# IT-Sicherheit

## - Sicherheit vernetzter Systeme -

## Kapitel 15: Anti-Spam-Maßnahmen

# Inhalt

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-) Mails zurückweisen“
     - Phase II: Inhaltliche Bewertung und Markierung

# 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. protokollkonformes Verhalten)
  - Statistische Analysen
  - Überprüfungen des sendenden Mailservers
  - Frühzeitige Verifizierung der Empfängeradressen
  - Keine (aufwendige!) inhaltliche Analyse (Mail-Body)
- Ziel: Ressourcenschonende 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

2010

| The 10 Worst Spam Origin Countries | | As at 04 January 2010 |
|---|---|---|
| Rank | Country | Number of Current Known Spam Issues |
| 1 | United States | 2388 |
| 2 | China | 552 |
| 3 | Russian Federation | 428 |
| 4 | United Kingdom | 290 |
| 5 | Spain | 240 |
| 6 | Argentina | 231 |
| 7 | Italy | 183 |
| 8 | Brazil | 183 |
| 9 | France | 179 |
| 10 | Germany | 177 |

Quelle:

www.spamhaus.org

2012

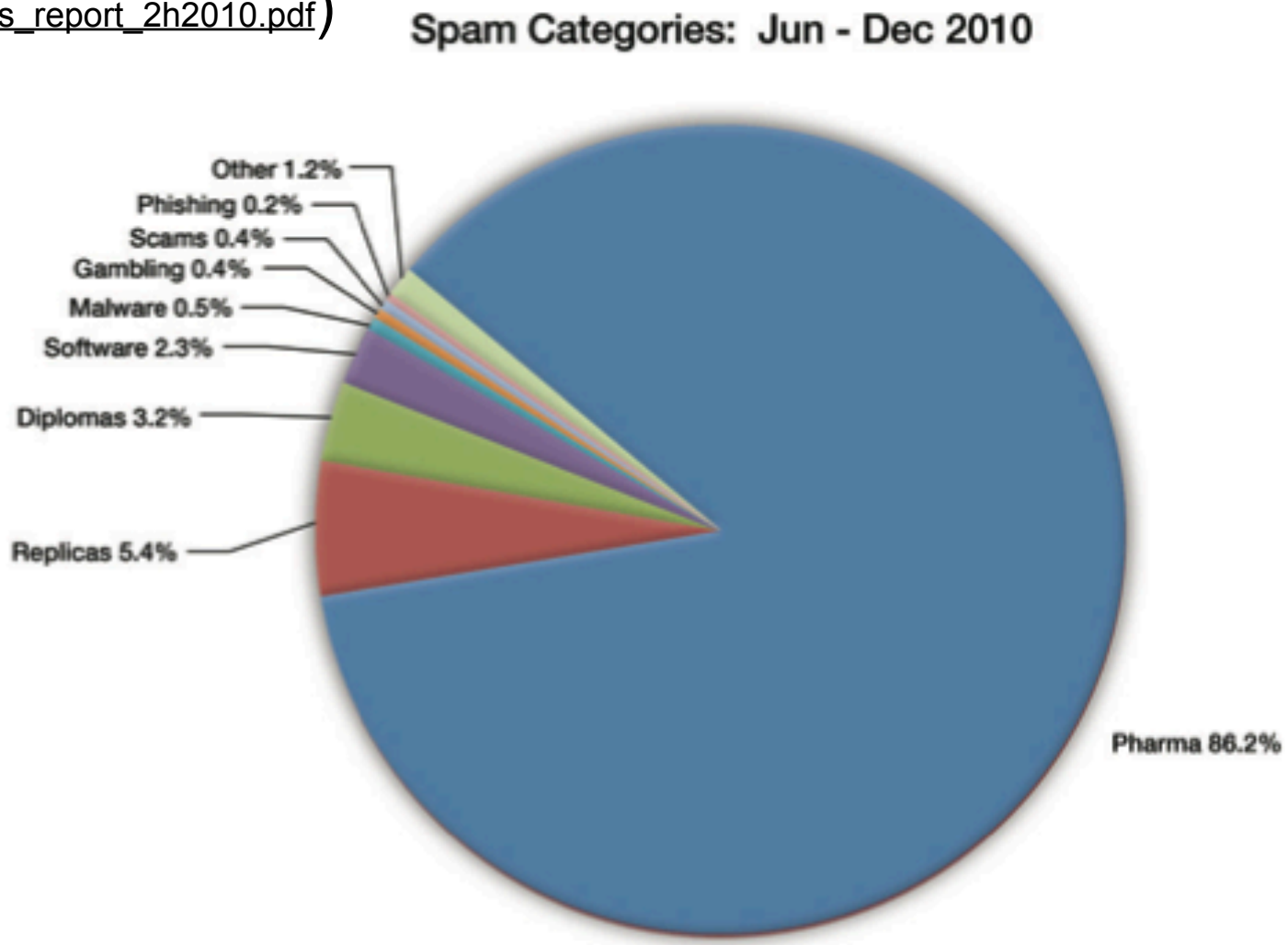
**The 10 Worst Spam Countries**

As at 27 January 2012 the world's worst Spam Haven countries for production and export of spam are:

| | | |
|---|---|---|
| 1 | United States | Number of Current Live Spam Issues: 2509 |
| 2 | China | Number of Current Live Spam Issues: 1183 |
| 3 | Russian Federation | Number of Current Live Spam Issues: 673 |
| 4 | United Kingdom | Number of Current Live Spam Issues: 486 |
| 5 | Germany | Number of Current Live Spam Issues: 276 |
| 6 | Brazil | Number of Current Live Spam Issues: 256 |
| 7 | Japan | Number of Current Live Spam Issues: 253 |
| 8 | Ukraine | Number of Current Live Spam Issues: 246 |
| 9 | Canada | Number of Current Live Spam Issues: 241 |
| 10 | Korea, Republic Of | Number of Current Live Spam Issues: 226 |

# Spam-Statistik: Inhaltliche Klassifikation

- Quelle: www.marshal.com (www.m86security.com/documents/pdfs/security_labs/m86_security_labs_report_2h2010.pdf)



# Top Spammer (www.spamhaus.org)

1

**Canadian Pharmacy** - **Ukraine**

A long time running pharmacy spam operation. They send tens of millions of spams per day using botnet techniques. Probably based in Eastern Europe, Ukraine/Russia. Host spammed web sites on botnets and on bulletproof Chinese web hosting.

2

**Rove Digital** - **Estonia**

Botnets, malware, spam, pharming, DDoS. Inhoster, Cernel, Esthost, Atrivo. What else needs to be said?

3

**Alex Blood / Alexander Mosh / AlekseyB / Alex Polyakov** - **Ukraine**

So many Alex & Alexey spamming! Alex Blood tied to Pilot Holding & bbasafehosting.com long ago, then Alex Polyakov posted he owned them. Massive botnet and child-porn spam ring, also pharma, mortgage, and more. May work with Kuvayev and Yambo.

4

**Vincent Chan / yoric.net** - **Hong Kong**

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. They use vast numbers of compromised computers -- for sending, hosting and proxy hijacking.

5

**Peter Severa / Peter Levashov** - **Russian Federation**

A spamming partner of Alan Ralsky and other spam gangs.

Stand: 01/2012

# Wichtigste Spam-Quellen

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

# Spam-Quellen: Bot-Netze / „Viren“

- Start 2003: Wurmfamilien wie Sobig bauen Botnet auf
- Frühe (Spam-) Botnetze:
  - Optimiert, um 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 von Mensch
  - Beispiel (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. 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-) Mails zurückweisen“
     - Phase II: Inhaltliche Bewertung und Markierung

# 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 Heterogenität 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 wie 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-Net-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 Netzverantwortliche

# 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
    - ➡ Secomat
  - 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 (vgl. folgende Folien)
    - Derzeit keine automatischen Reaktionen
    - Alarmierung, (menschliche) Überprüfung und Reaktion / Eskalation
    - 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 Mailserver
  2. Legitimer Rechner generiert viele Mails (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 infizierter Commodity-PC (= Rechner der „Aldi-Klasse“)?
  - bis zu 3.500 Mails / 5 Min.
  - bis zu 18.000 Mails / 1 h

# Eigene Spamquellen: Gegenmaßnahmen

- Nutzer-Authentifizierung beim Mail-Versand
  - Nutzer muss sich vor Mail-Versand beim Server authentisieren
    - z.B. mit Benutzername und Passwort
  - RFC 2476 („Message Submission“; 1998)
  - 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 Resource 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 mit SPF

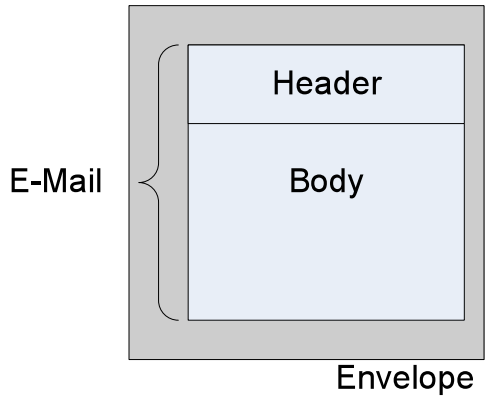
- Spammer verwenden Domains mit korrekter SPF-Konfiguration
  - „Einwegdomains“
  - Der größte Teil der Domains mit SPF-Konfiguration gehört Spammern
- Bot-Net-Client aus korrekt konfigurierter Domain versendet Spam
- Zum Teil schlechte Usability:
  - Weiterleitung von E-Mails mit Beibehalten der ursprünglichen Absenderadresse erfordert Whitelists
  - Bei mehreren E-Mail-Konten Nutzung verschiedener Mailserver zum Mailversand notwendig, aber aus Sicherheitsgründen oft eingeschränkt

# Inhalt

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

# Aufbau von E-Mails

- Header:
  Meta-Informationen wie Absender, Empfänger, ...
- Body:
  Eigentlicher Inhalt, bestehend aus „Body Parts“
- Beim Versand:




```
Message-Id: <87488y4@1nannyplace.com>
Date: Thu,  5 Aug 2004 15:49:10 -0400
Subject: Cheap software - Save up to 60%
From: "Maricela" <wtdxc@1nannyplace.com>
To: Wolfgang.Hommel@lrz-muenchen.de

Hello,                          Leerzeile!

We offer all the software you can imagine!
     Best prices on the net!

Examples:

$60 Ahead NERO 6.3 POWERPACK
$140 Adobe Premiere Pro 7.0
$40 Quicken 2004 Premier Home & Biz
$60 Ahead NERO 6.3 POWERPACK
$20 McAFEE Personal Firewall Plus 2004
```

# Verwendung von MIME in E-Mails

Multipurpose Internet Mail Extension

```
Date: Wed, 28 Jun 2006 15:35:16 +0200
MIME-Version: 1.0
To: Wolfgang Hommel <Wolfgang.Hommel@lrz-muenchen.de>
Subject: Word-Dokument
Content-Type: multipart/mixed;
 boundary="------------030407050703000207030304"

This is a multi-part message in MIME format.
--------------030407050703000207030304
Content-Type: text/plain; charset=ISO-8859-15;
format=flowed
Content-Transfer-Encoding: 8bit


Anbei die gewünschte Word-Datei…

--------------030407050703000207030304
Content-Type: application/msword;
 name="blabla.doc"
Content-Transfer-Encoding: base64
Content-Disposition: inline;
 filename="blabla.doc"

0M8R4KGxGuEAAAAAAAAAAAAAAAAAAAAAPgADAP 7/
CQAGAAAAAAAAAAAAAAABAAAAKwAAAAAA
AAAAEAAALQAAAAEAAAD+////
AAAAACoAAAD//////////////////////////////////
…..
AAAAAAAA
--------------030407050703000207030304--
```

Base64-Kodierung für Binärdaten

MIME-Parts werden durch Boundaries voneinander getrennt

# 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

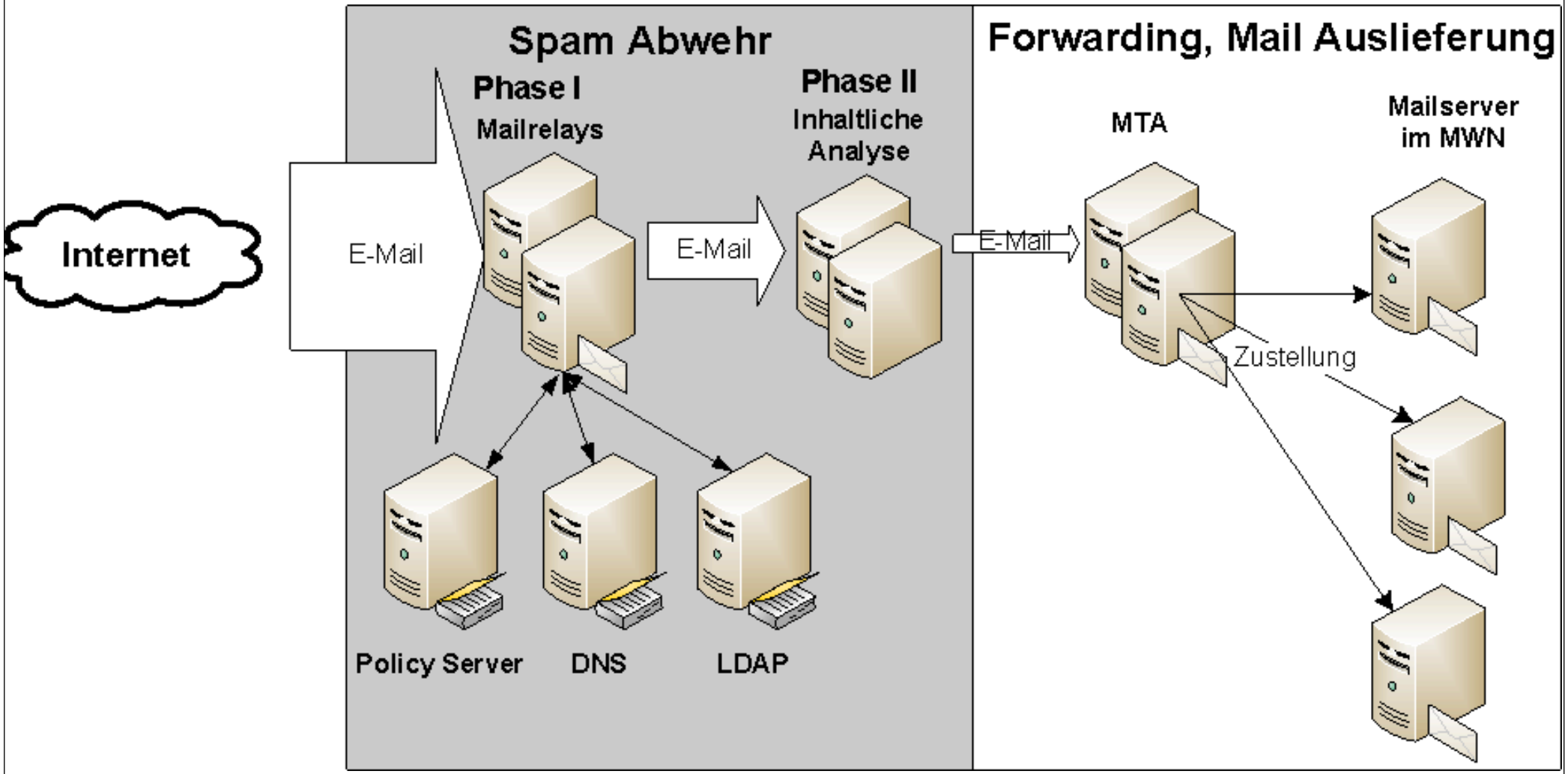
- Protokollablauf Fortsetzung

| Client | Server | Erklärung |
|---|---|---|
| FROM: fake@fake.de<br>TO: <gast@gast.de><br>Subject: Testmail<br><br>*<Leerzeile>*<br><br>Und hier kommen dann die Daten.<br>;-)<br>. | | Client gibt Maildaten an;<br>Hinweis:<br>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 integritätsgeschützt
  - Adressen lassen sich leicht fälschen
- Vertraulichkeit des E-Mail-Inhalts ist nicht sichergestellt
- Verschlüsselung des E-Mail-Body schützt nicht vor Verkehrsflussanalyse

# Mail-Infrastruktur im MWN




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

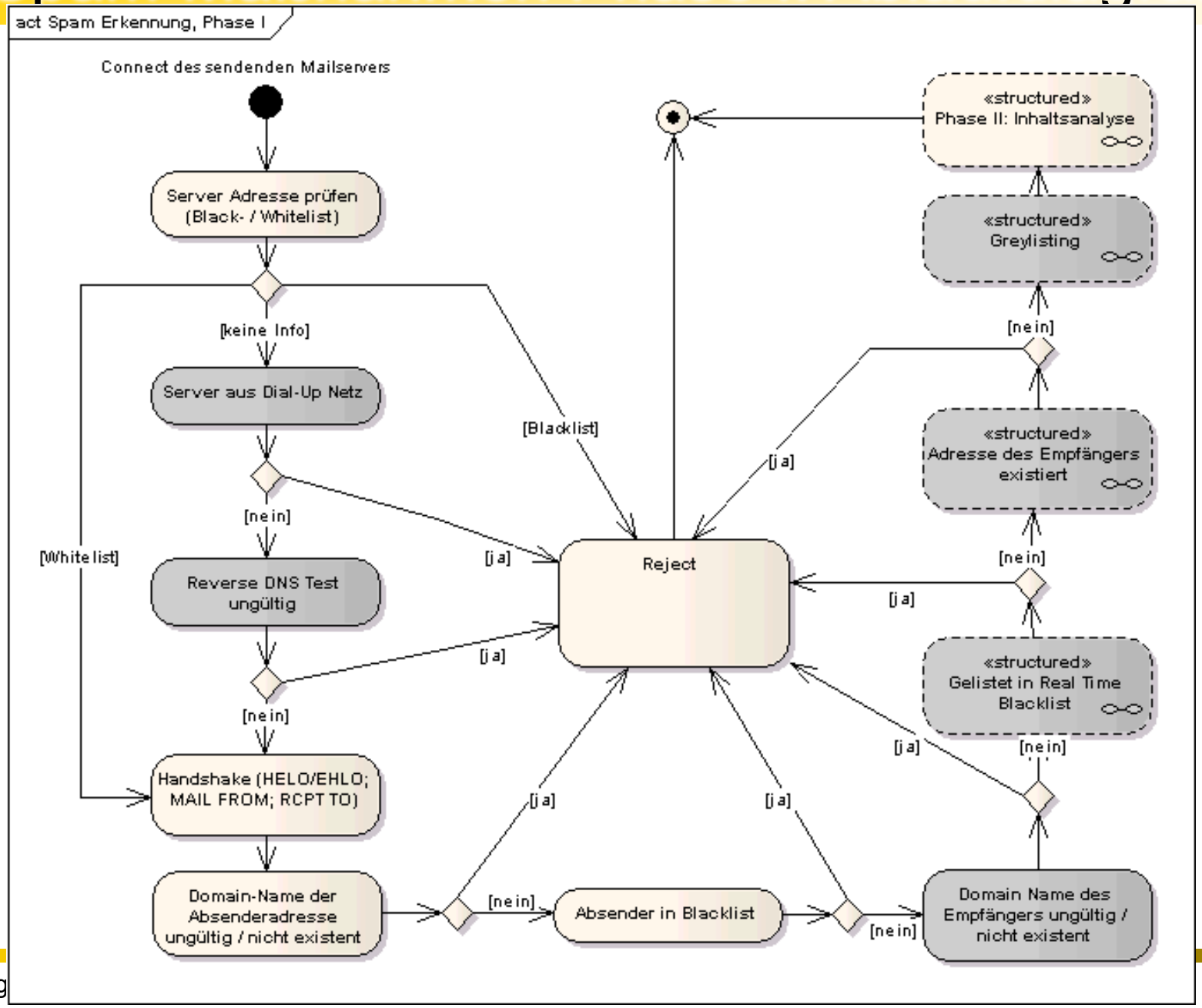
# Spam Abwehr Grundlagen

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

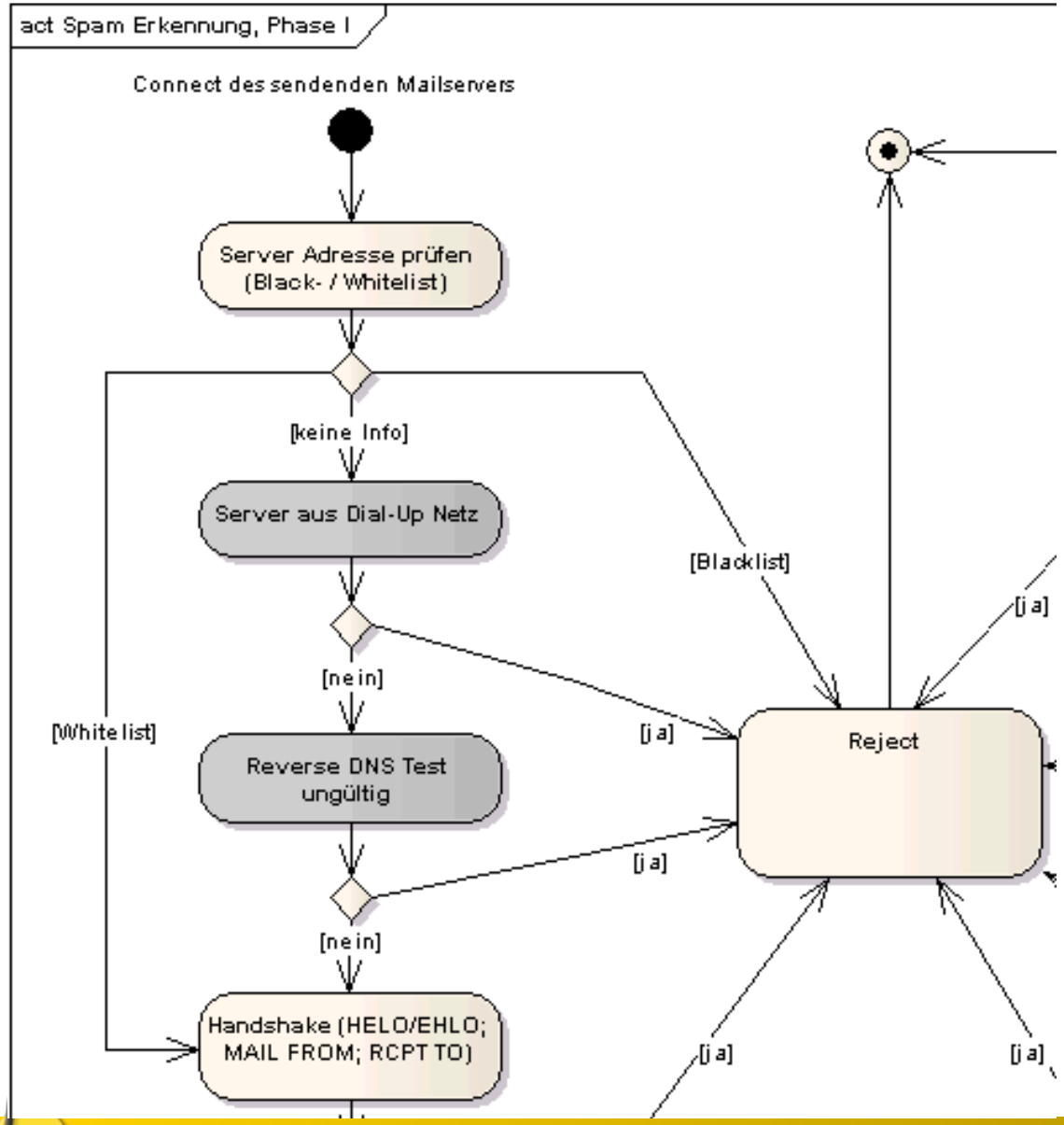
# Spam-Abwehr: Phase I

- 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 Envelope
- Formale Kriterien finden, die Spammer (z.B. Bot) von regulärem MTA unterscheiden; dann
  - Mail sehr früh und ohne weiteren Ressourceneinsatz ablehnen
  - Regulärer MTA
    - korrekt implementiert
    - korrekt konfiguriert
    - gut administriert

# Spam-Maßnahmen Phase I: Ablaufdiagramm



# Spam-Maßnahmen Phase I: Ablaufdiagramm

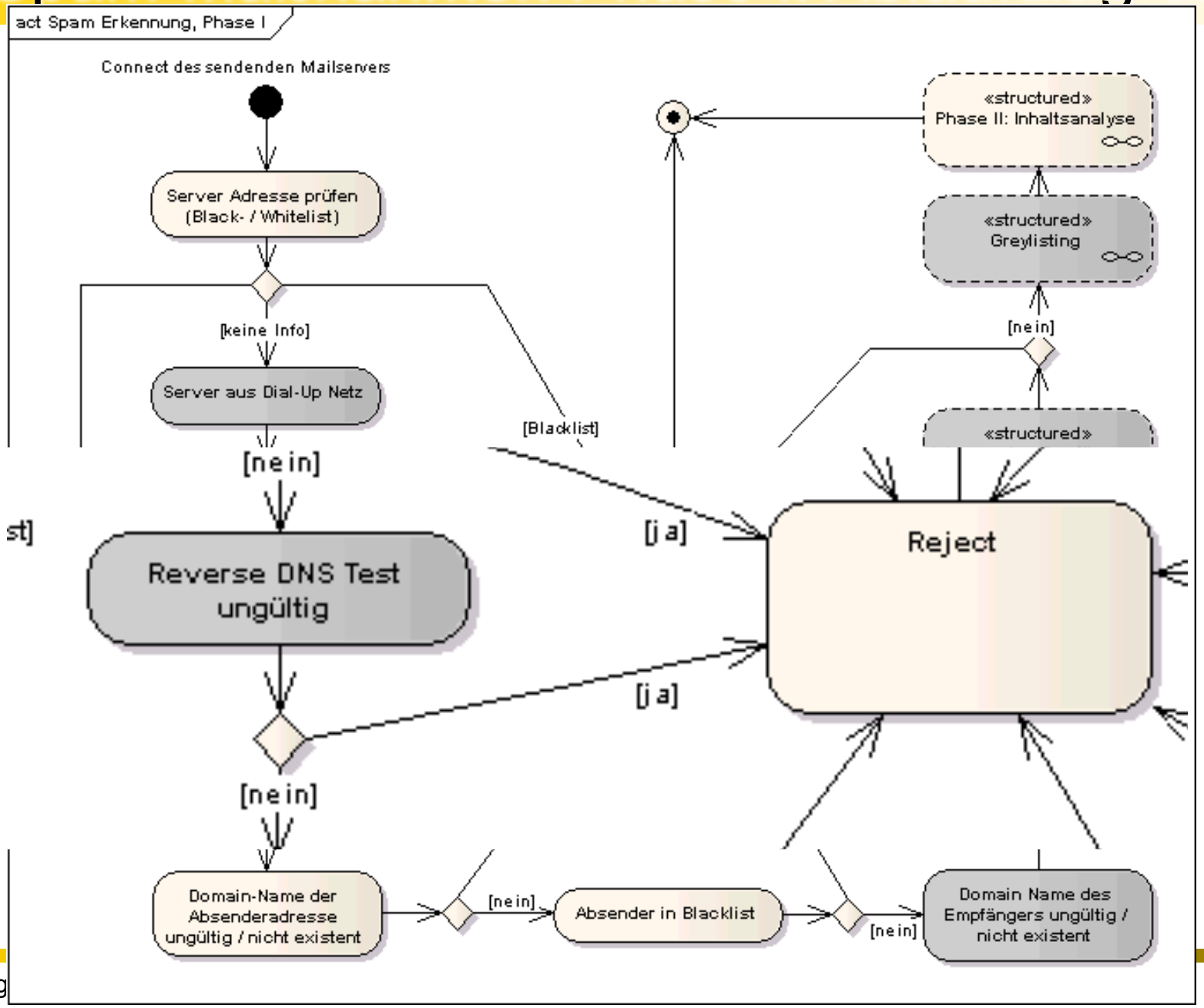



- Black-/Whitelist
- Blacklist
  - Adressen und Domainnamen bekannter Spammer
  - Vom LRZ selbst erstellt und gepflegt
  - ➡ Mail wird abgelehnt
- Whitelist
  - Ausnahmeliste von Servern, die als valide Mailquellen betrachtet werden
  - Bsp.: Prof. erhält Mail aus bekannter Spam-Domain
  - ➡ Handshake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

# Phase I: Server aus Dial-Up Netzen?

- Bots finden größte Verbreitung auf PCs von Heimanwendern
  - Leider oft schlecht administriert; keine Sicherheitsadministration
  - ISPs führen oft keine Missbrauchserkennung durch
  - Mit recht hoher Bandbreite (DSL/Kabel) 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

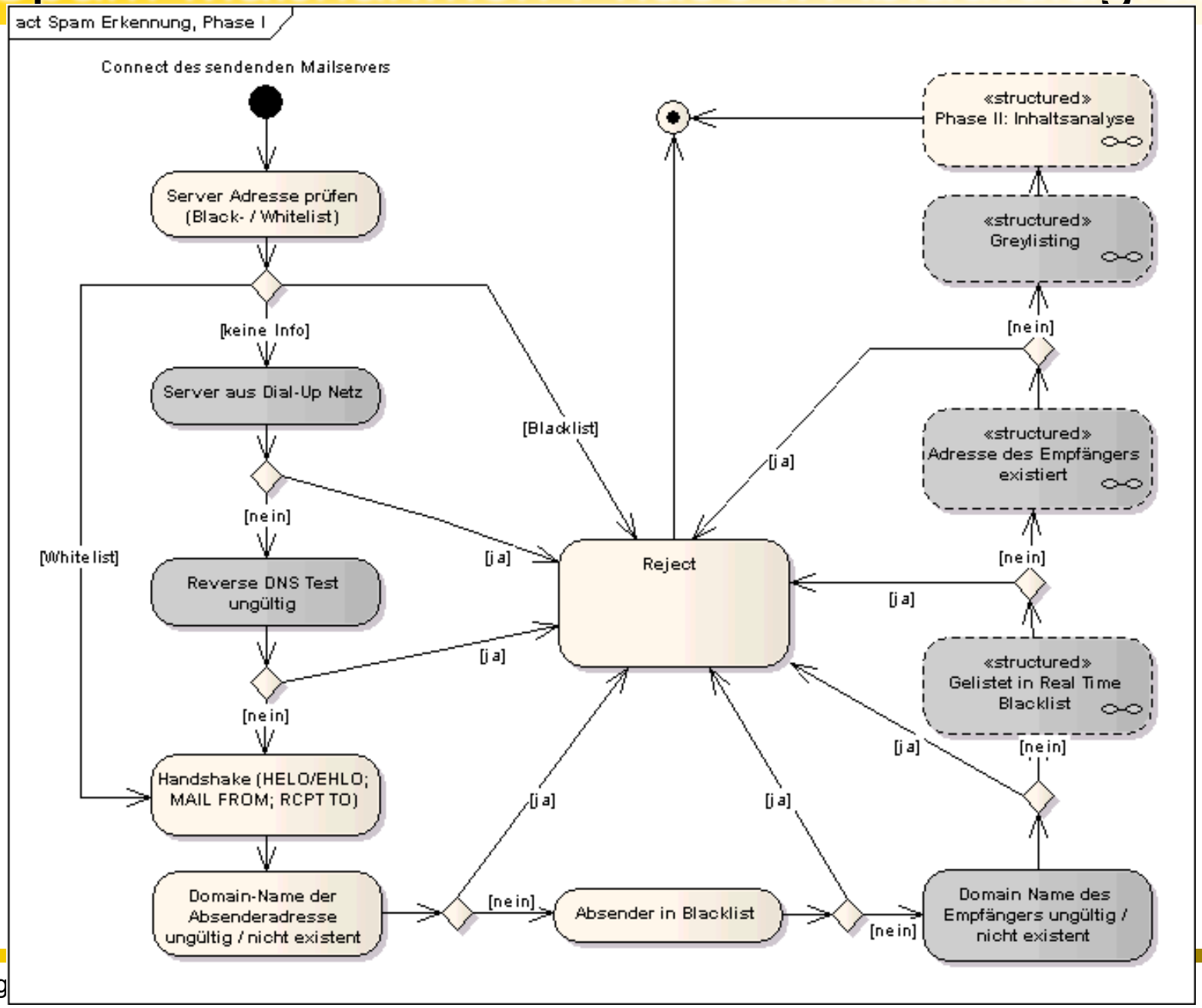
# Spam-Maßnahmen Phase I: Ablaufdiagramm



# Reverse DNS-Test

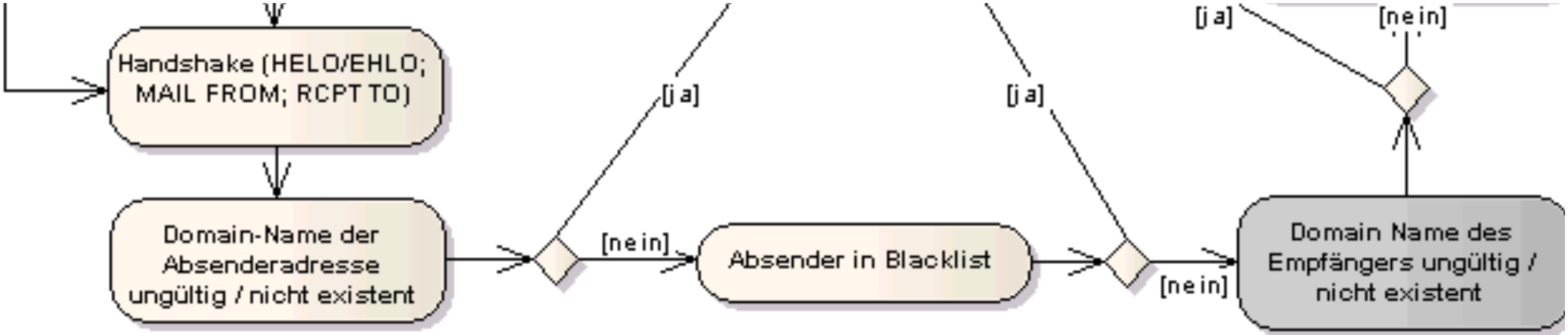
- Konsistenzprüfung bezüglich DNS-Konfiguration
- Dreistufiges Verfahren:
  1. Existiert zur aufrufenden IP-Adresse der zugehörige Name? (PTR Record im DNS)
  2. Gibt es zu jedem Namen eine zugehörige IP-Adresse? (A Record im DNS)
  3. Stimmen aufrufende IP-Adresse und IP-Adresse aus dem A Record überein?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

# Spam-Maßnahmen Phase I: Ablaufdiagramm

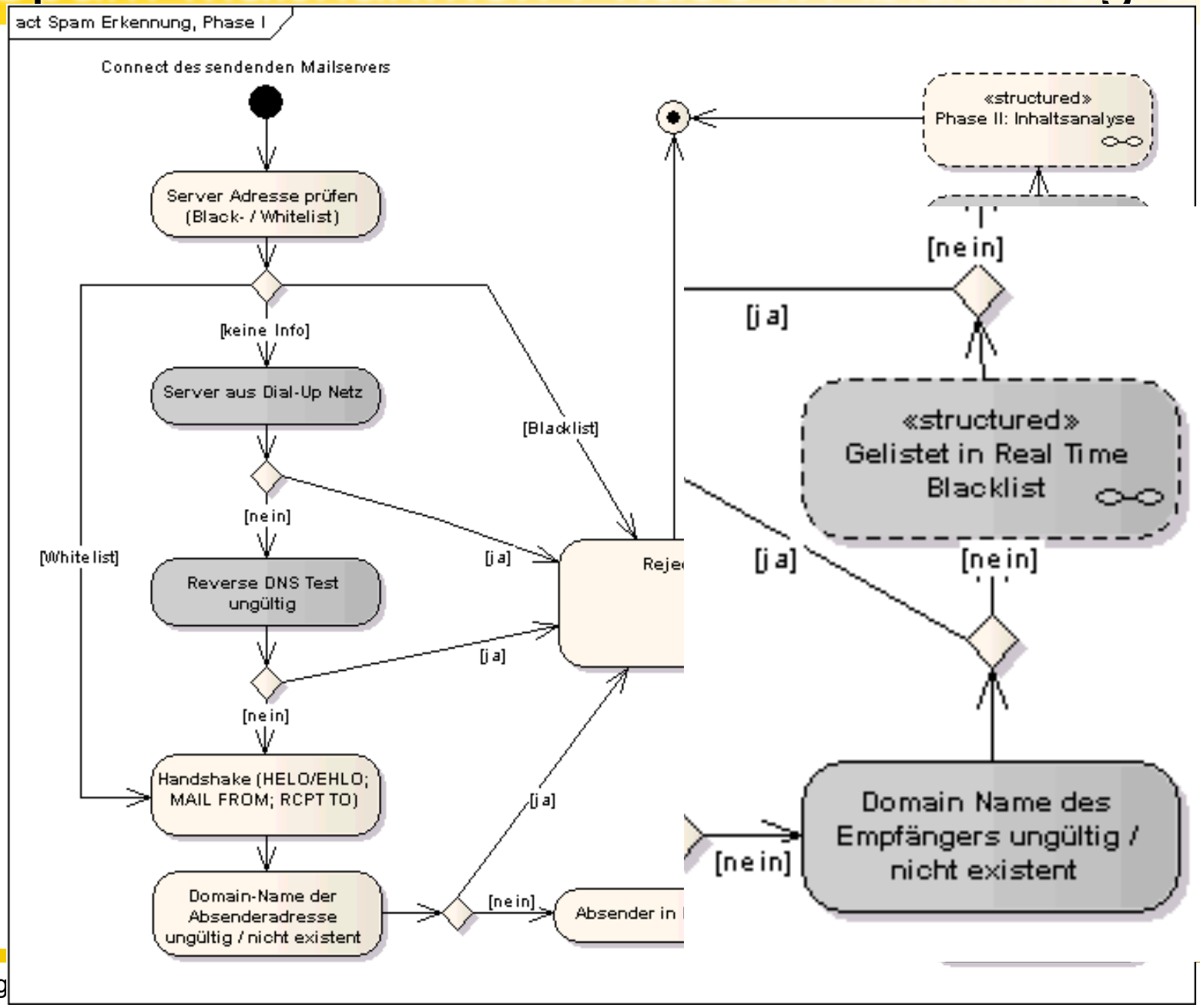


# Spam-Maßnahmen Phase I: Ablaufdiagramm

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



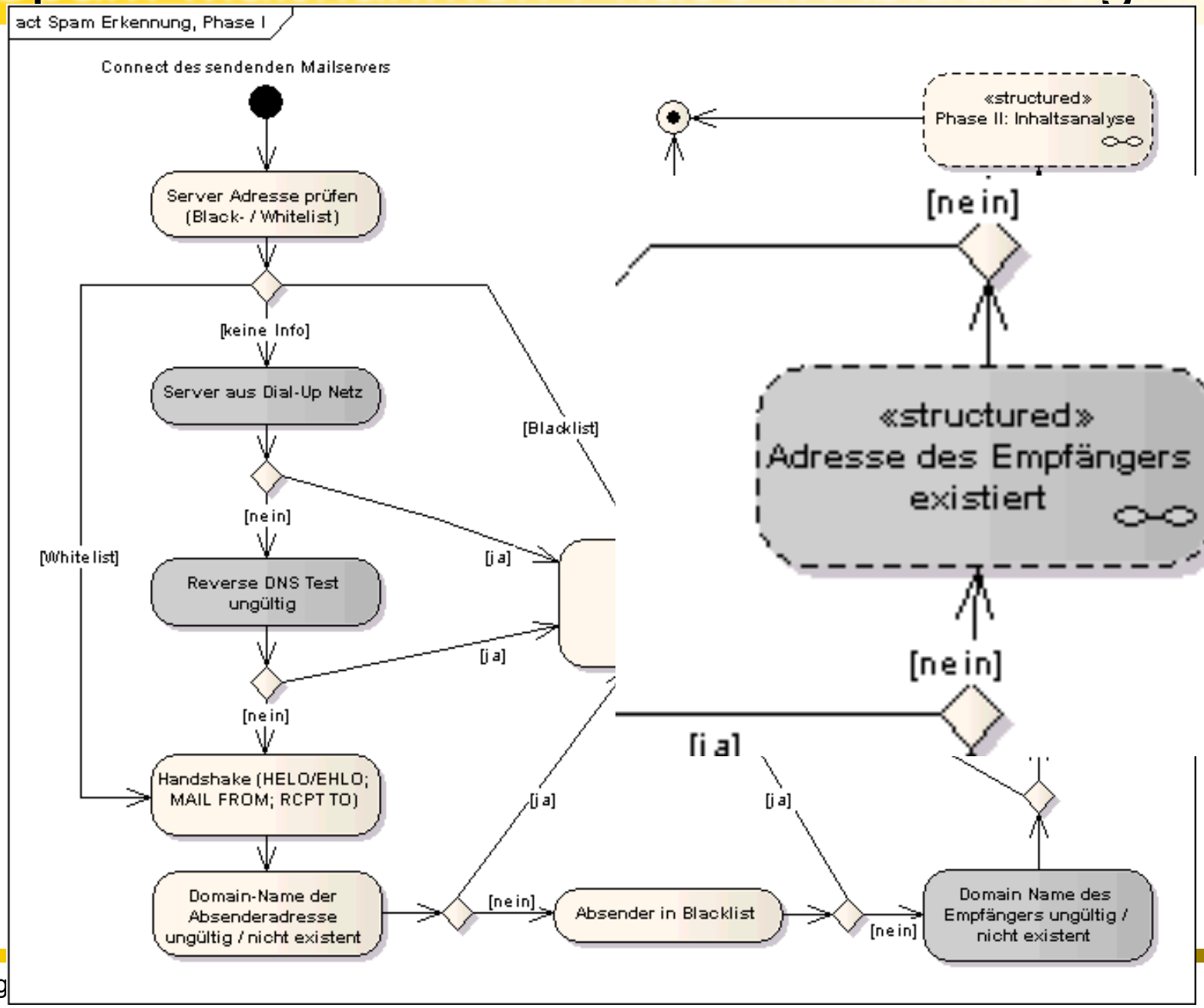
# Spam-Maßnahmen Phase I: Ablaufdiagramm



# Realtime Blacklisting (RTB)

- Bekannte Spammer bzw. deren IP-Adressen werden in spezieller DNS-Zone gespeichert
- Für jede 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



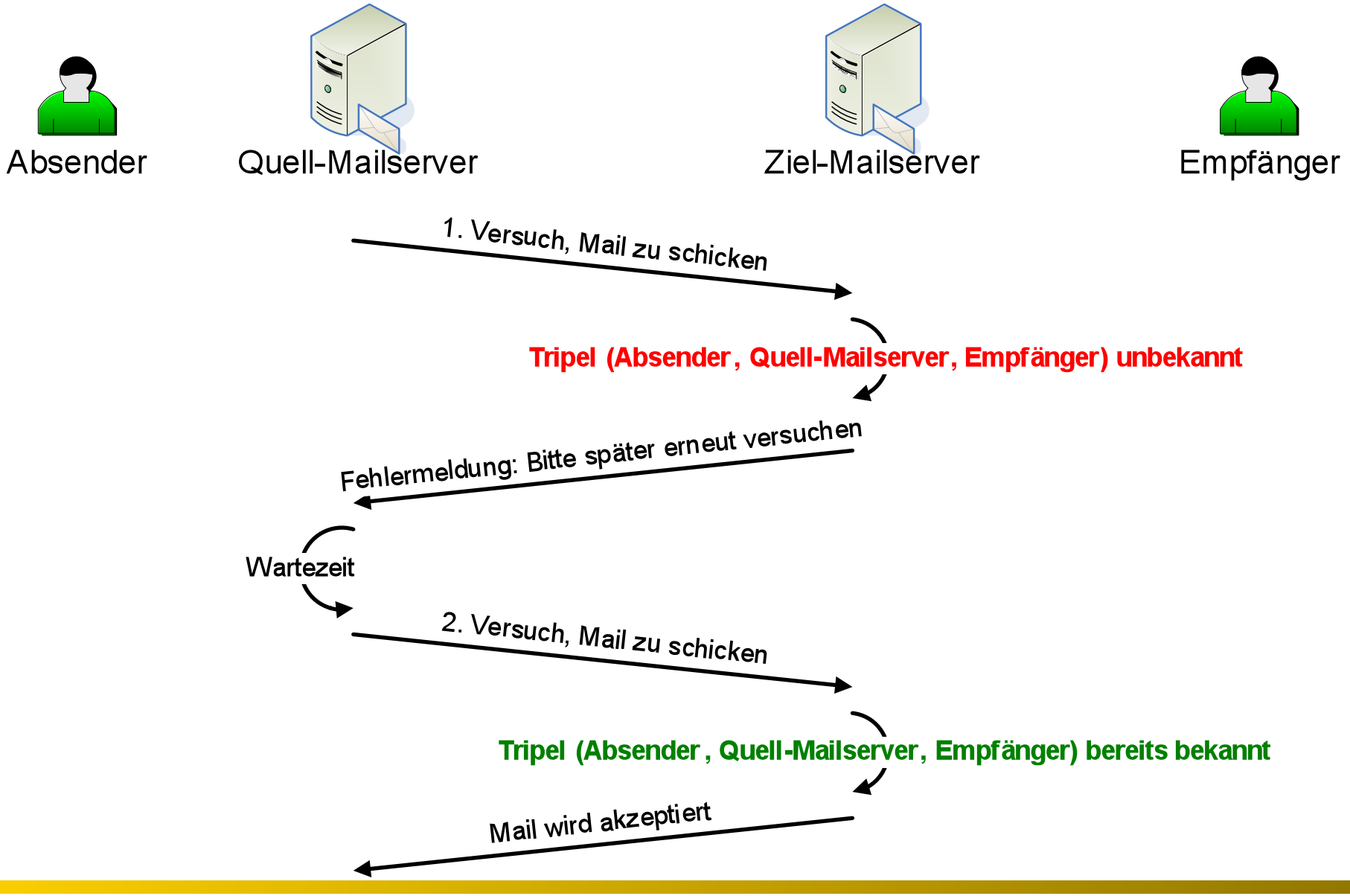
# Test: Empfängeradresse existiert?

- 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
  - Mailserver, 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
  - Empfängeradresse
- 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 - Ablaufdiagramm



# Greylisting

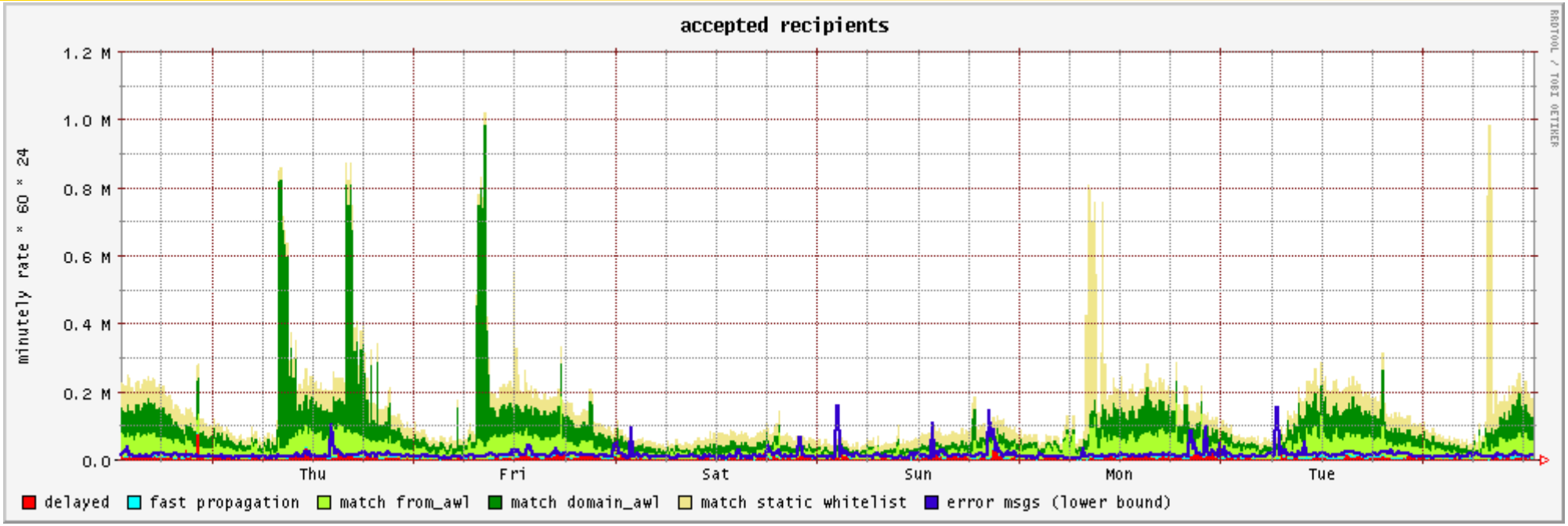
- Nachteil: Verzögerung der 1. Mail einer Relation (Blocking Time)
- Vorteil: In der Vergangenheit extrem wirkungsvoll (> 90 %)

- 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 wird (früher oder später) seine Wirksamkeit verlieren

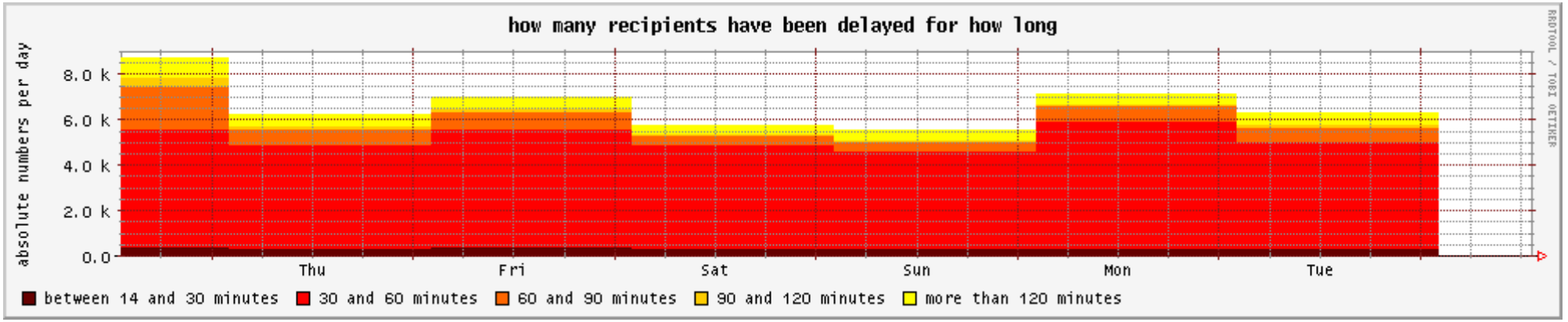
- Greylisting wurde durch die anderen (vorgestellten) Maßnahmen „nach hinten“ verschoben (vgl. Ablaufdiagramm)

# 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

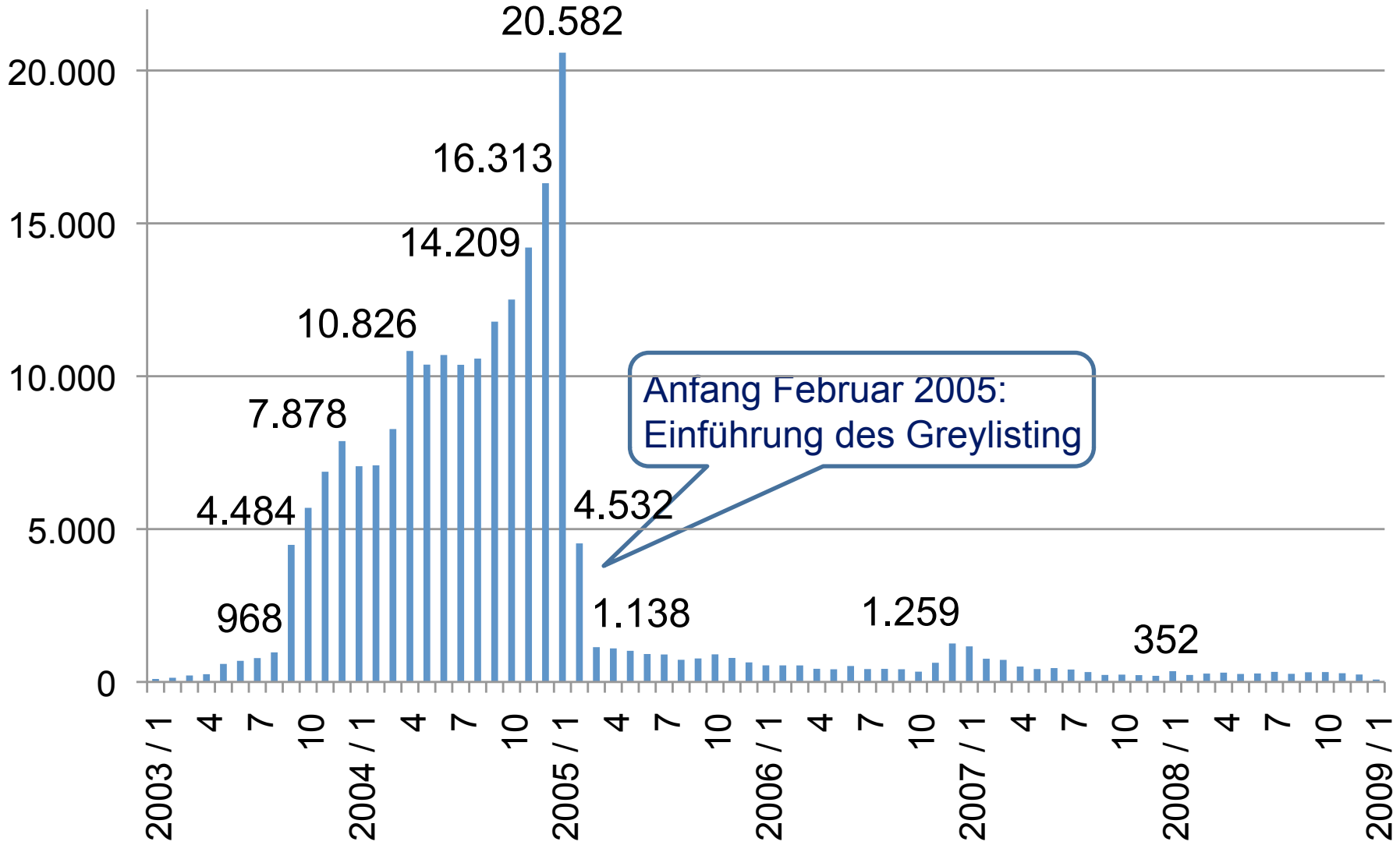
- Erst nach Abschluss der Phase I werden die eigentlichen Mail-Daten (DATA) angenommen
- Damit werden zusätzliche Ressourcen benötigt

- Phase II: Inhaltliche Analyse
- Spam-Filter: Spam-Assassin markiert potentielle Spam-Mails
- Viren-Filterung: Quarantäne mit Benachrichtigung

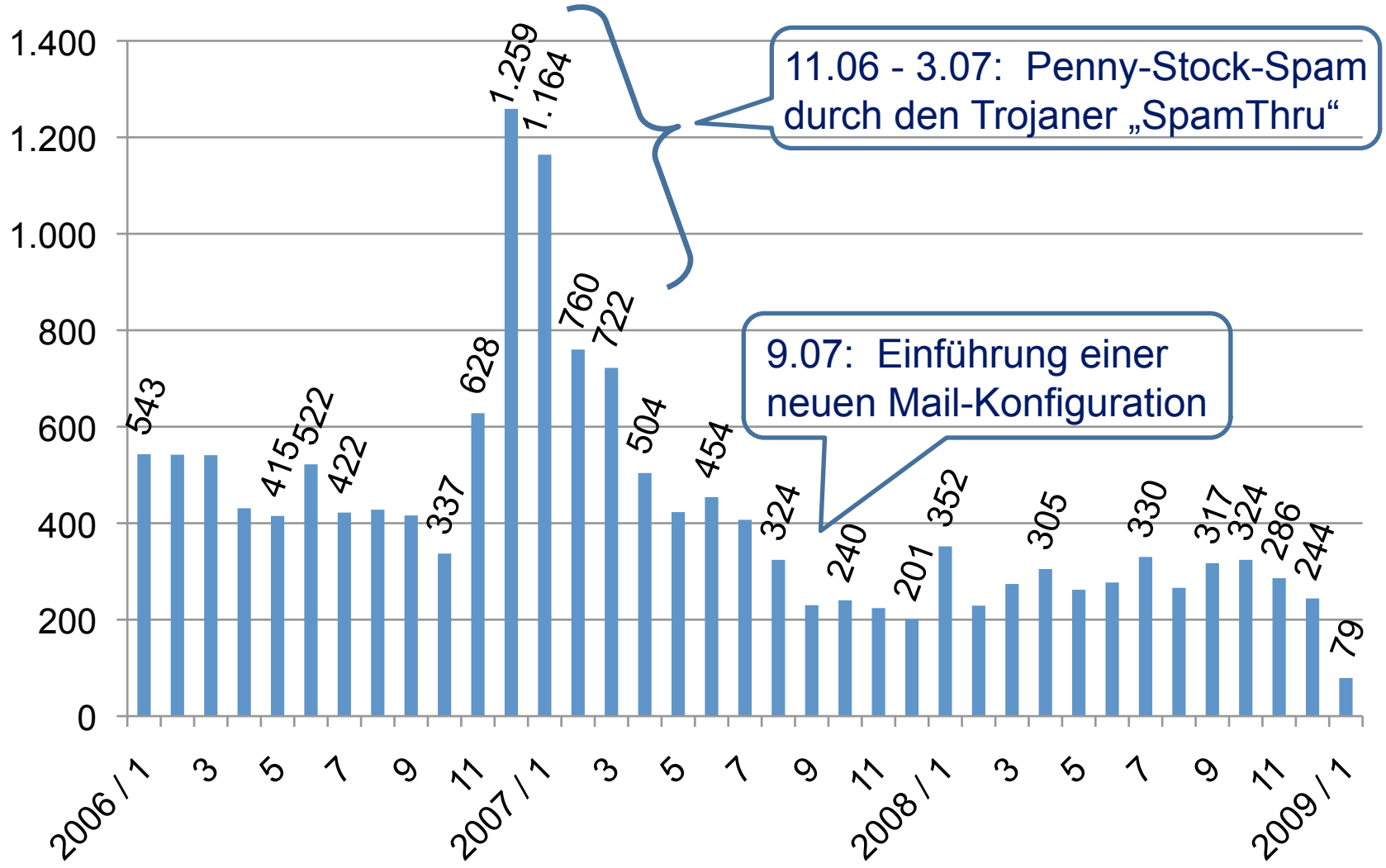
# Inhalt (1)

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

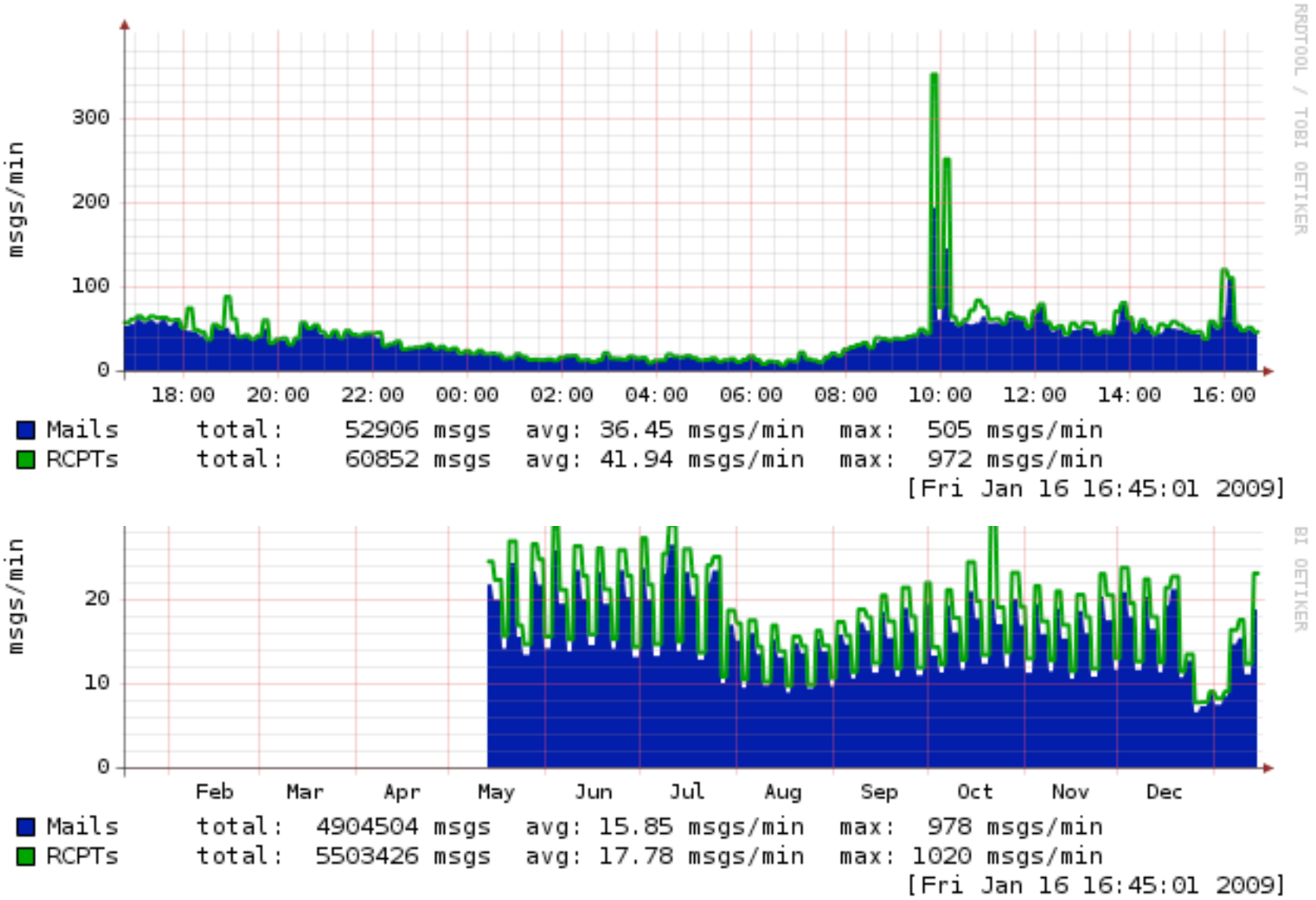
# Persönliche Spam-Statistik eines LRZ-Mitarbeiters



# Persönliche Spam-Statistik eines LRZ-Mitarbeiters



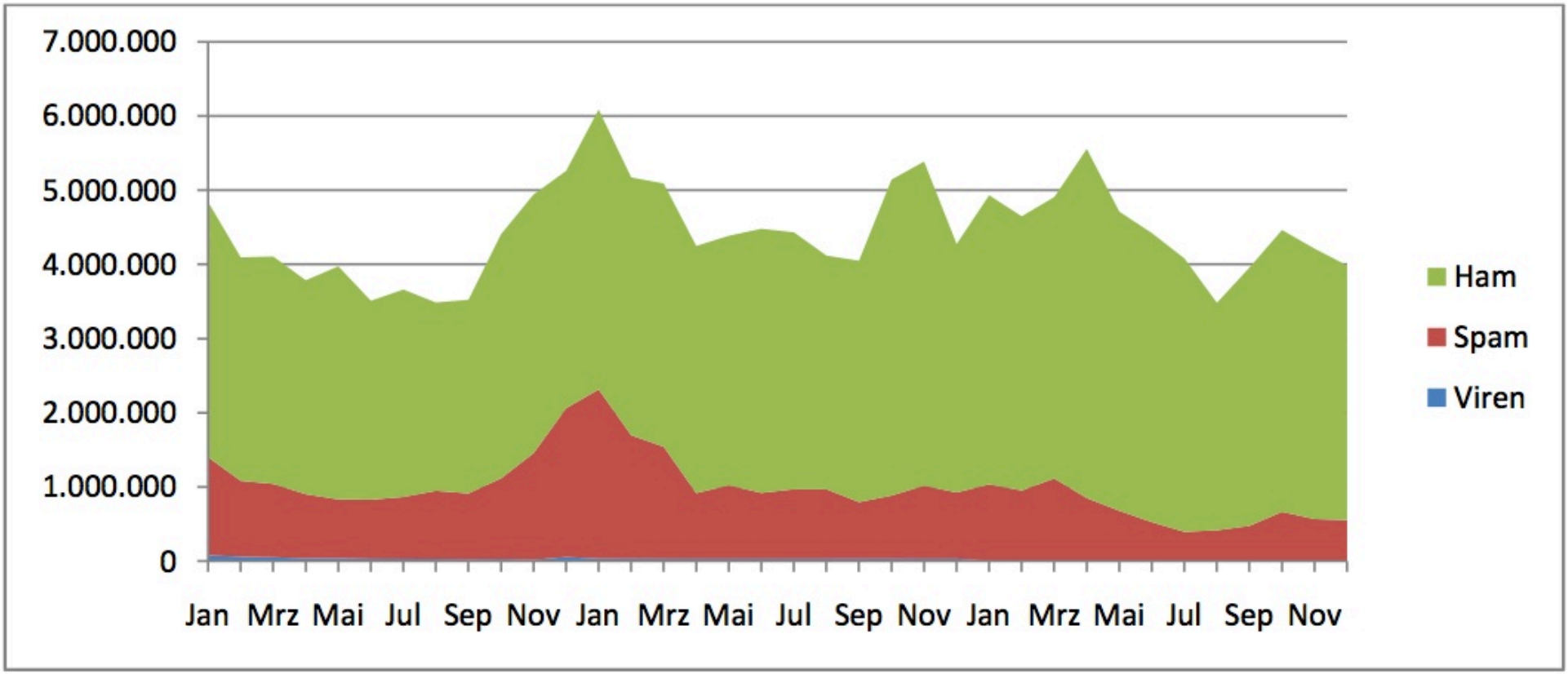
# Betriebserfahrungen: Maildurchsatz



# Mailnutzung im MWN

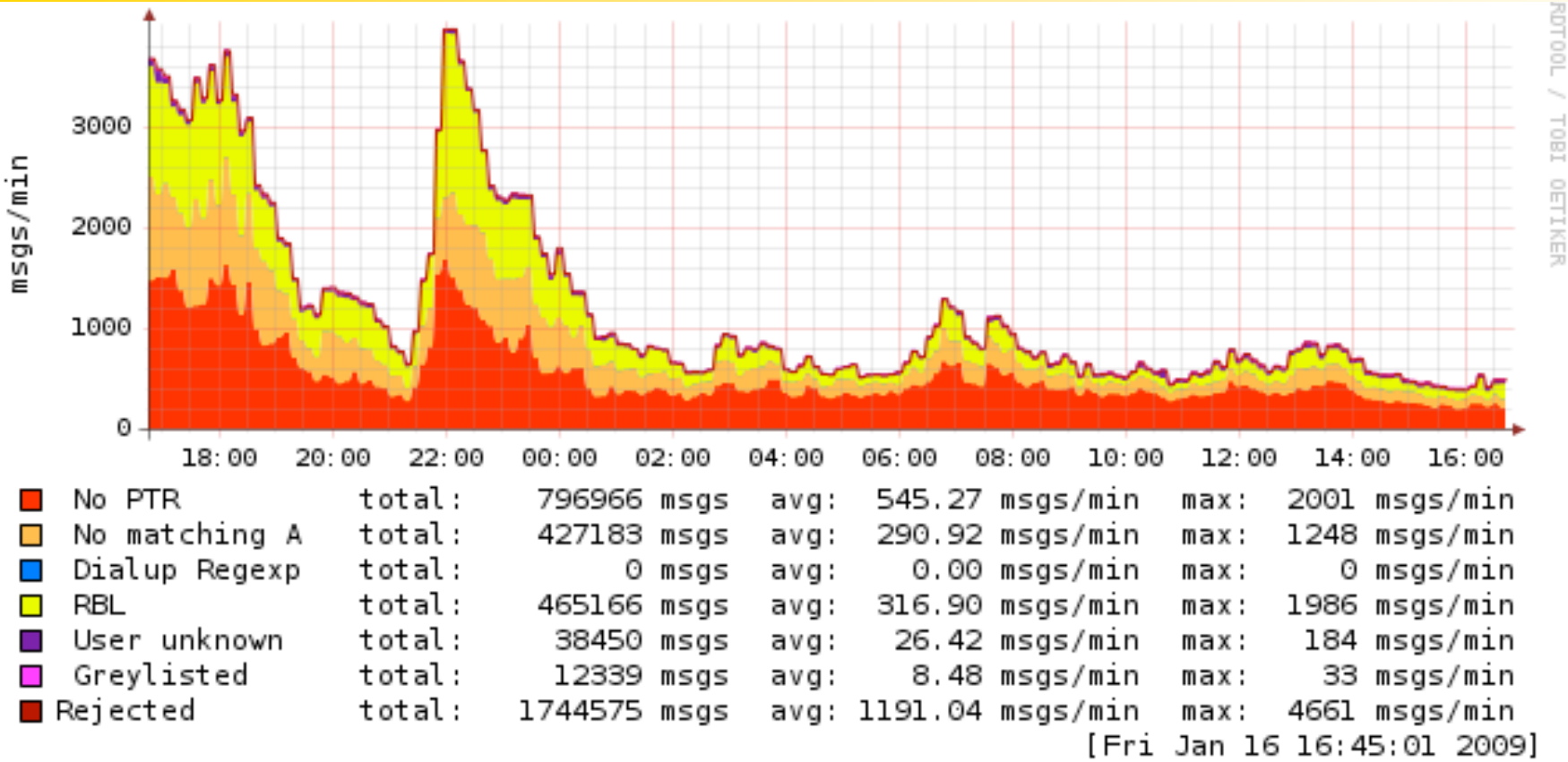
| POP/IMAP-Server für … | | Anzahl Benutzer |
|---|---|---|
| … Mitarbeiter der vom LRZ bedienten Einrichtungen (Mailserver „mailin“): | | |
| Ludwig-Maximilians-Universität München | 6.870 | |
| Technische Universität München | 5.347 | |
| Bayer. Akademie der Wissenschaften (inklusive LRZ) | 603 | |
| Fachhochschule München | 190 | |
| andere bayerische Hochschulen | 182 | |
| andere wissenschaftliche Einrichtungen | 1.862 | 15.054 |
| … die Fakultät Physik der Technischen Universität München | | 2.434 |
| … das myTUM-Portal der Technischen Universität München | | 33.746 |
| … Studenten der Ludwig-Maximilians-Universität München (Campus$^{LMU}$) | | 47.023 |
| … Studenten anderer Münchner Hochschulen | | 1.657 |
| Gesamt | | 99.914 |

# Betriebserfahrung: Ham, Spam und Viren



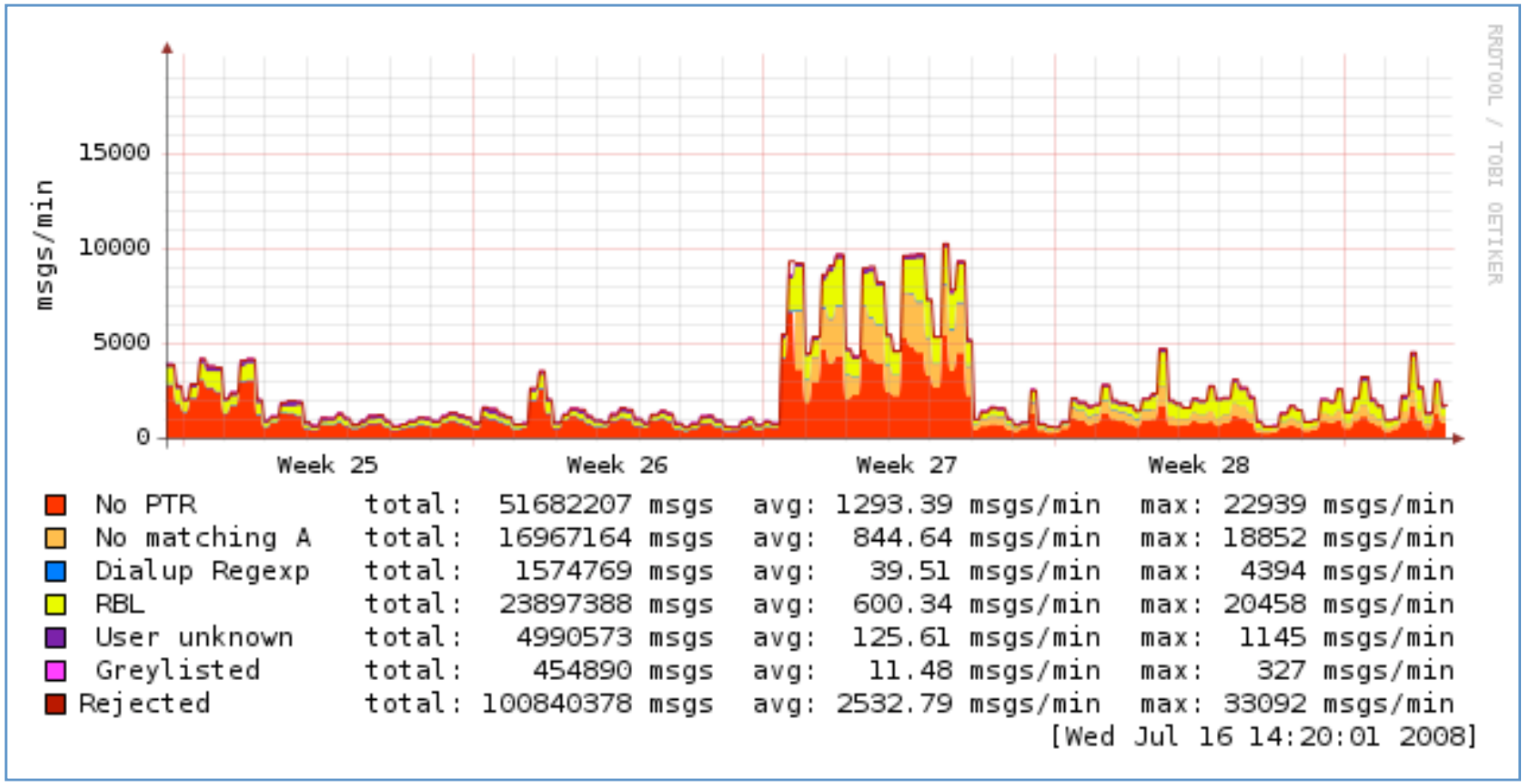

Ham-, Spam- und Virenaufkommen pro Monat in den Jahren 2006 bis 2008

# 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

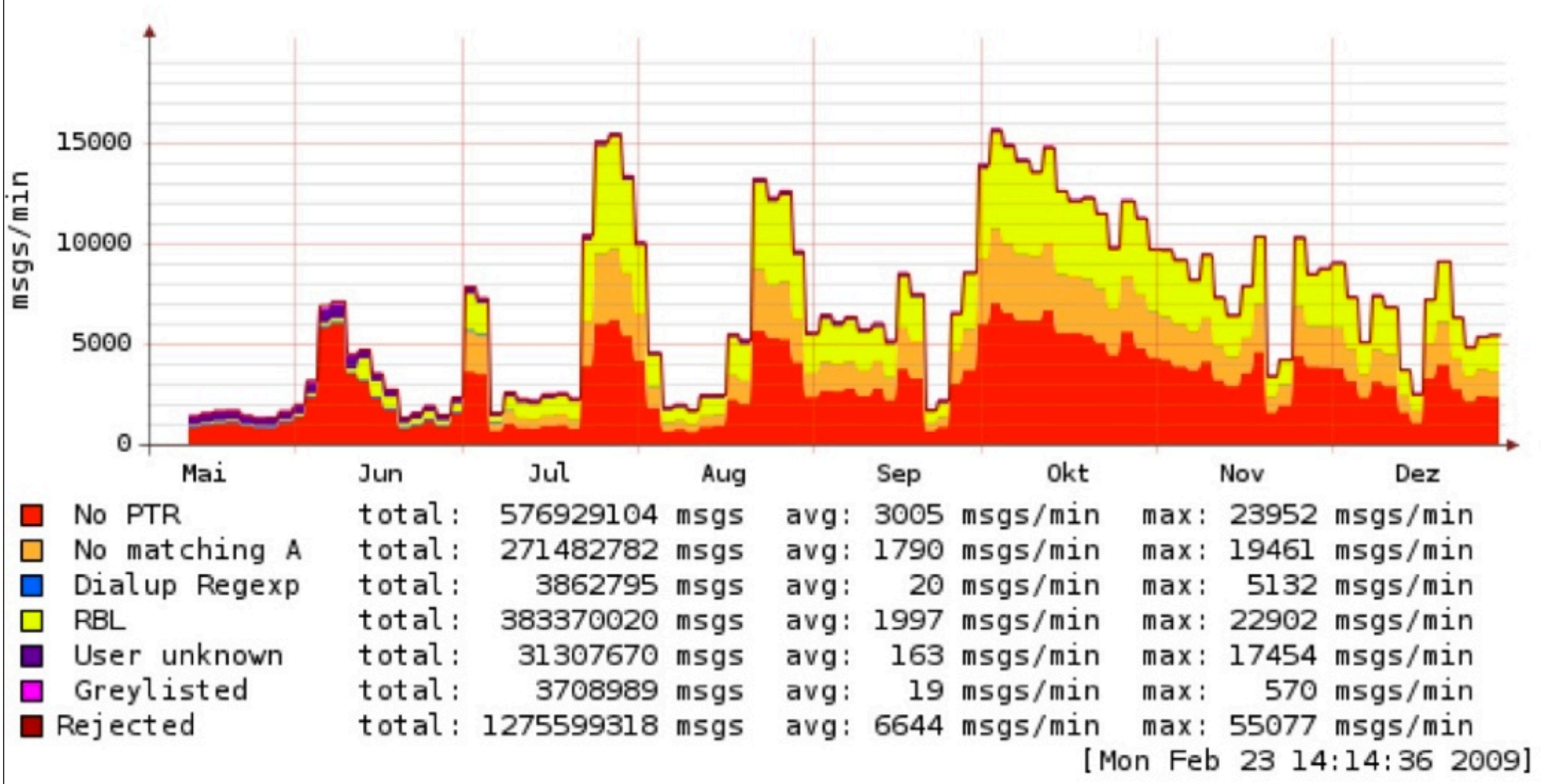
# Betriebserfahrung: Spam-Wellen




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

# Betriebserfahrung: Spam-Wellen

- Spam-Wellen



# Betriebserfahrungen: Wirksamkeit der Mechanismen