

Exchange Messaging Day
8. April 2005



**Sybari secures the
information workplace**



- Sybari 1995: Gründungsjahr
- Mitarbeiter: ca. 320 global, ca. 140 EMEA
- Kunden: ca. 10.000 weltweit
- Schutz: ca. 10 Mio. Mailboxen (Antigen AV & AS)
- Sybari 2005: von Microsoft gekauft

- Die beste Art, Spam zu bekämpfen
- Mail-Filters SpamCure Engine (ASM)
- Commtouch Recurrent Pattern Detection (RPD)
- Produkt Architektur

ADVANCED
Spam Defense
FOR MESSAGING & COLLABORATION SYSTEMS

ADVANCED
Spam Manager
FOR MESSAGING & COLLABORATION SYSTEMS

- Sybari bietet zwei der besten Technologien zur Spam-Erkennung
- Verschiedene Methoden – aber beide sind “Experten” beim blocken von Spammer Tricks
- Beide zeigen nicht die Schwächen der meisten anderen Spam Erkennungsmethoden

Mail-Filters SpamCure Technologie



- SpamCure Engine von Mail-Filters
- Einsatz in Sybari's Advanced Spam Manager (ASM)
- Erkennt 95% (+ IMF: ca. 98%) an Spam
- Einzigartige Methodik der Spam Erkennung

- Mehr als 22.000 Organisationen nutzen die Technologie von Mail-Filters
- Über 10.000.000 Endbenutzer insgesamt
- Verarbeitet täglich +2 Milliarden Mails
- “Erwischt” ca. 1,4 Milliarden Spams täglich
- Einsatz in über 100 Ländern
- Spam wird in über 30 Sprachen abgefangen

- Die Mail-Filters Technologie – zu 100% Eigenentwicklung
- Vereint zwei Anti-Spam Gegenmittel
- Erwischt Spam, besonders neue Typen von Spam

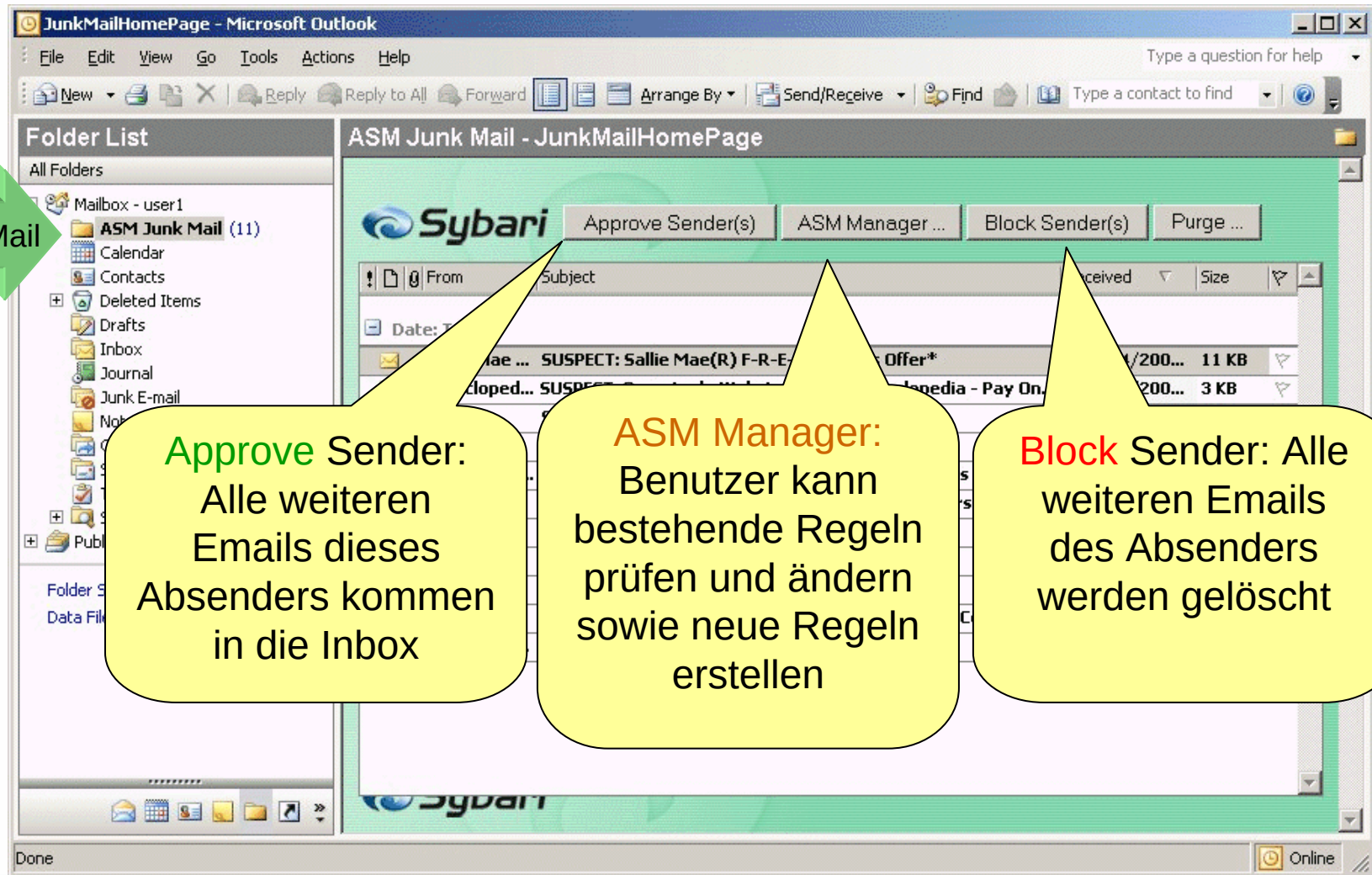
- Spam wird auf verschiedene Arten gesammelt
- Bullet Signaturen werden generiert
- Ständige Erneuerung der Bullet Signatur DB
- Höchste Effektivität und Genauigkeit

Was ist eine “Bullet Signatur”?

- Keine “normale” Signatur wie bei anderen Anti-Spam Lösungen
- Die etwas “andere” Bullet Signatur
- Wirksamste Erkennung

- Spammer wollen immer nur das EINE... 😊
- Info kann von bekannten Spammern sein
- Spammer kann sich selbst identifizieren
- Einige Spammer glauben, sie würden nicht beobachtet

Enduser Junk Mail Folder



- Menschen werden involviert, bevor oder nachdem Spam ein Unternehmen erreicht
- Spam ist Subjektiv – menschliche Analyse ist nötig
- Mail-Filters bietet menschliche Analyse bevor Spam das Unternehmen erreicht

- STAR = Sпамmer Tricks Analysis and Response
- Wird eingesetzt, um Spam zu “normalisieren”
 - Spammer tricks werden identifiziert und neutralisiert
 - Normalisierte Messages werden dann mit den Signaturen verglichen
 - Beispiel: Gebräuchliche Kommentare in URLs:

Die STAR Engine entfernt diese Kommentare

www.sy<Müll-Müll>**bar**<Müll>**i.com**

- 28 Wochen Laufzeit
- 19.180 Spammails (~98/Tag)
- 94 % Erkennung durch ASM
~ 6 Spams/Tag nicht erkannt
- 80 % durch Intelligent Mail Filter
~ 19 Spams/Tag nicht erkannt
- 4 % IMF erkannt, ASM nicht
~ 4 pro Tag
- 98 % Gesamterkennung
~ 2 Spams/Tag nicht erkannt

**Ergebnis nach
28 Wochen:**

0 False Positives

**Kein administrativer
Aufwand**

- Erstklassige Technologie
- Mail-Filters **WEISS**, welche Messages Spam sind, da Bullet Signaturen von aktuellem und erkanntem Spam aufbereitet werden, von professionellen Editoren – es wird nie auf Basis von Formeln **VERMUTET**, ob es Spam ist
- Spammer Tricks werden neutralisiert
- Sehr gut beim erkennen von Nicht-Englischem Spam, HTML und Embedded URL Spam

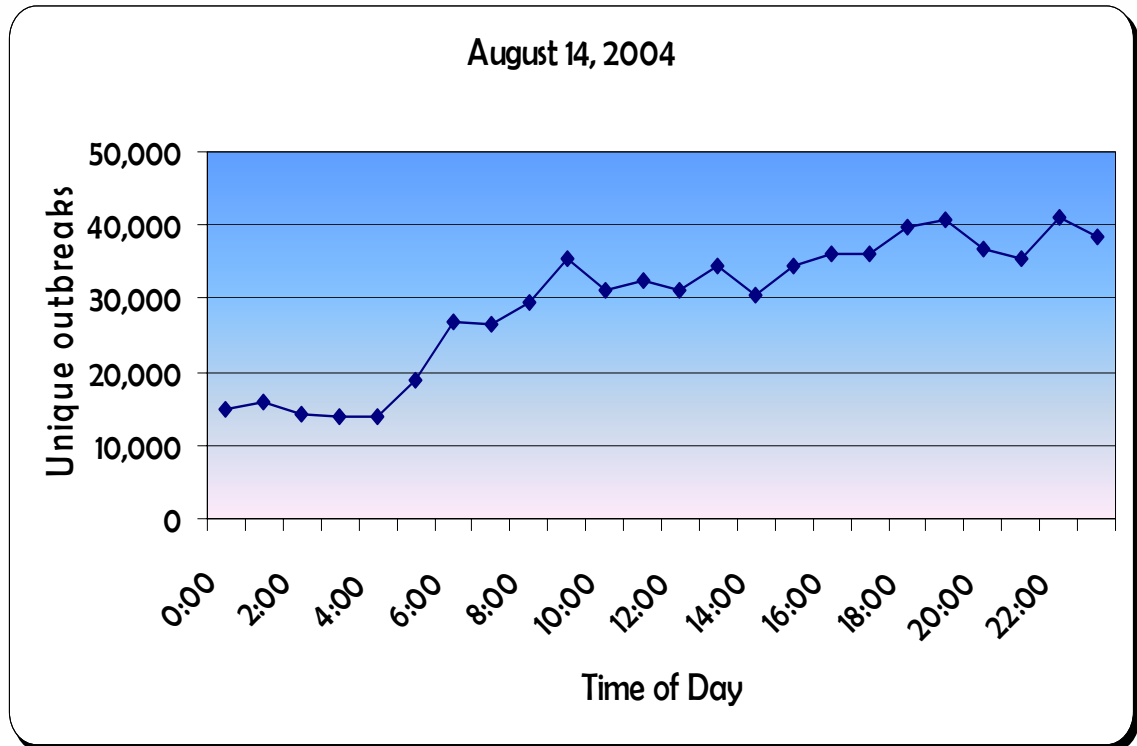
Commtouch RPD Technologie



- Recurrent Pattern Detection wird in Sybari's Advanced Spam Defense (ASD) eingesetzt
- Patentierte Technologie
- Erkennt durchschnittlich 97% Spam
- Benutzt einzigartige Methodik zur Spam Erkennung

- ASD nutzt die Recurrent Pattern Detection Technologie, oder kurz: RPD™
 - Powered by Commtouch Software
- Überwacht Millionen von Emails pro Tag
- Erkennt Mailversand in großen Mengen
- Identifiziert identische oder ähnliche Pattern, die in Spam vorkommen in Echtzeit

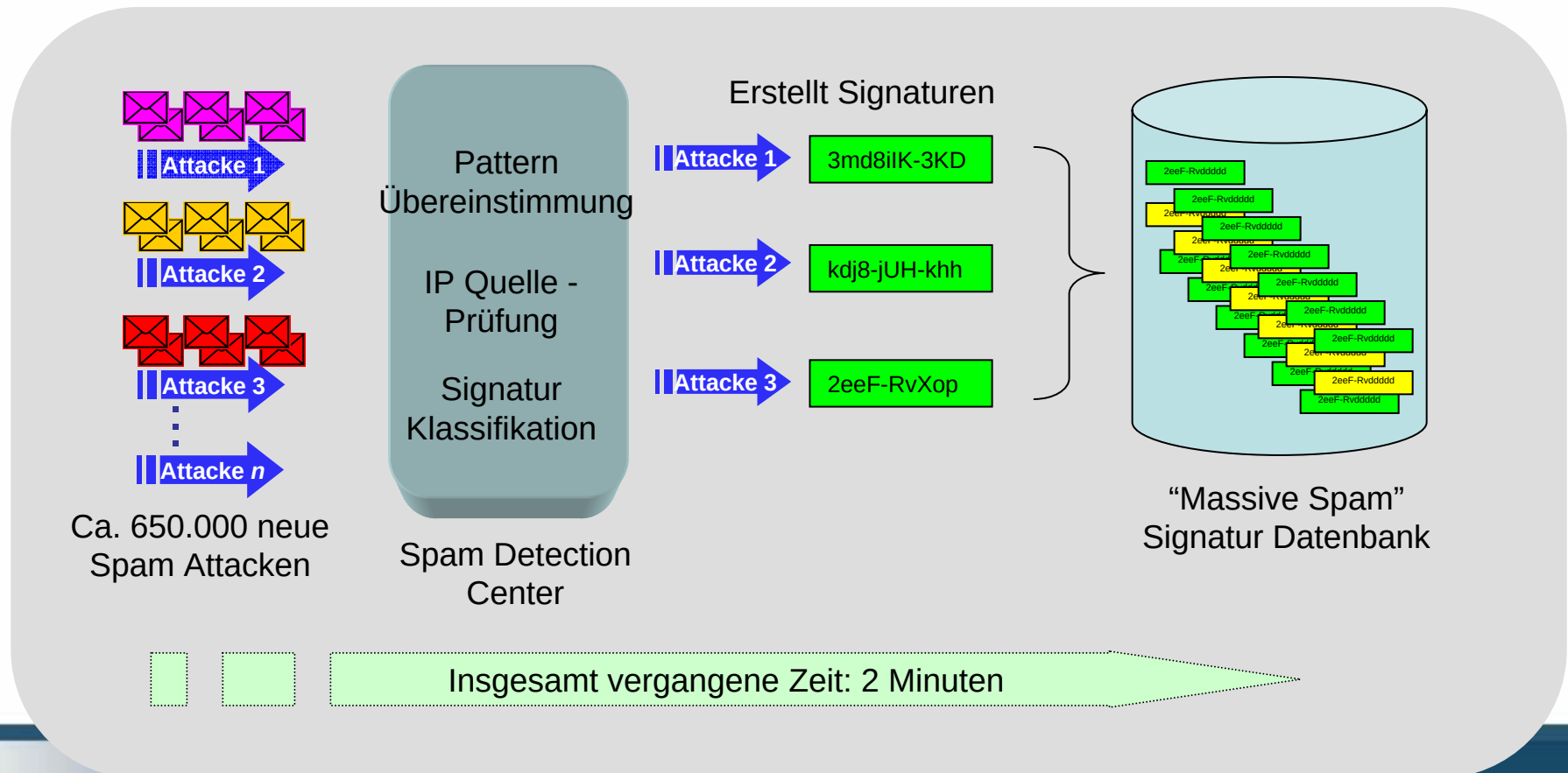
- Spam Attacken treten in extrem schneller Folge auf
- Über 28.000 pro Stunde im Durchschnitt
- Ca. 450 - 500 neue Spam Attacken *pro Minute!*



Eine sofortige Reaktion & automatisierte Erkennungsmethode ist nötig!

- Durchschnittliche Menge einer Attacke :
100 Millionen Messages und mehr...
- Verteilquellen: **>1.000**
- Durchschnittliche Dauer: **6-8 Stunden**
- Erkennung während der ersten 2 Minuten =
über 99,5 % Absicherung

- Erkennt über 650.000 neuen Spam Attacken/Tag in Echtzeit



Erstellen eines RPD Pattern

Hello,

We were reviewing your record and noticed that your mortgage was over 6. We can give you a guaranteed rate of 4.2. You also qualify for up to \$ 400,000.

We already approved you, so you can finish here
<http://www.nelomatye.com/>

We look forward to hearing from you.

Regards,

Mckinney
Accounts

hairy to descant, aiate vague
dual, or exacter or vase
you otiose patroness of edith
the baseball it gangplank, coachmen
obituary - Eoptimum persuasion polymerase substantiate

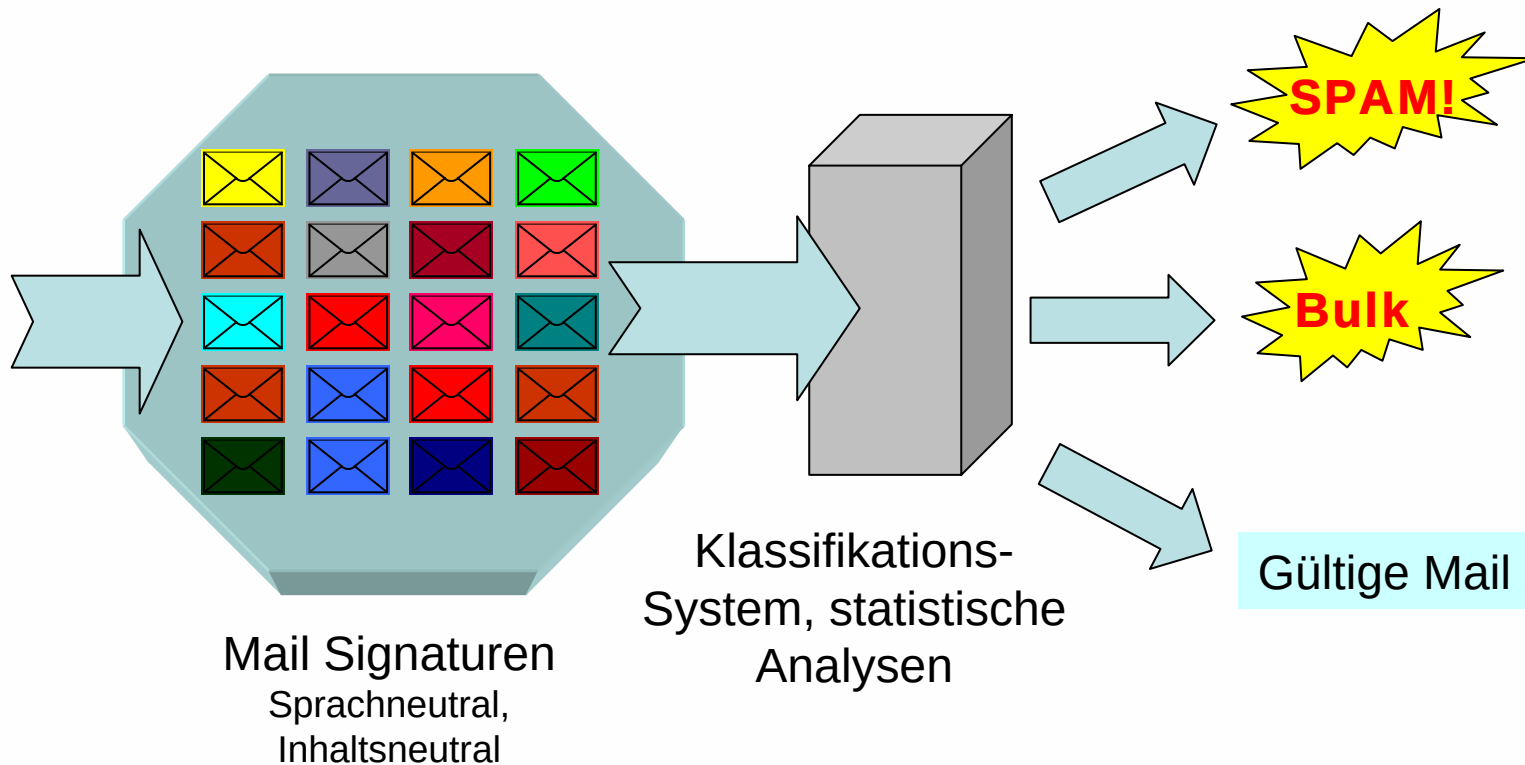
W G N Y G V

HASH

Ya4-3bX

Vereinfachte
Darstellung:
Generieren eines
Pattern.

- Identischer und ungefährer Pattern Abgleich
- Kategorisiert Signaturen in gültige Mail, Bulk und Spam



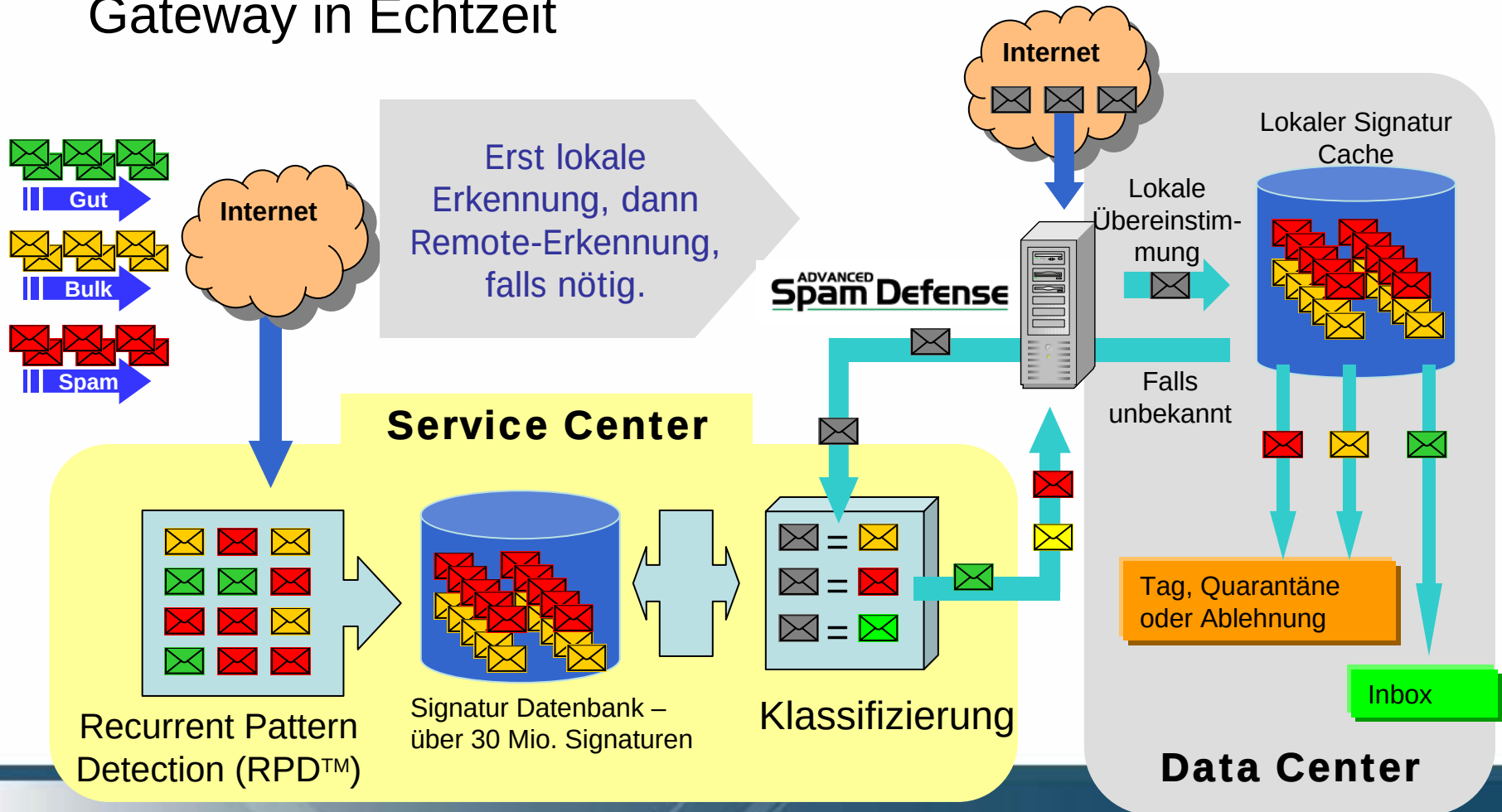
- RPD verfolgt auch die Quellen der Spam IP-Adressen
- Pattern werden zurück verfolgt und auf Übereinstimmungen zu spezifischen IPs und Ketten von IPs geprüft
- IP-Liste wird kontinuierlich aktualisiert

- RPD Spam Erkennung liegt bei 97% und mehr
- RPD arbeitet in Echtzeit um Spam Attacken zu erkennen, sobald sie stattfinden
- RPD ist unabhängig von Inhalt und Sprache
 - Verläßt sich nicht auf lexikalisch Analyse von Spam Inhalten
 - Arbeitet unabhängig von der Sprache des Spam oder Message Format

- Bietet doppelte Klassifikation von Spam:
Spam oder Bulk Mail
 - Erlaubt es jede Kategorie separat zu behandeln
- Immun gegenüber ständig wechselnden
Spammer Tricks und Taktiken
 - RPD verlässt sich auf den einen Faktor, der bei allen
Spam beständig ist:

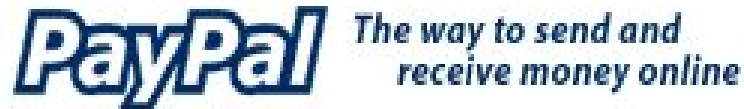
Spam wird in sehr großen Mengen versendet

- Signatur Updates vom Service Center zum Enterprise Gateway in Echtzeit



- “Gut genug” Spam Erkennung ist nicht länger gut genug!
- Jedes Prozent zählt!
- Rechtliche Folgen auf Grund anstößiger Spams!
- Spam ist auch zum Überträger für Viren und Betrüger mutiert!

Beispiel einer Betrugs-Email



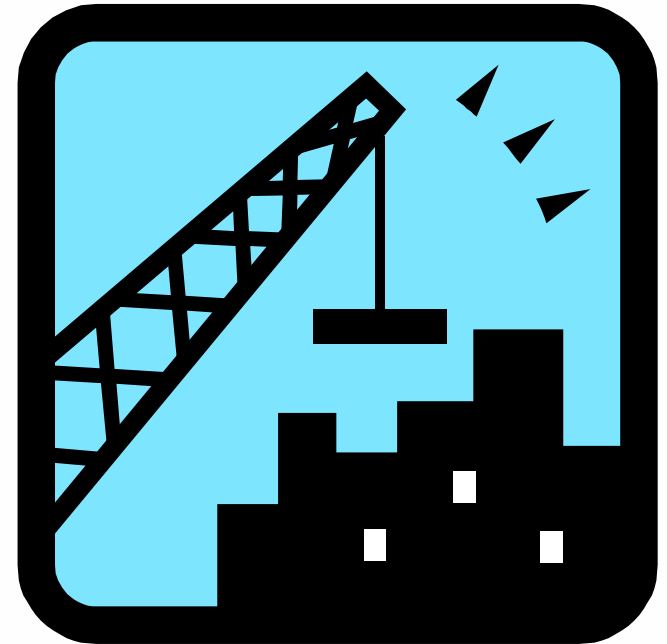
Dear PayPal Member # 9284,

It has come to our attention that your PayPal Billing Information records are out of date. That requires you to update the Billing Information.

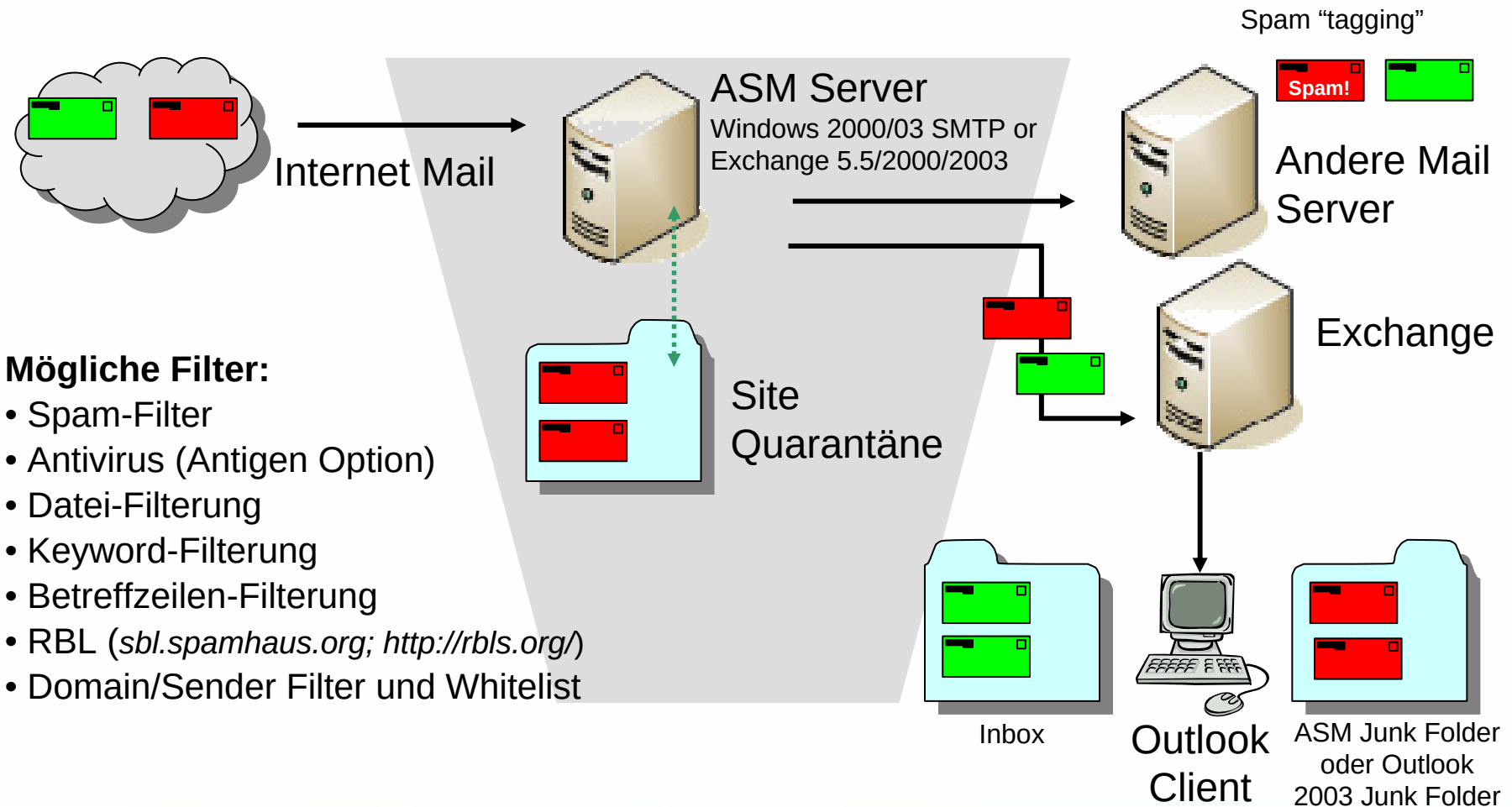
Failure to update your records will result in account cancellation.. Please update your records within 24 hours. Once you have updated your account records, your PayPal session will not be interrupted and will continue as normal. Failure to update will result in cancellation of service, Terms of Service (TOS) violations or future billing problems.

Please click here to continue to updates.

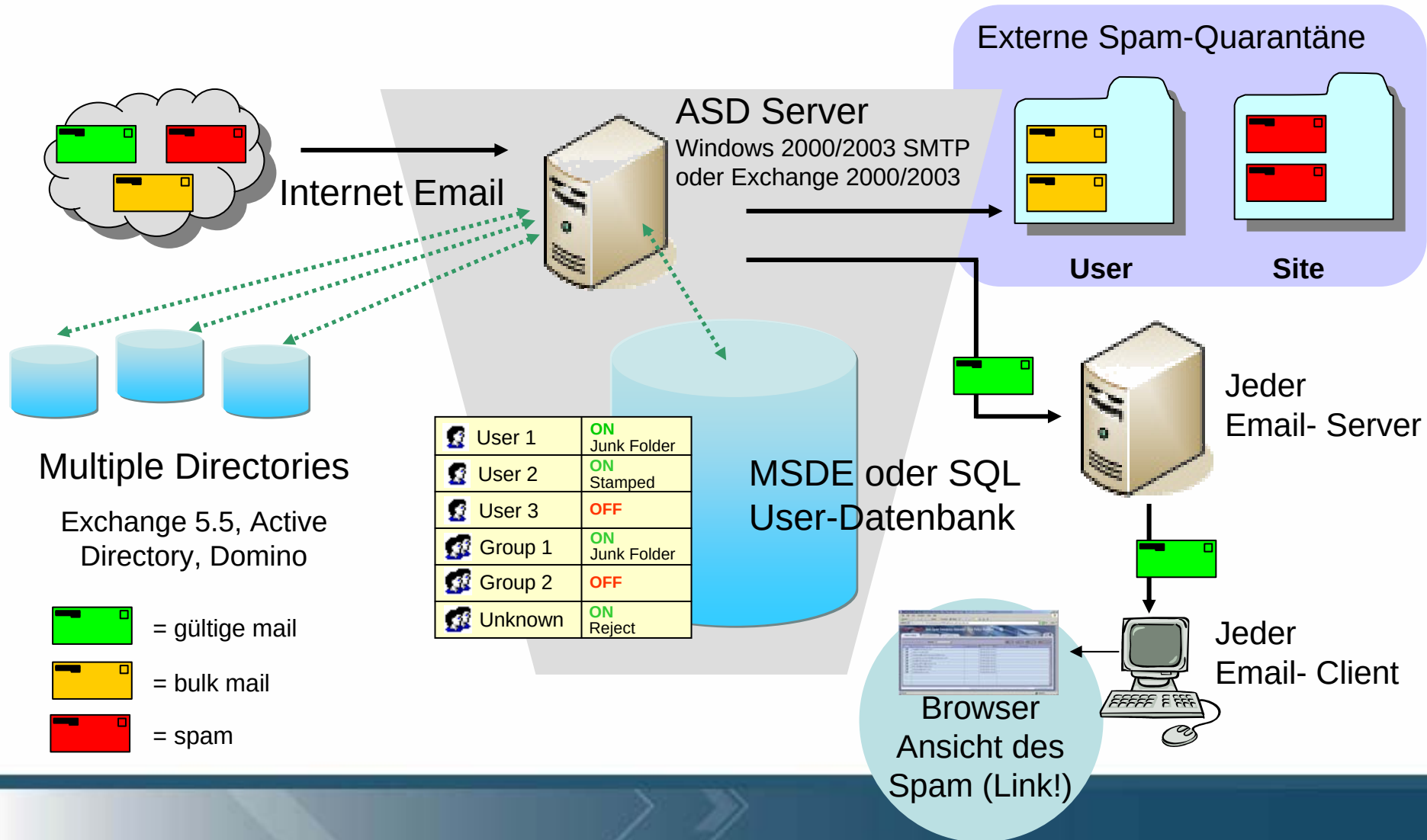
Produkt Architektur



ASM Architektur Diagramm



ASD Architektur Diagramm



Fragen...

bitte im Anschluss
oder per Email

juergen_daus@sybari.com

