



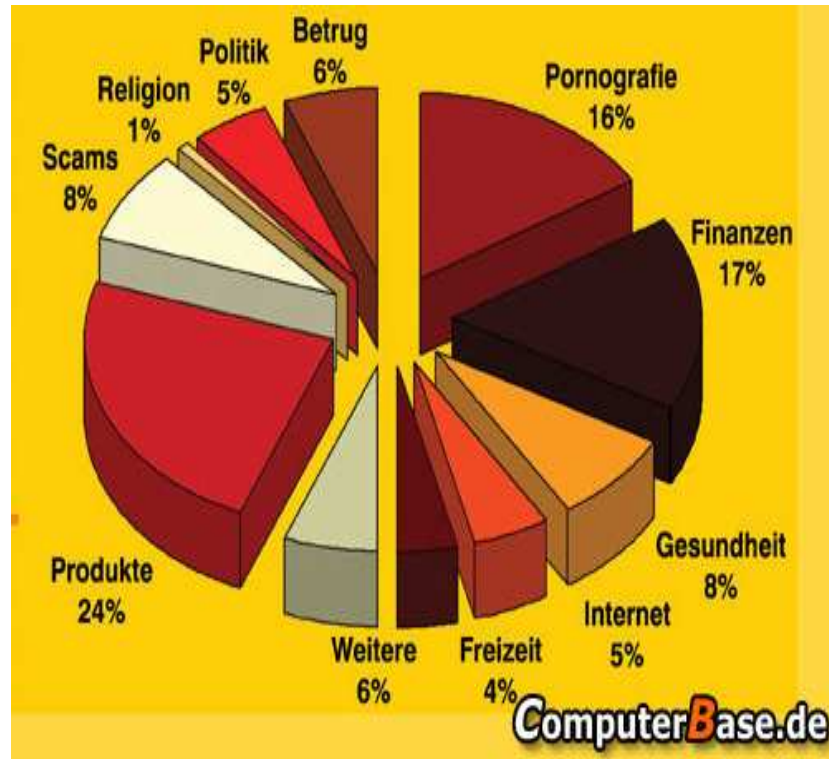
Maia Mailguard Opensource Antispam

die OpenSource Antispam- & Anti-
Virus-Lösung auf Basis von
Spamassassin, ClamAV und DCC

Beat Brunner, BRIT Informatik AG
b.brunner@brit.ch

präsentiert bei
Digicomp Academy AG

Schockierende Zahlen



- 70-80% aller E-Mails ist Spam
(Quelle: Versign)
- Spam-Volumen nimmt monatlich um 18% zu
(Quelle: ePrivacy Group)
- Bei Viren-Wellen ist in jedem 12 Mail ein Virus enthalten
(Quelle: MessageLabs)
- 1200 neue Viren jeden Monat
(Quelle: Sophos)
- Weltweite Kosten Spam:
50 Milliarden \$
(Quelle: Trend Micro)
- Durchschnittliche Kosten wegen Spam pro MA: \$ 1'934.—
(Quelle: Nucleus Research)

Die wichtigsten Tasks

- Erkennen von Spam
- Entdecken von Viren
- Blockieren und/oder betroffene Mails in Quarantäne festhalten
- Verwalten der problematischen Mails

Viren Erkennung

- Clam AntiVirus <http://www.calmav.net>
- Läuft als command-line und als daemon (auch Windows)
- Erkennt über 90'000 Viren-Signaturen
- Scannt komprimierte Files (Zip, TAR, GZip, cabinet etc.)
- Viren-Muster können von den User direkt hochgeladen werden
- Open Source Code
- Update Intervall 2h

Spam Erkennung

- SpamAssassin <http://spamassassin.apache.org>
- Pattern-basierende Erkennung
- DNSBL, RHSBL and SPF Unterstützung
- Verlinkt mit Razor, Pyzor, DCC
- Bayesian Klassifizierung
- Umfangreiche Scoring Möglichkeiten
- Verwendbar auf Server und Desktop
- Einfaches Customizing
- Erweiterbar mit Plug-ins
- Neue Pattern über User-Community

Spam Erkennung



- Was für Spam-Eigenschaften müssen erkannt werden?
 - Spamware Signaturen
 - Header Inkonsistenzen
 - HTML Body enthält nur Bild
 - Bekannte Scam Phrasen (z.B. Nigerian Letter

Spam-Erkennung

DNS-Based Tests

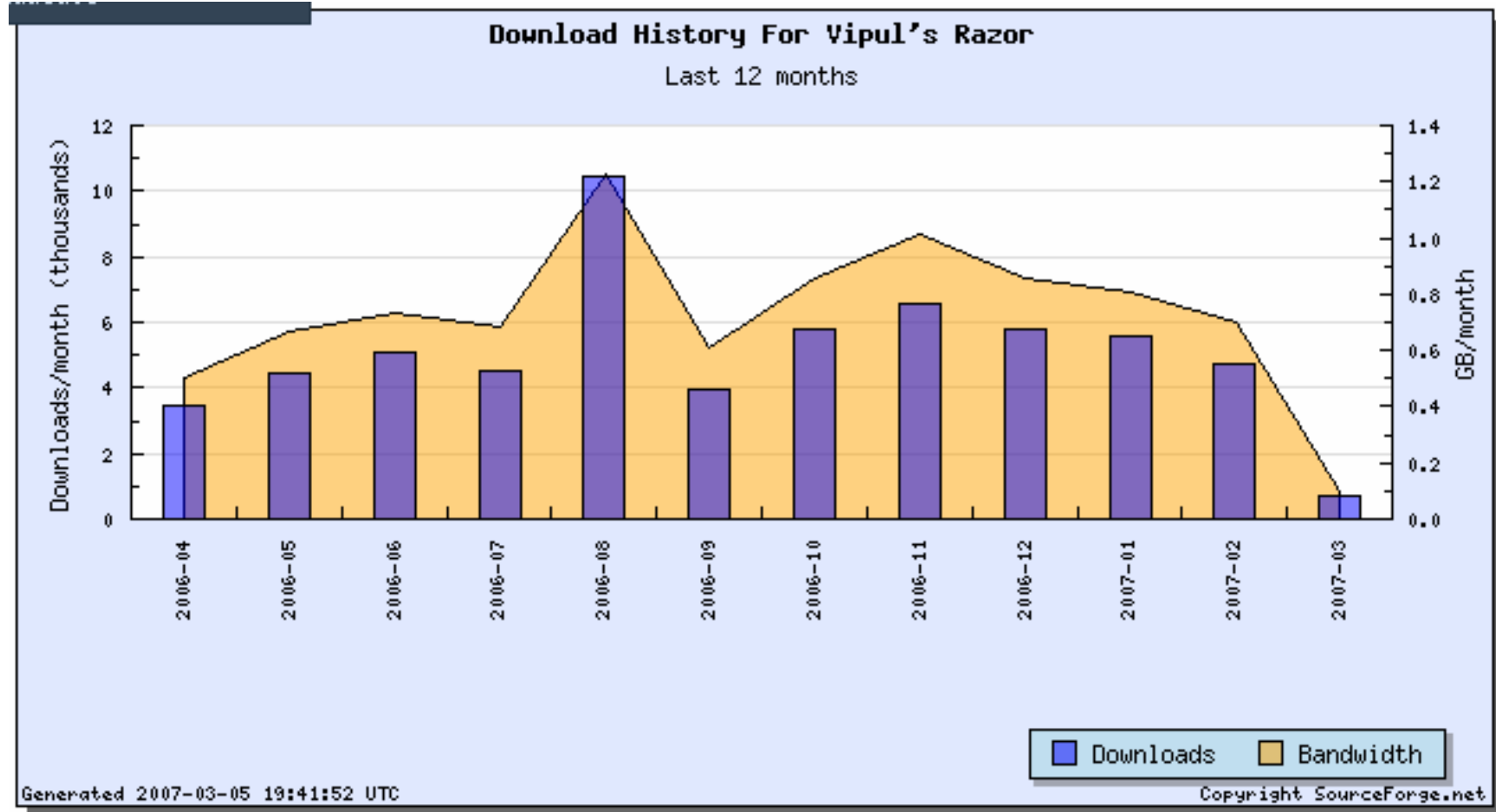
- DNSBLs (Domain Name Service Block Lists)
 - Testen der Peer-IP-Adresse gegenüber diversen Blacklists
 - Zuweisen von konfigurierbaren Scores für jedes DNSBL-Resultat
- RHSBLs (Right-Hand-Side Block Lists)
 - Testet URLs in Body des E-Mails gegenüber den Blacklisten
 - Jedes Resultat lässt sich mittels konfigurierbaren Scores werten
- SPF (Sender Policy Framework)
 - RFC 4408, DNS-Records: TXT, SPF-Record Ueberprüfung

Spam Erkennung

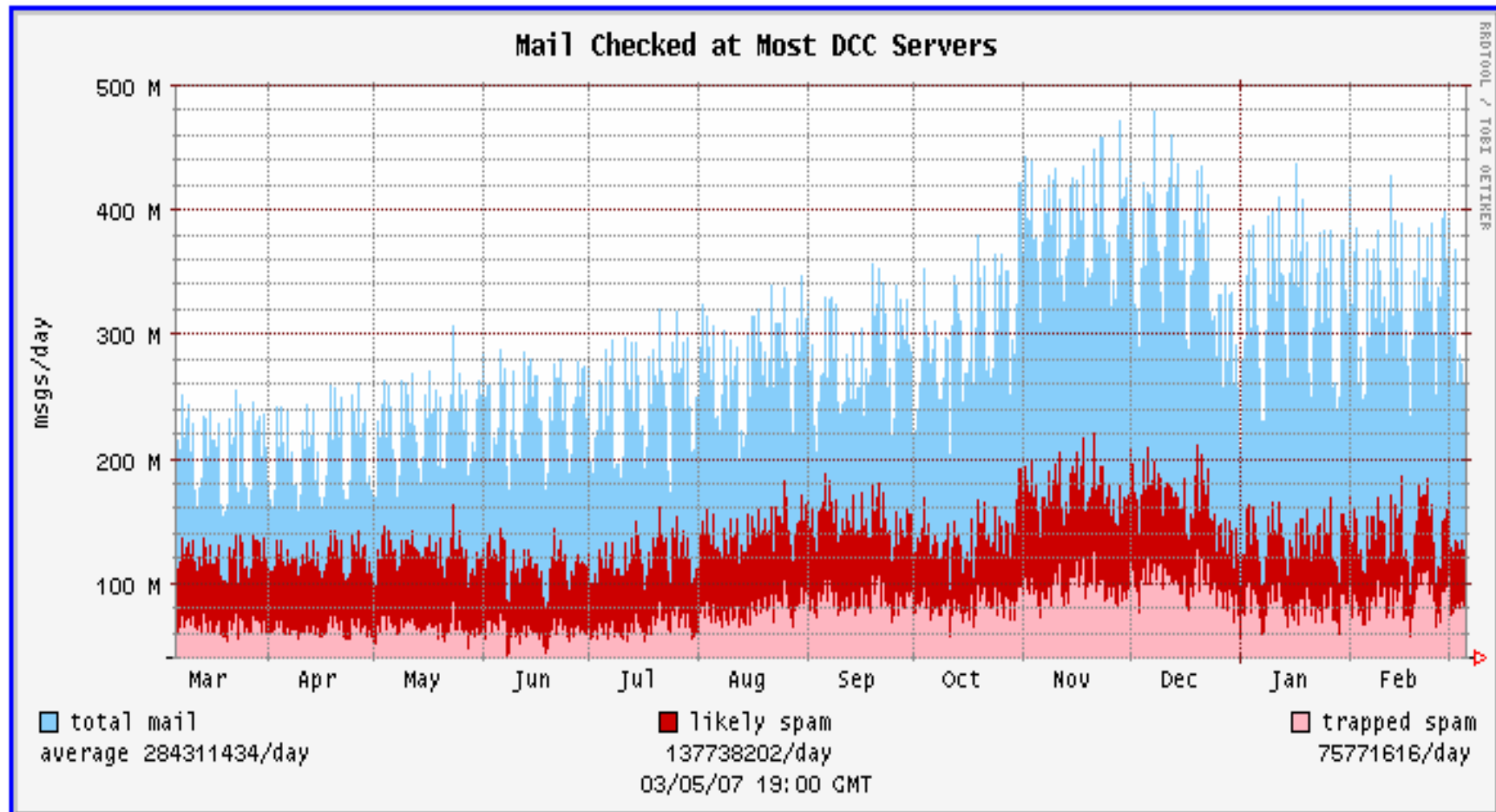
Reporting Netzwerke

- Millionen von Personen erhalten die identischen Spams
- 100'000 Lemminge können nicht falsch sein
- Datenbanken speichern Checksummen von gemeldeten Spams
 - Vipul's Razor <http://razor.sourceforge.net>
 - Pyzor <http://pyzor.sourceforge.net>
 - The Distributed Checksum Clearinghouse
 - <http://www.rhyolite.com/anti-spam/dcc>
- SpamAssassin kann wiederum ein Scoring zu diesen Einträgen vornehmen

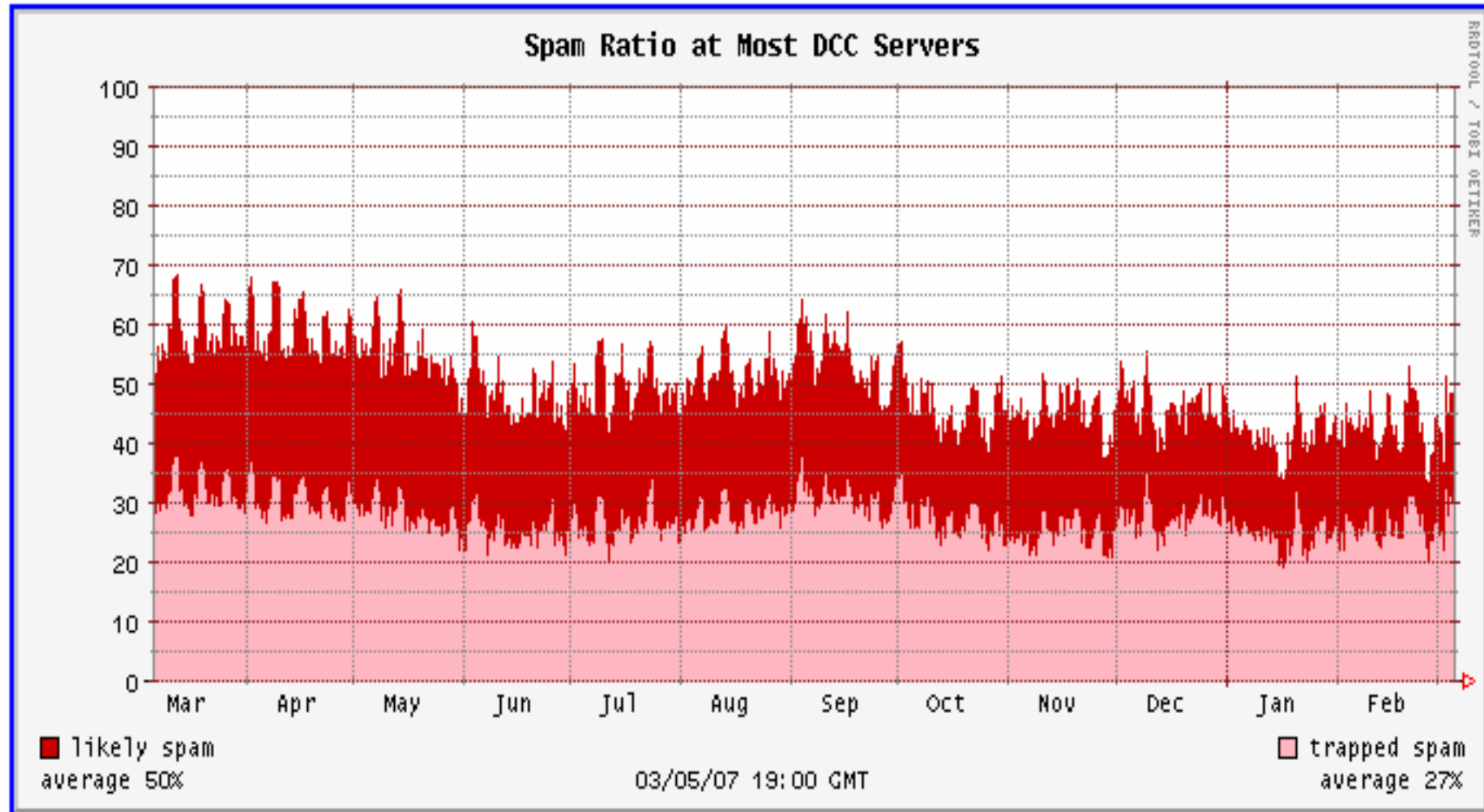
Vipul Razor Verarbeitung



DCC – Distributed Checksum Clearinghouse



DCC – Spam Quote



Spam Erkennung

Bayesian Klassifizierung

- Ist der interne Selbstlern-Mechanismus
- Analysiert die Frequenz von bestimmten Tokens der bestätigten Hams resp. Spams
- Spamassassin weist entsprechende Scores zu

Spam Erkennung

SpamAssassin Scoring Beispiel

| <u>Score</u> | <u>Rule Name</u> | <u>Rule Beschreibung</u> |
|--------------|-----------------------|--|
| 3.511 | PYZOR_CHECK | Listed in Pyzeor (http://pyzor.sourceforge.net) |
| 2.101 | BAYES_90 | Bayesian spam probability is 90 – 99% |
| 1.113 | RCVD_IN_SBL | Received via a relay in the Spamhaus Block List |
| 1.047 | RAZOR2_CHECK | Listed in razor2 |
| 0.876 | RAZOR2_CF_RANGE_11_50 | Razor2 rating between 11 – 50% |
| 0.705 | MSGID_FROM_MTA_HEADER | Message-ID was added by a relay |
| 0.336 | HTML_WEB_BUGS | Image tag intended to identify you |
| 0.320 | MIME_HTML_ONLY | Message only has text/html part MIME parts |
| 0.100 | HTML_MESSAGE | HTML included in message |
| <u>0.100</u> | SPAMCOP_URI_RBL | URI's domain appears in sc.surbl.org |
| 10.209 | <u>Total</u> | |

Blockieren und/oder Quarantäne der verdächtiger Mails

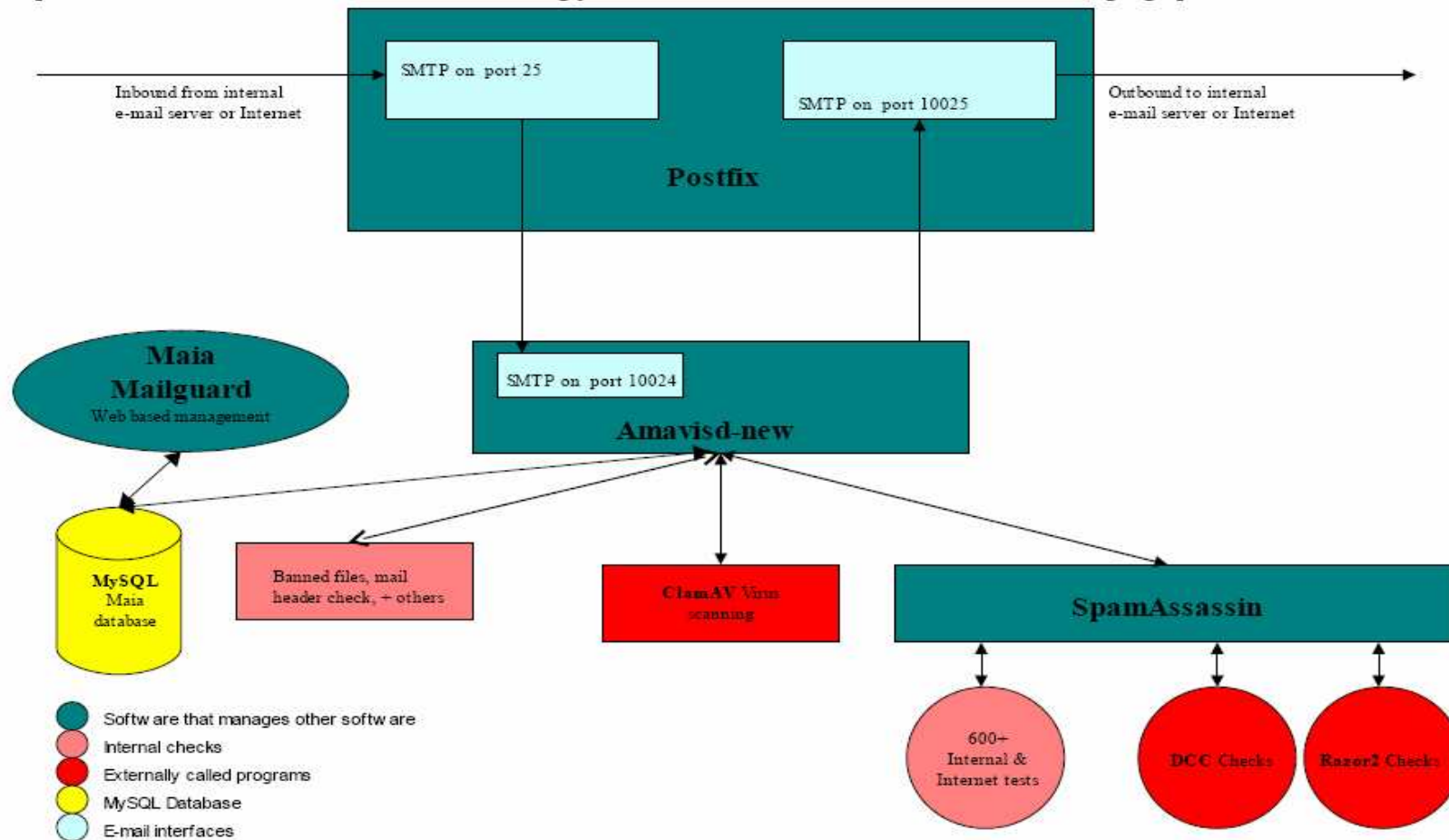
- Amavisd-new <http://www.ijs.si/software/amavisd>
- Content-basierends Framework für Viren-Scanner und Spam-Detektoren
- Identifiziert gefährliche File Attachements
- Qualifizierte Mails können zurückgewiesen, verworfen, in Quarantäne gesetzt, oder durchgelassen werden
- Per-User, per-Domain, system-weite White- und Black-Lists
- Per Benutzer definierbare Spam-Score-Limiten

Managing the Process

Maia Mailguard <http://www.maialmailguard.com>

- Web-based content filter management
- User managen ihre eigenen Content Filter Settings
- User managen ihre eigenen White- und Blacklists
- User managen ihre Quarantäne selbst
- User trainieren das eigene System (Bayes) mit Ihren Bestätigungen (ham/spam) auf
- System kann Feedback zu bestätigten Spams an die Community liefern
- Bündelt das Array von Lösungen zusammen

Maia Mailguard Architektur



User Interface








Aktueller Schutzlevel: Benutzerdefiniert

- Aus
- Niedrig
- Mittel
- Hoch

**Benutzerlevel sind aktiv:
Änderungen im Einstellungsmenü durchführen oder
eine der oben aufgeführten Voreinstellungen nutzen.

Level ändern

Inhalt des Zwischenspeichers

| | |
|---|--|
|  [Melden/Bestätigen] | Sie haben 32 eMails in Ihrem Ham-Zwischenspeicher. Klicken Sie hier um den Filter zu trainieren, oder diese eMail als Spam zu melden. |
|  [Melden/erneut zustellen] | Sie haben 90 eMails in Ihrem Spam-Zwischenspeicher. Klicken Sie hier um diese zu melden, oder eine versehentlich blockierte eMail erneut zuzustellen. |
|  [Löschen/erneut zustellen] | Sie haben 0 eMails in Ihrem Viren-Zwischenspeicher. Klicken Sie hier um diese zu löschen, oder eine versehentlich blockierte eMail erneut zuzustellen. |
|  [Löschen/erneut zustellen] | Sie haben 0 eMails im Zwischenspeicher für verbotene Dateianhänge. Klicken Sie hier um diese zu löschen, oder eine versehentlich blockierte eMail erneut zuzustellen. |
|  [Löschen/erneut zustellen] | Sie haben 0 eMails in Ihrem Zwischenspeicher für defekte Kopfzeilen. Klicken Sie hier um diese zu löschen, oder eine versehentlich blockierte eMail erneut zuzustellen. |

Alle eMails löschen

Maia Statistiken

| Statistiken für alle Benutzer | | | | | | | | | | | |
|--|--------|------------|---------|--------|--------|--------------|------------|--------|--------------|----------------|-------------|
| eMails | | | | Punkte | | | Größe (kB) | | | Bandbreite/Tag | |
| eMail-Typ | Anzahl | eMails/Tag | Prozent | Min | Max | Durchschnitt | Min | Max | Durchschnitt | MB | Kosten (\$) |
| Vermuteter Ham | 83 | 14.5 | 0.3% | 0.000 | 4.991 | 3.627 | 0.7 | 1058.1 | 69.3 | 0.98 | 0.000 |
| Bestätigter Ham | 2863 | 16.4 | 11.4% | -2.242 | 25.075 | 3.333 | 0.3 | 9114.6 | 90.1 | 1.45 | 0.000 |
| False Positives | 198 | 1.2 | 0.8% | 0.000 | 9.915 | 6.267 | 0.7 | 255.8 | 40.0 | 0.05 | 0.000 |
| Vermuteter Spam | 3792 | 123.5 | 15.1% | 0.000 | 50.504 | 15.336 | 0.3 | 86.0 | 15.7 | 1.89 | 0.000 |
| Bestätigter Spam | 15219 | 87.3 | 60.5% | 0.000 | 80.593 | 18.259 | 0.3 | 252.7 | 7.9 | 0.67 | 0.000 |
| False Negatives | 610 | 3.5 | 2.4% | -2.242 | 21.322 | 3.621 | 0.8 | 1886.1 | 17.1 | 0.06 | 0.000 |
| eMails in der Whiteliste | 1619 | 9.7 | 6.4% | - | - | - | 0.7 | 8378.1 | 116.8 | 1.11 | 0.000 |
| eMails in der Blacklist | - | - | - | - | - | - | - | - | - | - | - |
| Viren/Malware | 541 | 3.2 | 2.2% | - | - | - | 1.7 | 154.1 | 40.6 | 0.13 | 0.000 |
| verbotene Dateianhänge | 137 | 0.8 | 0.5% | - | - | - | 0.3 | 3041.4 | 73.7 | 0.06 | 0.000 |
| defekte Kopfzeilen | 91 | 0.5 | 0.4% | - | - | - | 0.8 | 5816.5 | 75.9 | 0.04 | 0.000 |
| Übergroße eMails | - | - | - | - | - | - | - | - | - | - | - |
| Effizienz 95.72% False Positive 1.05% False Negative 3.23% Empfindlichkeit 96.15% PPV 98.72% Besonderheit 93.53% NPV 82.44% | | | | | | | | | | | |

Maia Spam-Einstellungen

| Adresse: b.brunner@brit.ch | |
|---|---|
| VirenScanner | <input checked="" type="radio"/> Aktiviert <input type="radio"/> Deaktiviert |
| Gefundene Viren werden ... | <input type="radio"/> Markiert <input checked="" type="radio"/> Quarantäne <input type="radio"/> Gelöscht |
| | |
| Spam-Filterung | <input checked="" type="radio"/> Aktiviert <input type="radio"/> Deaktiviert |
| Gefundener Spam wird ... | <input type="radio"/> Markiert <input checked="" type="radio"/> Quarantäne <input type="radio"/> Gelöscht |
| Präfix in den Bereff einer Spam-eMail? | <input type="radio"/> Ja <input checked="" type="radio"/> Nein |
| Füge 'X-Spam: Headers' ein, wenn Punkte >= | <input type="text" value="-999.000"/> |
| Betrachte eMail als 'Spam', wenn Punkte >= | <input type="text" value="5.000"/> |
| Verschiebe in Quarantäne, wenn Punkte >= | <input type="text" value="5.000"/> |
| | |
| eMail-Anhang Filter | <input checked="" type="radio"/> Aktiviert <input type="radio"/> Deaktiviert |
| eMails mit gefährlichen Anhängen werden ... | <input checked="" type="radio"/> Markiert <input type="radio"/> Quarantäne <input type="radio"/> Gelöscht |
| | |
| Filter für defekte Kopfzeilen | <input checked="" type="radio"/> Aktiviert <input type="radio"/> Deaktiviert |
| eMails mit 'Bad Headers' werden ... | <input type="radio"/> Markiert <input checked="" type="radio"/> Quarantäne <input type="radio"/> Gelöscht |

Maia Spam-Auflistung

| Verdächtiger Spam (1 - 50 von 90) | | | | | | | |
|-------------------------------------|---------------------|----------------------|-------------------|------------------------|--|----------------------------|-------------------------------|
| Bestätige den Status dieser eMails | | | | | | | |
| 1 2 Weiter>> | | | | | | | |
| Punkte | Eingang | Von | Zu | Betreff | <input checked="" type="radio"/> Spam? | <input type="radio"/> Ham? | <input type="radio"/> Löschen |
| 5.9 | 2007-03-02 14:24:19 | list@comdirect.ch | b.brunner@brit.ch | Attraktive Mä... | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6.0 | 2007-03-01 11:27:14 | cyclicallygrapevi... | b.brunner@brit.ch | Bachelors, Master... | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6.1 | 2007-03-02 11:55:11 | agatonycad@anchor... | b.brunner@brit.ch | Cant Believe It | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6.4 | 2007-03-01 18:15:58 | shenmandimom@ocn.... | b.brunner@brit.ch | Last Wk | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 6.7 | 2007-03-01 16:29:22 | zwpao@pulte.com.mx | b.brunner@brit.ch | 6 as soon as poss... | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 7.2 | 2007-03-02 21:13:28 | therwolnyayt@rima... | b.brunner@brit.ch | Sorry | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 7.3 | 2007-03-02 07:30:07 | inaadger@k.st | b.brunner@brit.ch | Upptick Stock | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 7.5 | 2007-03-01 11:51:56 | 492alaa@icare.info | b.brunner@brit.ch | Re: You Need a Be... | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 7.8 | 2007-03-01 18:59:00 | dwscottmasonreale... | b.brunner@brit.ch | Don't forget to a... | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 8.5 | 2007-03-03 15:14:22 | hservitor@boursor... | b.brunner@brit.ch | by rutgers at cavort | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 8.5 | 2007-03-03 09:27:29 | gwavanat@srv1.bit... | b.brunner@brit.ch | [GWAVA Nation New... | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 8.8 | 2007-03-03 02:38:48 | talbright@brigado... | b.brunner@brit.ch | PC PhoneHome and ... | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 9.1 | 2007-03-02 22:54:49 | jwhans@atlanticbb... | b.brunner@brit.ch | Not magnate by eucre | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 9.1 | 2007-03-02 23:27:43 | yyvbarbarism@arab... | b.brunner@brit.ch | An batavia he car... | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 9.3 | 2007-03-03 03:44:15 | mjchariot@miq.zzn... | b.brunner@brit.ch | Is it eye | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 9.7 | 2007-03-02 08:27:22 | cameron_coleys@ma... | b.brunner@brit.ch | Buy Rolex, Omega, P... | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 9.9 | 2007-03-01 12:20:03 | vgl@glenviewfarm.com | b.brunner@brit.ch | wavelength pagoda | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 9.9 | 2007-03-01 21:17:54 | asne@unioncreekor... | b.brunner@brit.ch | I hope I give pro... | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| 10.3 | 2007-03-03 13:47:35 | lnl@autotuning.cz | b.brunner@brit.ch | And he notes that... | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Maia Spam-Details

| Punkte | Regel ausgelöst | Erklärung |
|----------------------|---|---|
| 3.500 | BAYES_99 | Bayesian spam probability is 99 to 100% |
| 1.867 | HTML_IMAGE_ONLY_12 | HTML: images with 800-1200 bytes of words |
| 1.660 | SARE_GIF_STOX | Inline Gif with little HTML |
| 0.750 | SARE_GIF_ATTACH | Email has a inline gif |
| 0.001 | HTML_MESSAGE | HTML included in message |
| FROM: | "Lina Bowe" <dwscottmasonrealestatem@scottmasonrealestate.com> | |
| TO: | <b.brunner@brit.ch> | |
| SUBJECT: | Don't forget to ask for discount! | |
| CONTENT-TYPE: | multipart/related | |

CONTENT-TYPE: multipart/alternative

CONTENT-TYPE: text/plain

Isbelthe woman and I will do as. Oft expectation fails and most.
Needs go that the devil drives. In war?Faith sir he has led the. What
should be said?If thou. Shall be servedSo make the. All the secrets of
our camp. Very much content my lord and. Heaven delights to hearAnd
loves. Night so lust doth playWith.

CONTENT-TYPE: text/html



Maia Black- und White-List

| | |
|--|--|
| eMail-Adresse oder Domain hinzufügen: | <input type="text"/> |
| Hinzufügen zu welcher Liste: | <input checked="" type="radio"/> Whitelist <input type="radio"/> Blacklist |
| <input type="button" value="Hinzufügen zu Liste"/> | |

| Adresse | Whitelist | Blacklist | Entfernen |
|------------------------|----------------------------------|-----------------------|-----------------------|
| a.kess@sigs-datacom.de | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| admin2@hp-ecomm.com | <input checked="" type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Maia System-Konfiguration

| Systemkonfiguration | |
|--|--|
| Benutzerkonten automatisch erstellen? [?] | <input type="radio"/> Ja <input checked="" type="radio"/> Nein |
| Automatisch Kennwörter für neue Benutzerkonten generieren? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| Verwaltung von falschen Negativen? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| Statistiken aktivieren? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| Erlaube Benutzern das aktivieren/deaktivieren des VirenScans? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| VirenScan aktivieren? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| Spamfilter aktivieren? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| Erlaube Benutzern das aktivieren/deaktivieren des Spamfilters? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| Auf verbotene eMail-Anhänge prüfen? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| Erlaube Benutzern das aktivieren/deaktivieren des Filters für verbotene Anhänge? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| Nach 'Bad Headers' (defekten Kopfzeilen) suchen? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| Erlaube Benutzern das aktivieren/deaktivieren des 'Bad Header' Filters? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| Benutzerkonten für Spamfallen zulassen? [?] | <input type="radio"/> Ja <input checked="" type="radio"/> Nein |
| Benutzern das verknüpfen von eMail-Adressen mit Ihren Konten erlauben? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| Dürfen Benutzer ihren Benutzernamen ändern? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| Dürfen Administratoren die eMails der Benutzer lesen? [?] | <input type="radio"/> Ja <input checked="" type="radio"/> Nein |
| Soll der Standard-Systembenutzer (@.) nur lokale Empfänger verwalten? [?] | <input checked="" type="radio"/> Ja <input type="radio"/> Nein |
| max. Größe der eMails (Bytes): [?] | <input type="text" value="1000000000"/> |
| Übergroße eMails werden ... [?] | <input type="radio"/> Akzeptiert <input checked="" type="radio"/> Zurückgewiesen |

Automatische Updates

- RuleSets werden mit RoulesDuJour aktualisiert
- TRUSTED_RULESETS auf www.rulesemporium.com
- durch Cron-Jobs wird alles automatisch aktualisiert

Implementierte Basis

- Alle Installation auf SLES
(Suse Linux Enterprise Server)
- Hardware-Anforderungen:
 - Mindestens 1.5 GHz CPU
 - Mindestens 20 GB HD
 - Mindestens 1 GB RAM

Zufriedene Kunden



- Echos:
 - Einfache Bedienung
 - Stabil / Sicher
 - Sehr hohe Erkennungs-Quote (oft 95%)
 - Günstig, nur Implementations-Aufwand
 - Absolut konkurrenzfähig gegen über kostenpflichtiger Software
 - Prompter Support



Konsequenz:



- Just use it!

