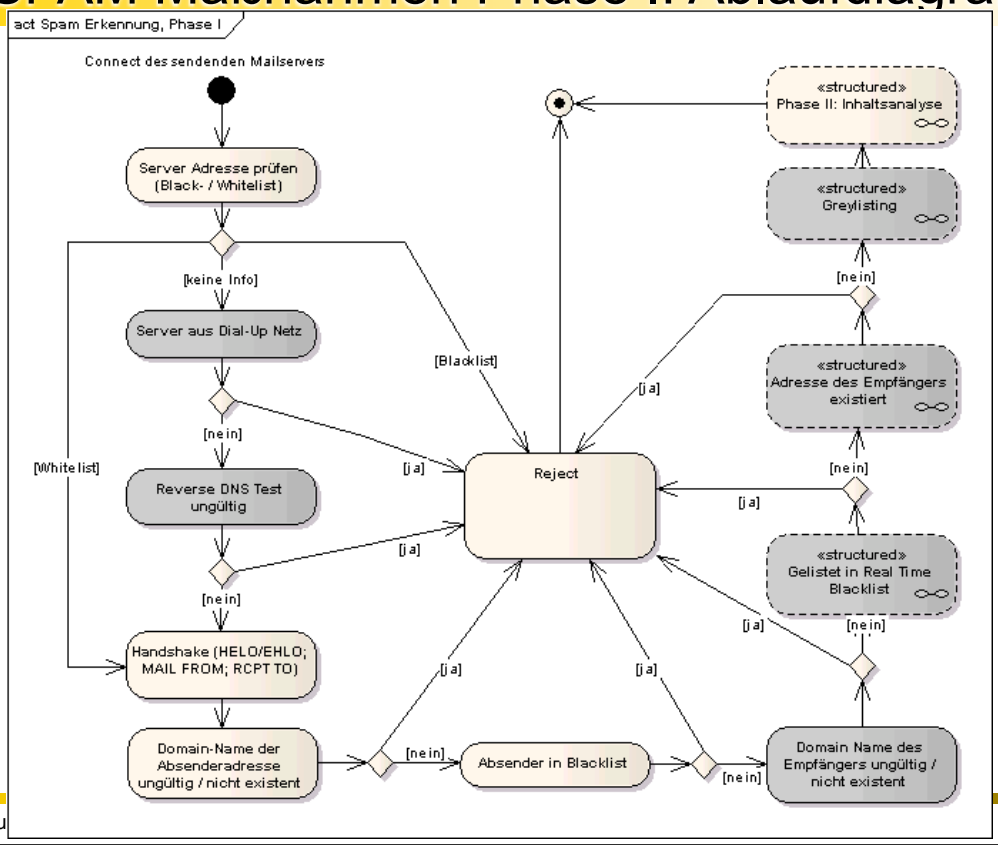
Spam Abwehr Grundlagen

- LRZ: Spam Anteil 95 - 99,5 %
- Ressourcen schonende Verfahren unbedingt erforderlich
- Grundidee:
  - Annahme nicht regelkonformer Mails ablehnen
  - März 2008: ca. 6 Mio (99,5%) Mails werden täglich abgelehnt
  - Spitzen: 20 Mio täglich
  - Sowenig inhaltliche Analyse wie möglich
  - Billige Aktionen am Anfang, teure am Ende

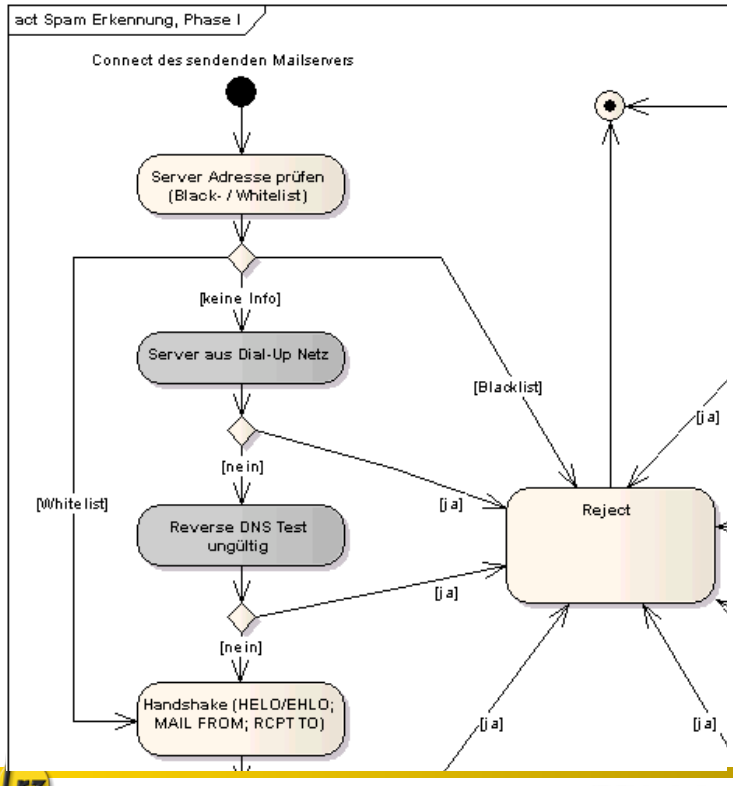
Spam Abwehr: Phase I

- Völliger Verzicht auf inhaltliche Analyse
- Kriterien zur Ablehnung abgeleitet aus Protokolllogik
- Hierfür nutzbare Daten:
  - IP-Adresse des sendenden Mail Transfer Agent (MTA)
  - Domain aus Protokollelementen HELO bzw. EHLO (vergleichbar mit HELO + zus. Info über Server-Features; ESMTP)
  - Mail-Adresse aus Envelope
  - Mail-Adresse der Empfänger aus dem Envelope
- Formale Kriterien finden die Spammer (z.B. Bot) von regulärem MTA unterscheiden; dann
- Mail sehr früh und ohne weiteren Ressourceneinsatz abgelehnen
- Regulärer MTA
  - korrekt implementiert
  - korrekt konfiguriert
  - gut administriert

SPAM Maßnahmen Phase I: Ablaufdiagramm



SPAM Maßnahmen Phase I: Ablaufdiagramm

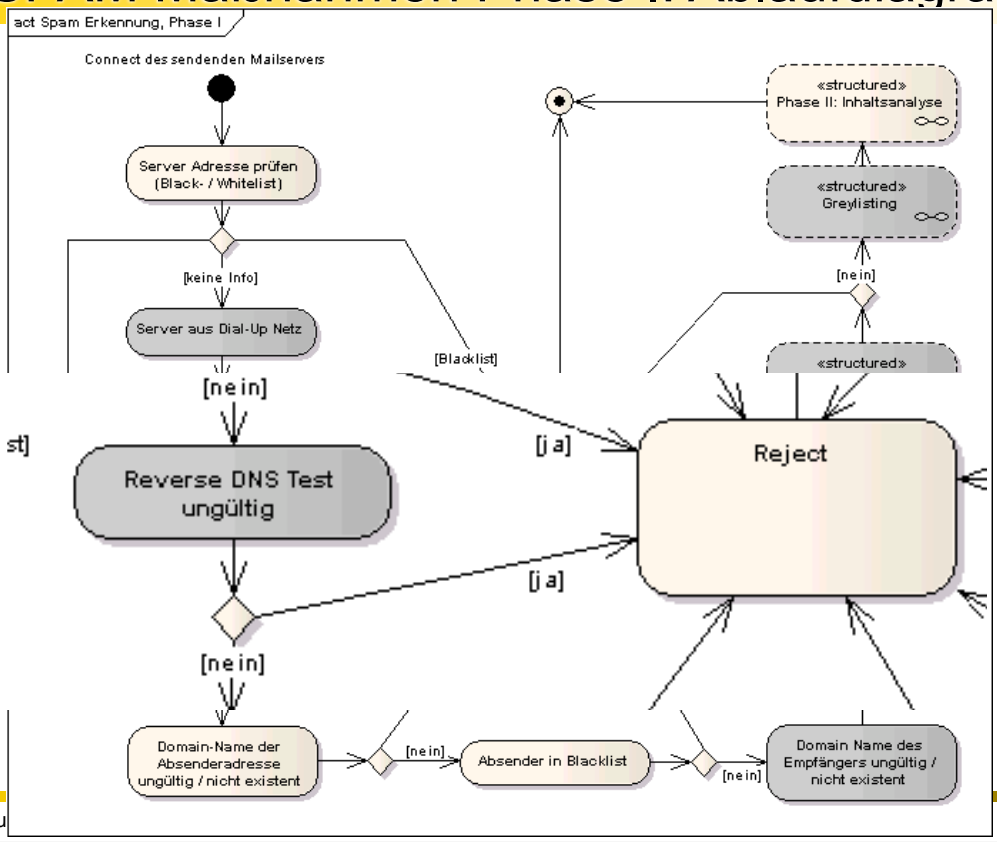


- Black/Whitelist
- Blacklist
  - Adressen und Domainnamen bekannter Spammer
  - Vom LRZ selbst erstellt und gepflegt
  - ➡ Mail wird abgelehnt
- Whitelist
  - Ausnahmeliste von Servern die als valide Mailquellen betrachtet werden
  - Bsp.: Prof. erhält Mail aus bekannter Spam Domain
  - ➡ Handshake wird ausgeführt

Phase I: Server aus Dial-Up Netzen?

- Bots finden größte Verbreitung auf PCs von Home Nutzern
  - Oft schlecht administriert; keine Sicherheitsadministration
  - ISPs führen oft keine Missbrauchserkennung durch
  - Breitbandig (DSL) ans Internet angebunden
  - Charakteristika: erhalten bei Verbindungsaufbau dynamische IP Adresse
- Wie sind Dial-Up Netze erkennbar
  - Namensgebung (z.B. t-dialin.net)
  - Idealfall: alle ISPs weltweit dokumentieren Art der Nutzung
  - Eintrag als Kommentar in der RIR-Datenbank (z.B. bei RIPE o. DENIC)
  - Markierung in DNS-basierten Blacklisten (z.B. Spamhaus PBL; vgl. später in Vorlesung)
- Können auch „reguläre“ MTAs ausgeschlossen werden?
  - Ja! Aber:
  - Statische statt dynamischer Adressen verwenden
  - tritt selten auf
  - Eintrag in Whitelist möglich

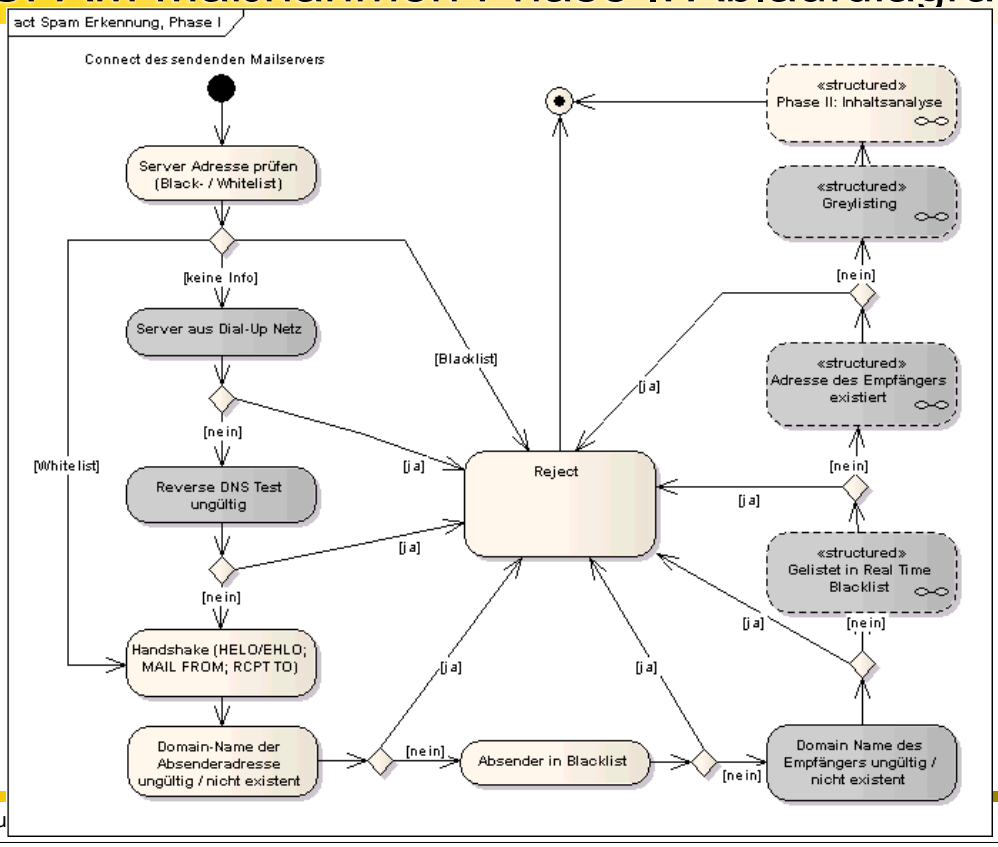
SPAM Maßnahmen Phase I: Ablaufdiagramm



Reverse DNS-Test

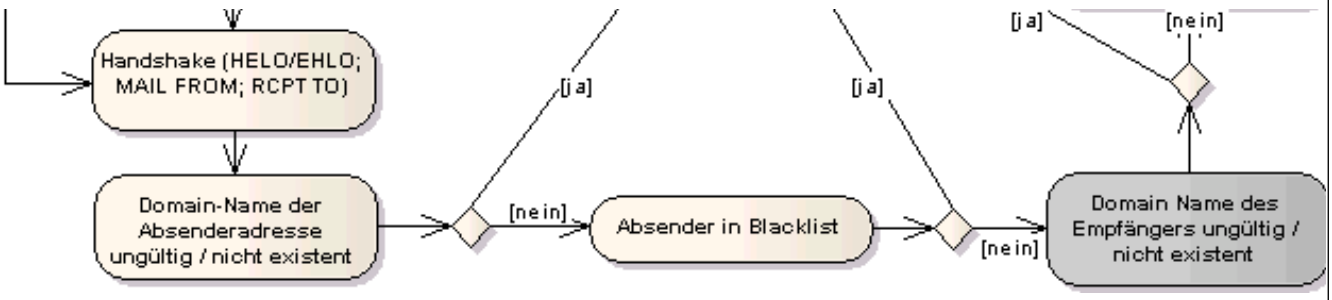
- Konsistenzprüfung bezüglich DNS-Konfiguration
- 3 Stufiges Verfahren:
  1. Existiert zur aufrufenden IP-Adresse zugehörige Name(n) (PTR Record im DNS)
  2. Gibt es zu jedem Namen eine zugehörige IP-Adresse (A Record im DNS)
  3. Stimmen aufrufende IP-Adresse und IP-Adresse aus dem A Record überein
- Viele Provider wenden nur 1. an
- Auch für diesen Check ist wieder eine Whitelist erforderlich

SPAM Maßnahmen Phase I: Ablaufdiagramm

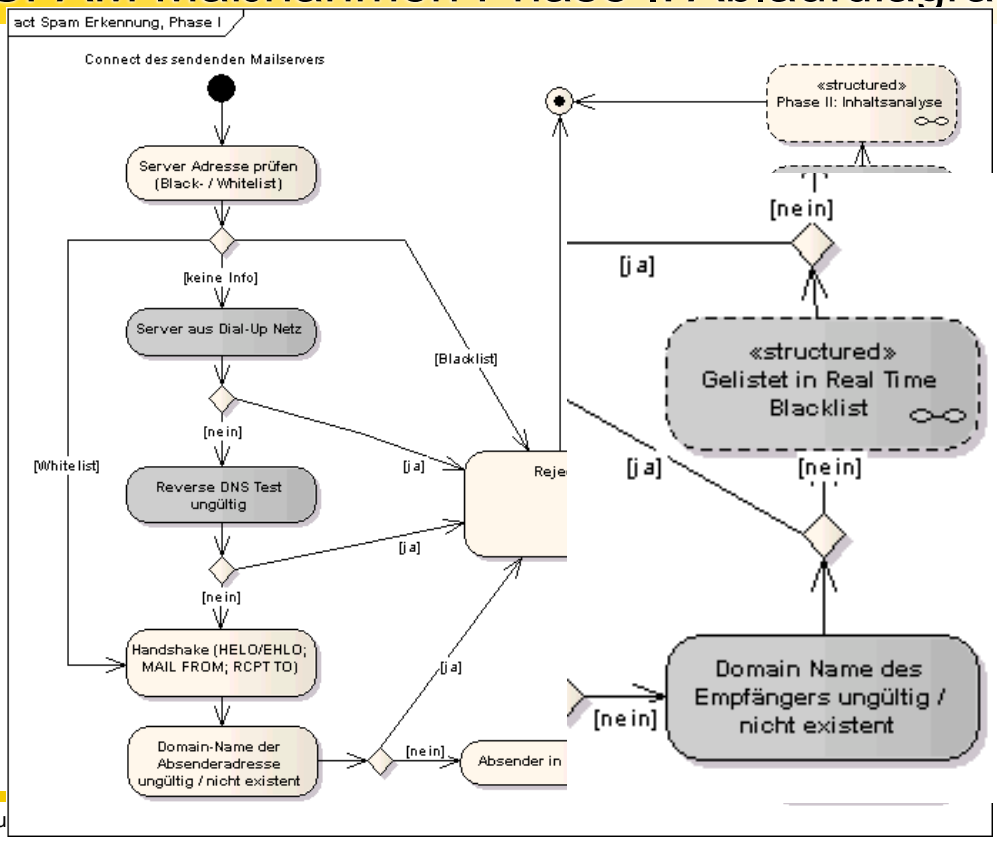


SPAM Maßnahmen Phase I: Ablaufdiagramm

- Erst jetzt wird Handshake durchgeführt (HELO/EHLO)
- Test auf Gültigkeit/Existenz des Domain-Namens aus Handshake
- Absender in Blacklist (MAIL FROM:)
- Test auf Gültigkeit/Existenz der Empfänger Domain (RCPT TO:)



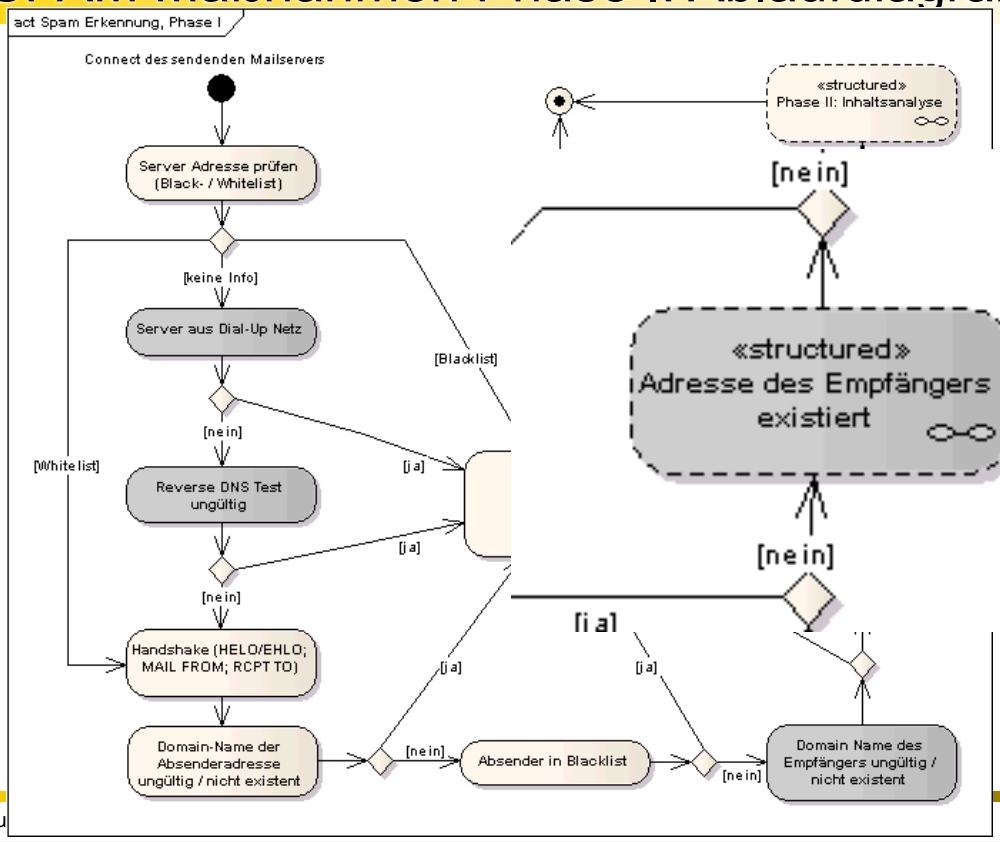
SPAM Maßnahmen Phase I: Ablaufdiagramm



Realtime Blacklisting

- Bekannte Spammer, bzw. deren IP-Adressen, werden in spezieller DNS-Zone gespeichert
- Pro Mail: Reverse DNS-Lookup in dieser Zone nach IP des Absenders
- Bei (spezieller) Antwort:
  - Absender ist gelistet
  - D.h. Spammer
- Bsp.: Mail von mailout.lrz-muenchen.de (129.187.254.112)
  - dig, host oder nslookup 112.254.187.129.pbl.spamhaus.org
    keine Antwort
- Bsp.: Mail von 217.227.25.81 (xxxxxxx.dip.t-dialin.net)
  - dig, host oder nslookup auf 81.25.227.217.pbl.spamhaus.org
    Antwort: Address: 127.0.0.11

SPAM Maßnahmen Phase I: Ablaufdiagramm



Empfängeradresse existiert

- Früher wurden alle Mails angenommen
  - Relays konnten nicht prüfen ob Adresse gültig; diese Info ist nur bei Endsystemen (MTA) der Institute bekannt
  - Problem: evtl. Backscatter Spam bei nicht existenter Adresse
  - LRZ könnte auf Blacklist landen
- Heute: Adressprüfung
- Benutzerverwaltung basiert auf LDAP
- Mailadressen über LDAP im MWN abfragbar
- Falls LDAP nicht unterstützt:
  - SMTP Callout (Rückfrage beim Mail-Server der Empfänger Domain)
  - Teuer; deshalb nur Ausnahmefall

Greylisting

- Ursprüngliches Ziel: Last für Server Betreiber reduzieren
- Ausnutzung des „fire and forget“ Prinzips vieler Spammer
  - SPAM wird nur einmal verschickt
  - Mail Server der Mail nicht zustellen kann, versucht Zustellung mehrmals
- Idee: 1. Versuch der Zustellung wird abgelehnt
- Daten zur Erkennung einer „Mail-Relationship“:
  - IP Adresse des sendenden Mail-Servers
  - Absenderadresse
  - Senderadresse
- Realisierung: Blocking Time
  - Mail-Relation erst nach Ablauf der Blocking Time akzeptieren
  - danach jede weitere Sendung in der Relation sofort akzeptieren
  - Häufig verwendete Werte: 50 Sek. bis 5 Minuten
  - LRZ: anfangs 15 Minuten, heute 29 Minuten

Greylisting

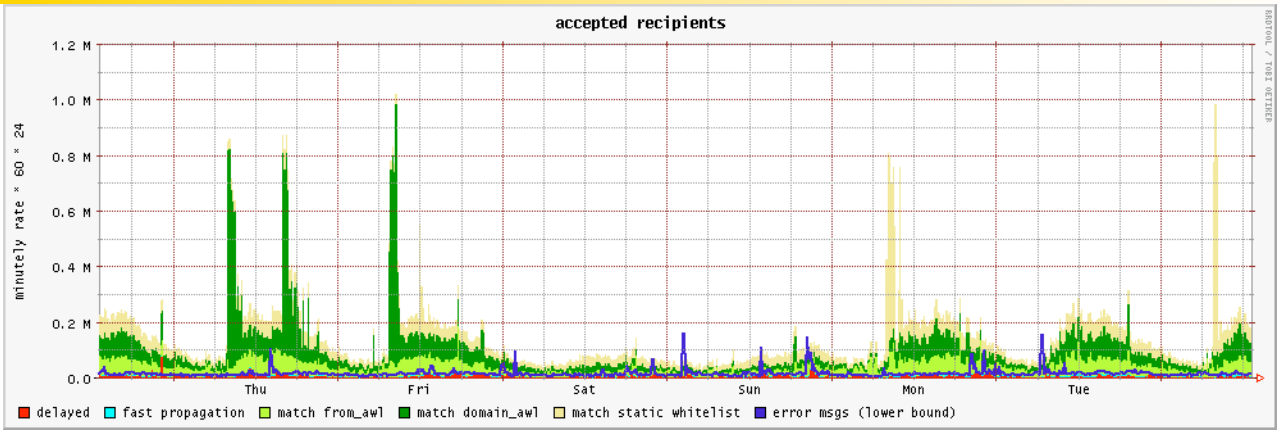
- Nachteil: Verzögerung der 1. Mail einer Relation (Blocking Time)
- Vorteil: In der Vergangenheit extrem Wirkungsvoll (> 90 %)

- Probleme:
  - Phisher mit systematischen Retry-Versuchen (seit September 2006)
  - 4 Versuche mit 5 Minuten Abstand (daher die neue Grenze mit 29 Min)
  - Erste Spammer mit „langen“ Retry-Versuchen

⇨ Greylisting könnte seine Wirksamkeit zu verlieren

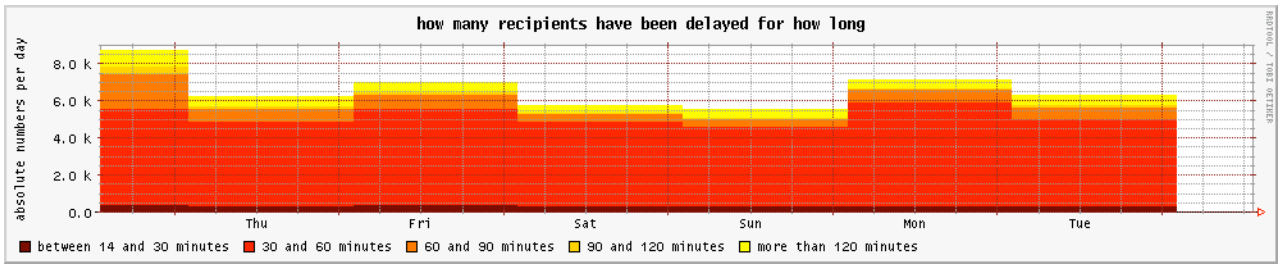
- Greylisting wurde durch die anderen (vorgestellten) Maßnahmen „nach hinten“ verschoben (vgl. Ablaufdiagramm)

Greylisting am LRZ: Akzeptierte Verbindungen



- Zeitraum: Mi. 18.10.06 bis Mittwoch 25.10.06
- awl = Automatic White List
  (LRZ verwendet IP Adresse des Servers und Absenderadresse; Empfängeradresse wird nicht berücksichtigt)
- from_awl: awl der Absenderadressen
- domain_awl: awl der Domainnamen
- error msgs: Fremde Mailserver antworten mit Fehlermeldungen

Greylisting am LRZ: Verzögerung



- Zeitraum: Mi. 18.10.06 bis Mittwoch 25.10.06
- Im Normalfall liegt die Verzögerung bei 30 Minuten
  (für die erste Verbindung – eines Servers - der noch nicht in der awl ist)

Phase II: Inhaltliche Analyse

- Erst nach Abschluss der Phase I werden die eigentlichen Mail-Daten (DATA) angenommen
- Damit werden zusätzliche Ressourcen benötigt

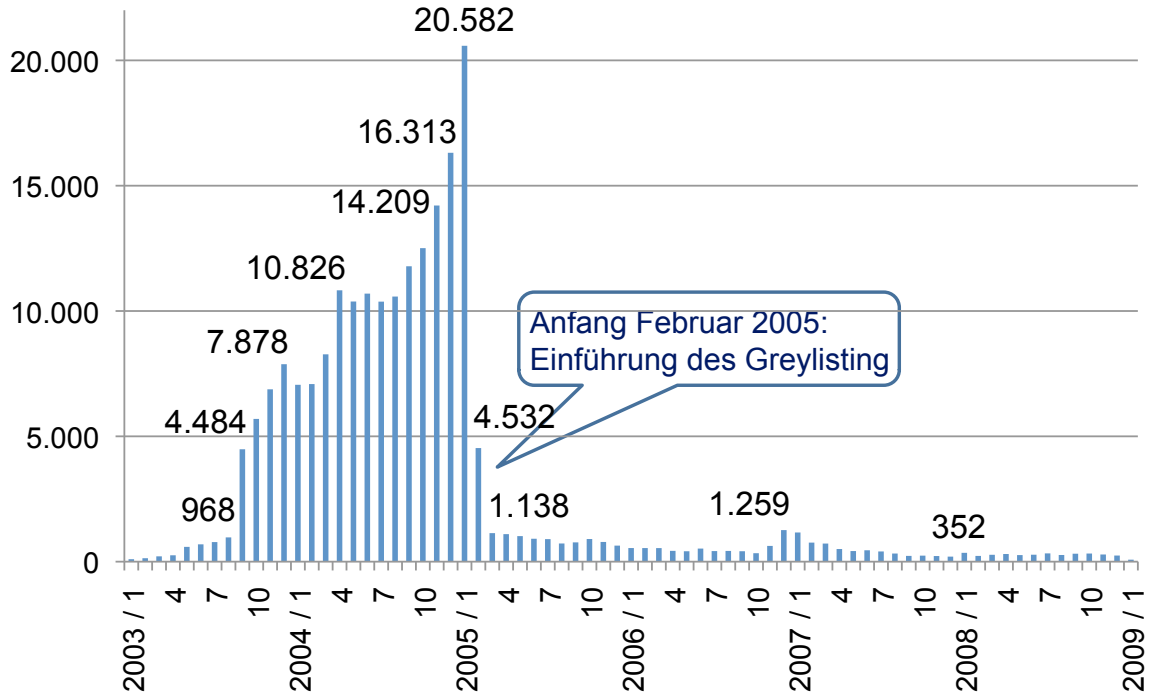
- Phase II: Inhaltliche Analyse
- Spam-Filter: Spam-Assassin markiert und ausgeliefert
- Viren-Filterung: Quarantäne mit Benachrichtigung

Inhalt (1)

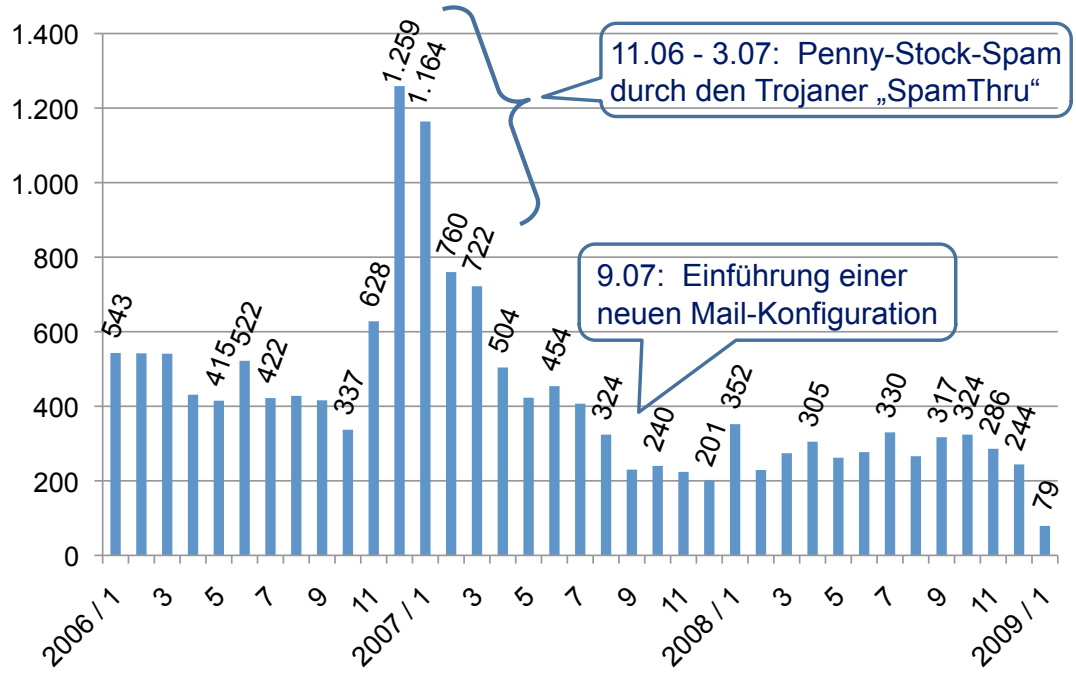
4. Abwehrmaßnahmen im Münchner Wissenschaftsnetz (MWN)
   - Mail aus dem MWN ins Internet
     - .....
   - Überblick über das Simple Mail Transfer Protokoll
   - Mail Infrastruktur im LRZ
   - Mail aus dem Internet ins MWN
     - Phase I: „(Spam) Mail zurückweisen“
     - Phase II: Inhaltliche Bewertung und Markierung
   - Betriebserfahrungen und Statistiken

- Dank an: E. Bötsch, M. Diehn, B. Schmidt, M. Storz

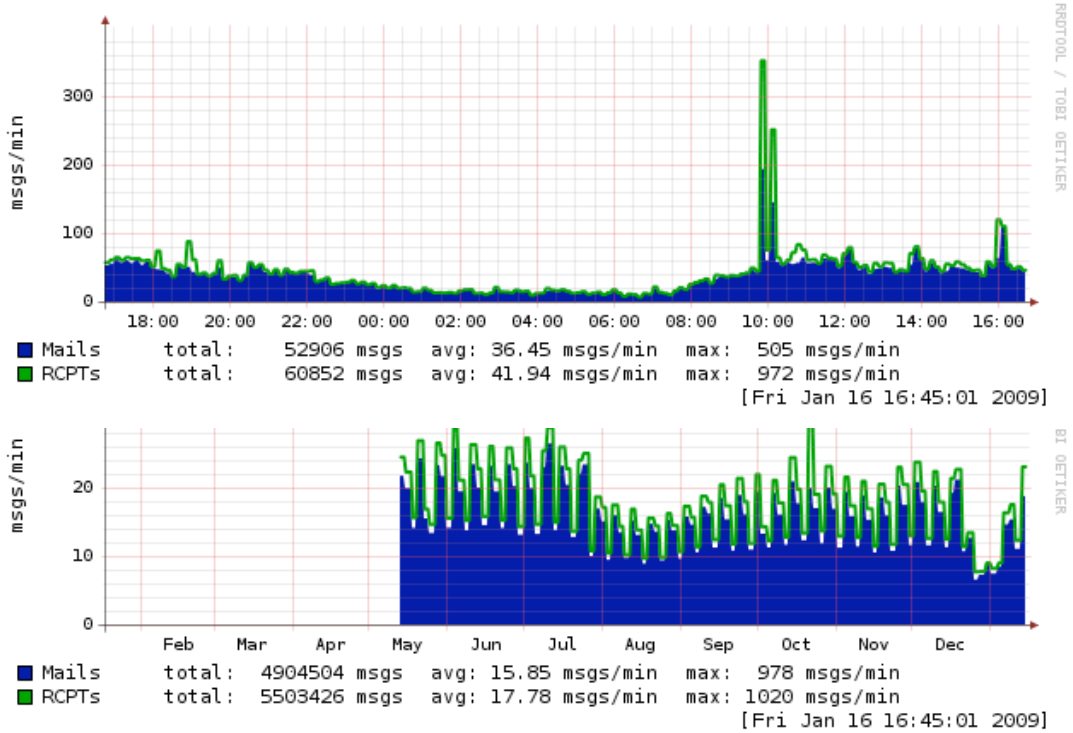
Persönliche Spam Statistik eines LRZ Mitarbeiters



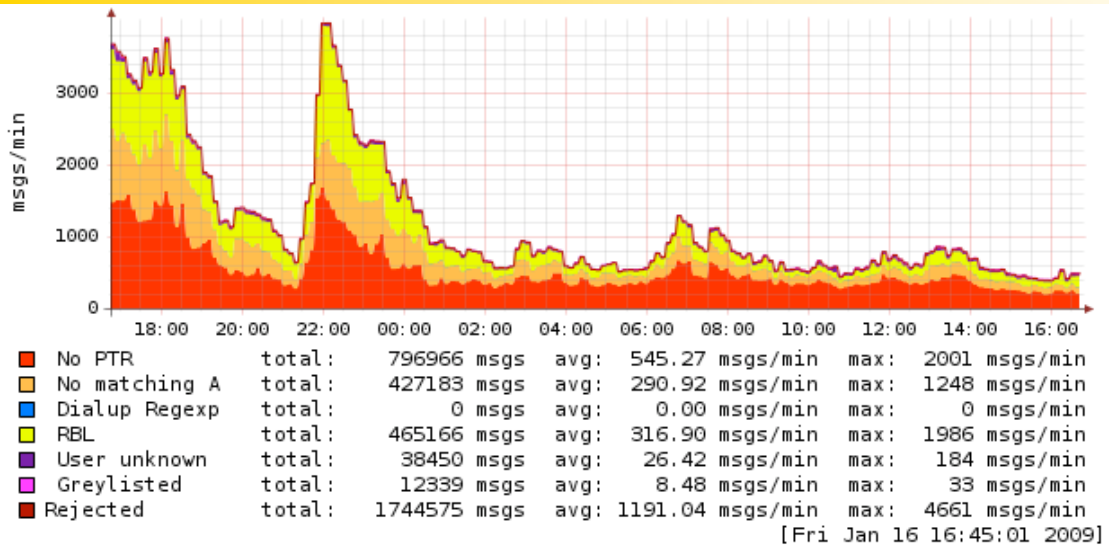
Persönliche Spam Statistik eines LRZ Mitarbeiters



Betriebserfahrungen: Maildurchsatz

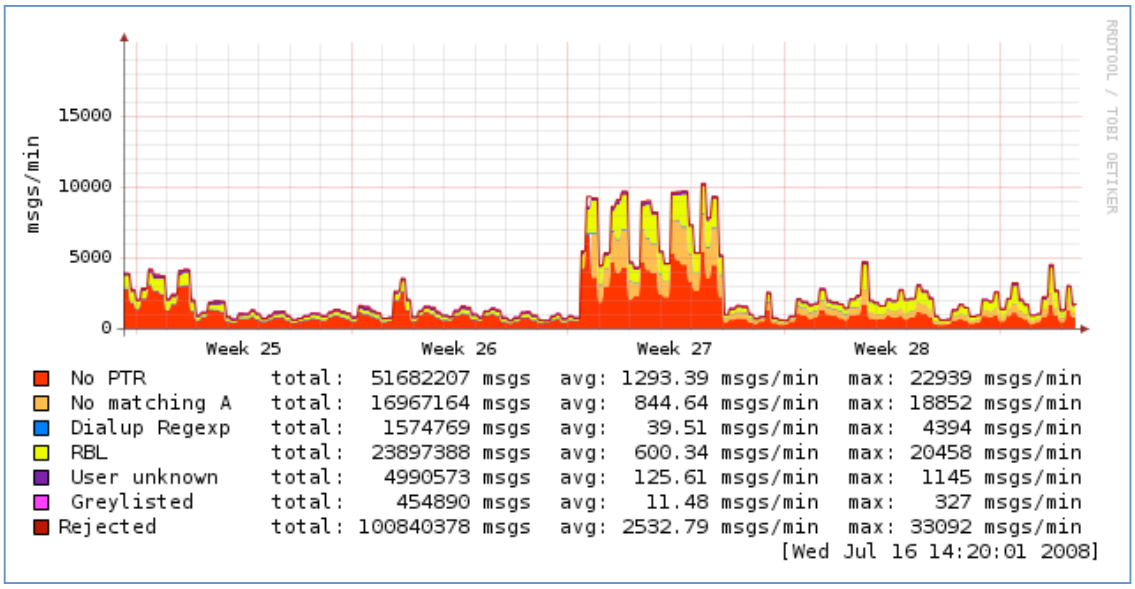


Betriebserfahrungen: Anti-Spam Mechanismen



- No PTR = IP Adresse zu Name
- No matching A = keine Adresse zum Namen
- Dialup Regexp = eigene Regeln für Dialup-Erkennung
- RBL = Real Time Black Lists

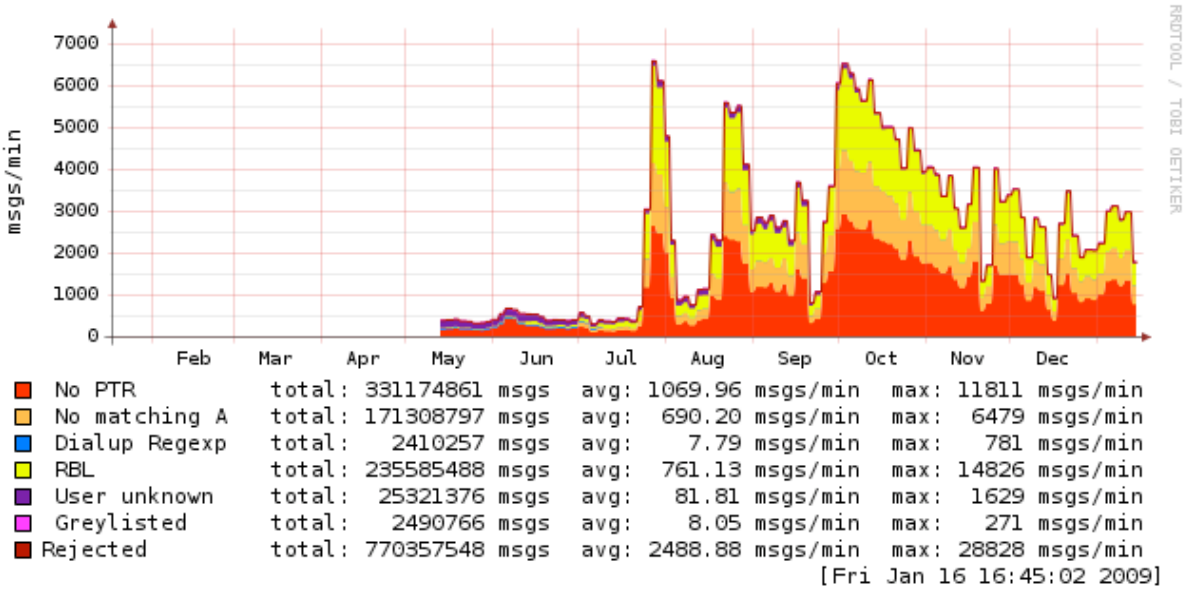
Betriebserfahrung: Spam-Wellen



- Mo. 30.06.08 12:00 bis Fr. 04.07.08 24:00
- Spitzenwert: 33.092 Mails / Min

Betriebserfahrungen: Spam Wellen

- Spam-Wellen



Betriebserfahrungen: Wirksamkeit der Mechanismen