E-Mail-Sicherheit
- neue Systeme im Test -

Dr. Damian Bucher

Zentrum für Informationsverarbeitung

ZENTRUM FÜR
INFORMATIONS
VERARBEITUNG

Inhalt

- Einleitung
  - Was ist E-Mail ?
  - Problematik
  - alter Zustand
- Lösungsansätze
- Details zur Ironport-Lösung
- Zukunft

ZENTRUM FÜR
INFORMATIONS
VERARBEITUNG

Was ist E-Mail ?

- ein Medium das wir alle kennen/benutzen
- häufig als "sicheres" Kommunikationsmedium angesehen

- aber ein sehr einfaches, unsicheres Protokoll (SMTP, Simple Mail Transfer Protokoll)
  - nicht sicher/geheim
  - fälschbar

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

E-Mail-Versand

- Client liefert bei SMTP-Server1 ein
  - Angabe:
    - Identifikation
      - HELO *rechnername* (je nach angesprochenem Server fälschbar)
    - Absender
      - MAIL FROM: <bundeskanzlerin@regierung.de> (fälschbar!)
    - Empfänger
      - RCPT TO: <bucher@uni-muenster.de>
    - Text (enthält Titel, scheinbaren Empfänger TO:..., usw.) (fälschbar!)
  - Server1 nimmt die Mail an und versucht sie zuzustellen
- Server1 sendet an SMTP-Server2 (uni-muenster.de)

Vertrauenswürdig ?

```
Received: from murder ([unix socket]) by zivstore02 (Cyrus v2.2.12-Invoca-RPM-2.2.12-3.RHEL4.1)
    with LMTPA; Wed, 26 Apr 2006 18:46:12 +0200X-Sieve: CMU Sieve 2.2
Received: from batch14.uni-muenster.de (BATCH14.UNI-MUENSTER.DE [128.176.188.112])by zivstore02
    (Postfix) with ESMTP id 68F131DC099for <bucher@zivstore02.uni-muenster.de>; Wed, 26 Apr 2006
    18:46:12 +0200 (CEST)
Received: by batch14.uni-muenster.de (Postfix)id B6245C43; Wed, 26 Apr 2006 18:44:49 +0200
    (MES)Delivered-To: bucher@uni-muenster.de
Received: from mailfilter1.uni-muenster.de (MAILFILTER1.UNI-MUENSTER.DE [128.176.188.130])by
    batch14.uni-muenster.de (Postfix) with ESMTP id 9BA57C34for <bucher@uni-muenster.de>; Wed, 26
    Apr 2006 18:44:49 +0200 (MES)
Received: from zivlnx07.uni-muenster.de (ZIVLNX07.UNI-MUENSTER.DE [128.176.188.154])by
    mailfilter1.uni-muenster.de (Symantec Mail Security) with ESMTP id C1B10400002for <bucher@uni-
    muenster.de>; Wed, 26 Apr 2006 18:46:11 +0200 (CEST)
Received: from mlurr (Z-s9-0-0-24-0-S1.gw10.tor1.rogerstelecom.net [206.186.248.26])by
    zivlnx07.uni-muenster.de (Postfix) with SMTP id 409637F83for <bucher@uni-muenster.de>; Wed, 26
    Apr 2006 18:46:10 +0200 (CEST)
From: "Mrs. Denira Wilkins" dw@yahoo.ca
Subject: Thornhill E-Games
To: bucher@uni-muenster.de
Reply-To: denirawilkins@yahoo.ca
Date: Wed, 26 Apr 2006 12:46:13 -0400

Thornhill E-games 2006,
...
```

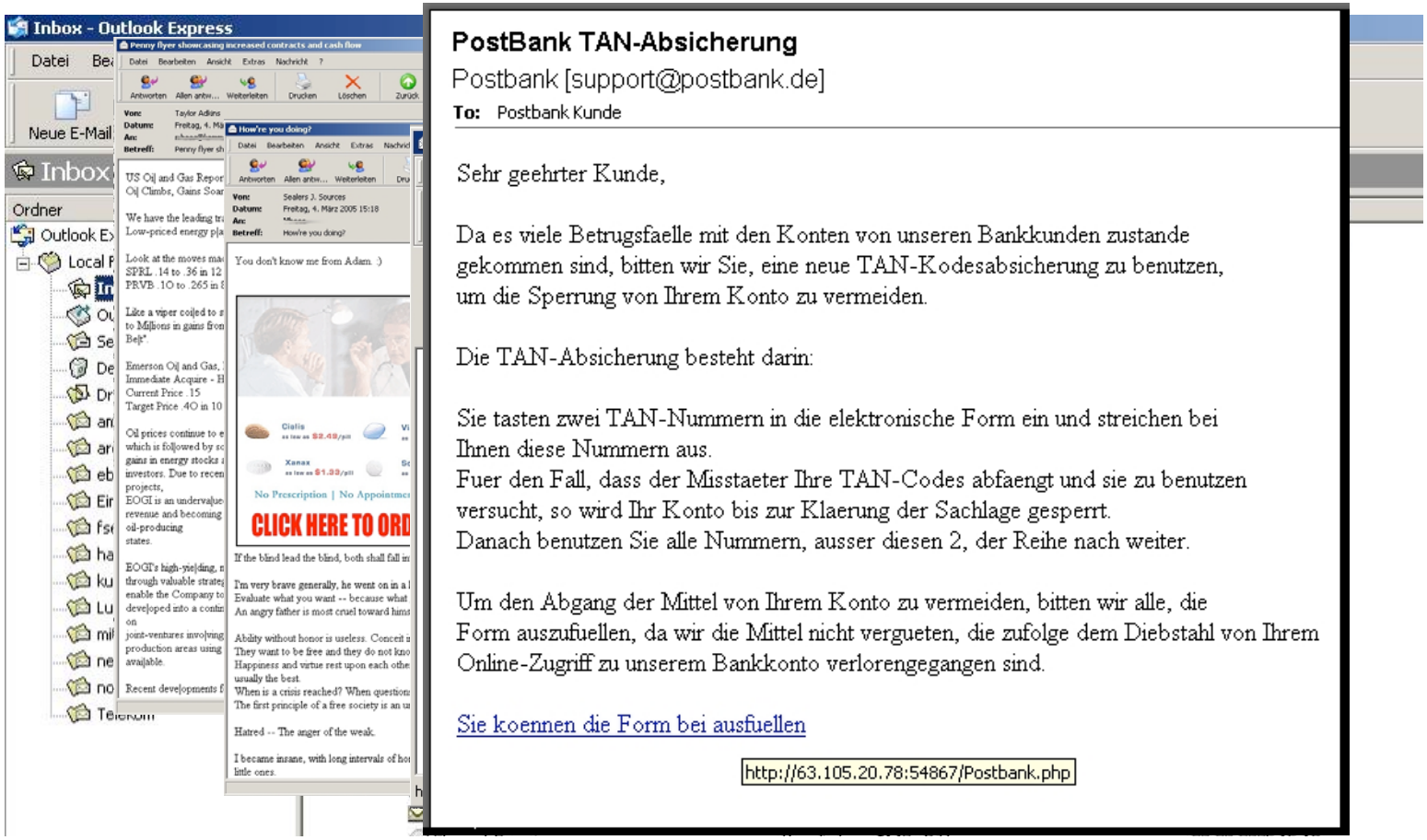
ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Problematiken

- SPAM
  - automatisierte Massensendung
  - unerwünschte Werbung
  - Betrugsversuche (Scam "Nigeria Connection, Phishing ...)
  - teilweise > 80% aller Mails
- Malware (Viren ,Würmer, Trojaner)
- DoS-Attacken (Denial of Service)
- Directory-Harvest-Attacks

ZENTRUM FÜR
INFORMATIONS
VERARBEITUNG

Problem: Der Posteingang



ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Momentaner Zustand

- Frontend MTAs (MailTransferAgent)
  - RedHat AS4 + postfix (MTA)
  - nehmen Mail für gültige *uni-muenster.de*-Adressen an
  - Scannen nach Viren und markieren SPAM
    - Virenscan: McAffee
    - SPAM: spamassassin (opensource)
  - haben keine (weiteren) Nutzerinformationen
- lokale Mailer
  - nehmen Mails von den Frontend-MTAs an
  - liefern in User-Mailboxen im DFS aus (AIX)

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

SPAM-Erkennung (alt)

- spamassassin
  - beruht auf einer großen Menge an Regeln (teilweise trainierbar/Bayes-Filter)
  - jede Regel gibt einen Score
  - Benutzertrainierter Filter (neuronales Netz) kombiniert die Scores zu einem Wert
  - Wert > Schwelle --> Mail ist Spam
  - Nachteile:
    - Erkennungsrate nur 30-50%, da nicht individuell trainiert.
    - muss bei neuen SPAM-Mustern neu trainiert werde

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Grenzen (Bsp.)

- Können Sie Folgendes lesen:

  Gmäeß eneir Sutide eneir elgnihcesn Uvinisterät, ist es nchit witihcg in wlecehr Rneflogheie die Bstachuebn in eneim Wrot snid, das ezniige was wcthiig ist, ist daß der estre und der leztte Bstabchue an der ritihcegn Pstoiion snid.

  Der Rset knan ein ttoaelr Bsinöldn sien, tedztorm knan man ihn onhe Pemoblre lseen.

- Spamassassin hat Probleme mit solcher SPAM

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Neue Lösungen

- Ziele (ursprünglich nur auf SPAM bezogen):
  - sehr gute SPAM-Erkennung (unabhängig vom Nutzerprofil !)
  - extrem niedrige False-Positiv-Rate
    - =fälschlicherweise als SPAM erkannte Mails
    - dadurch kann Löschung ohne Kontrolle empfohlen werden
  - Mandantenfähigkeit
    - individuelle Nutzerentscheidung bzgl. SPAM-Behandlung (markieren/löschen)
- Erprobung zweier Appliances

  Symantec 8260 (erster Test)

  Ironport C600

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Ergebnisse

- SPAM-Erkennung und false-positive: OK
- Symantec Appliance fehlt die Mandantenfähigkeit in dem von uns geforderten Maßtab (>50k Nutzer)
- Ironport (und teilweise auch Symantec) bietet zusätzliche Features bzgl. SPAM-, Virenerkennung und Serversicherheit

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Details zur Ironport C600 HW

- DELL 2HE Dual Xeon
  - 4x 146GB SCSI-Disk, RAID 10
    - 70GB Queue Kapazität
    - 110GB für Logs, Backups, Konfiguration ...
  - 2 x GB-Ethernet + 1 10/100BaseT
  - Hotplug Powersupplies
  - für Sites >5000 User
- Vorschlag für Uni Münster:
  - 1 C600 + 1 C600 (Hot-Standby)

ZENTRUM FÜR
INFORMATIONS
VERARBEITUNG

Ironport SW

- Betriebsystem AsyncOS
  - basiert auf BSD-Kernel
  - speziell auf MTA-Funktionalitäten optimiert
  - spezieller Scheduler
  - eigenes Fielsystem für Mailqueues
- Hochperformant im MTA-Bereich
  - 10.000 gleichzeitige smtp-Connections

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

SPAM-Erkennung

- 2 Stufig
  - SenderBase Reputation Service (SBRS)
    - beeinflußt die Verbindungsaufnahme auf IP-Ebene
  - Brightmail Antispam
    - Bewertet angenommene Emails

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

SBRS

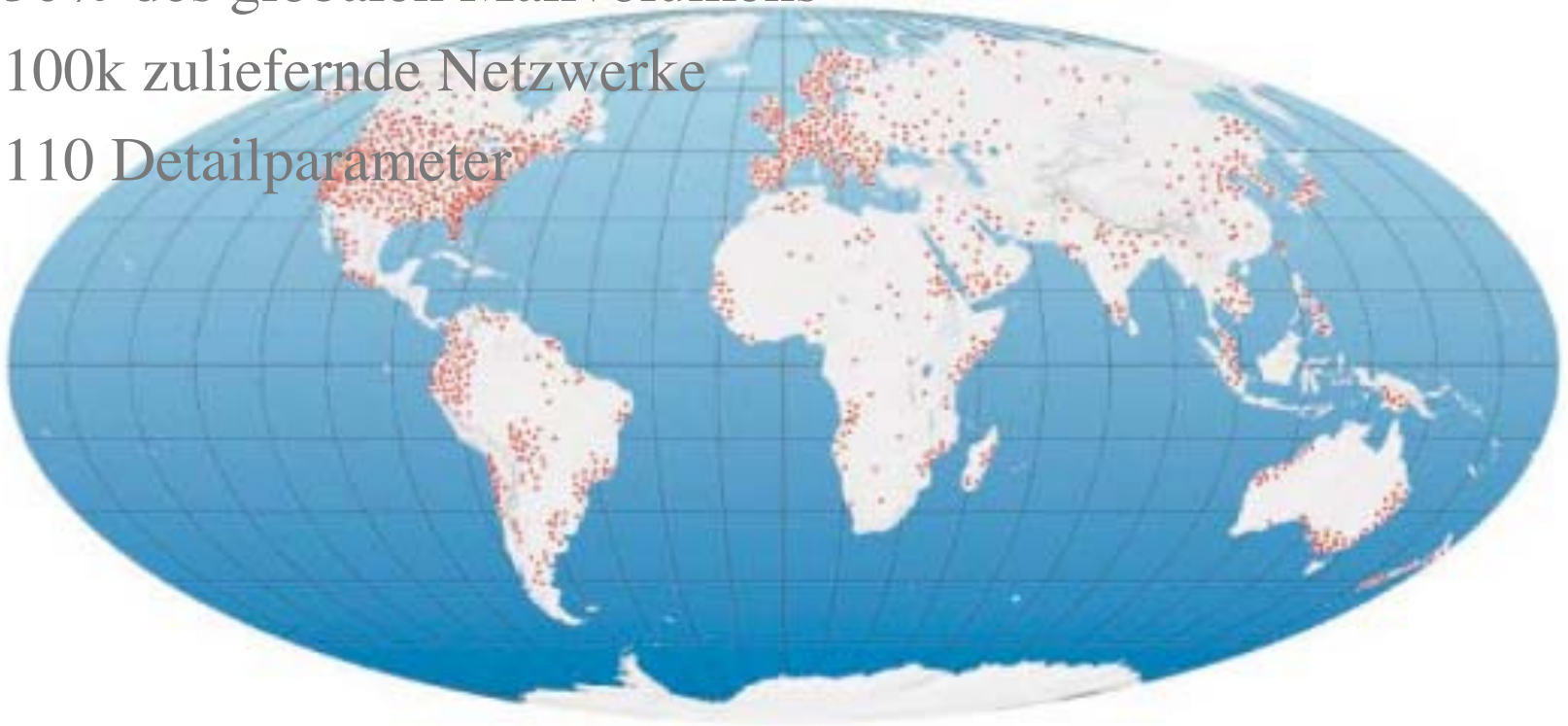
- IPs erhalten von Ironport einen SB-Score zwischen -10 ... 10
  - -10 : "übelster Spammer"
  - 10 : "absolut vertrauenswürdig"
- Entscheidung bei der Verbindungsaufnahme
- intelligentes Blacklisting
  - Blocking und throttling in Abhängigkeit vom SB-Score möglich
  - weitere Einschränkungen/Tests einstellbar

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

SBRS

Beobachtung und Bewertung des weltweiten Email-Verkehrs

- 30% des globalen Mailvolumens
- 100k zuliefernde Netzwerke
- 110 Detailparameter



ZENTRUM FÜR INFORMATIONS VERARBEITUNG

SenderBase-Score

Spam, phishing, virus reports

Complaint Reports

SpamCop, SpamHaus (SBL), NJABL, Bonded Sender

IP Blacklists & Whitelists

Domain Blacklists & Safelists

Spamvertized URLs, phishing URLs, spyware sites

SpamCop, ISPs, customer contributions

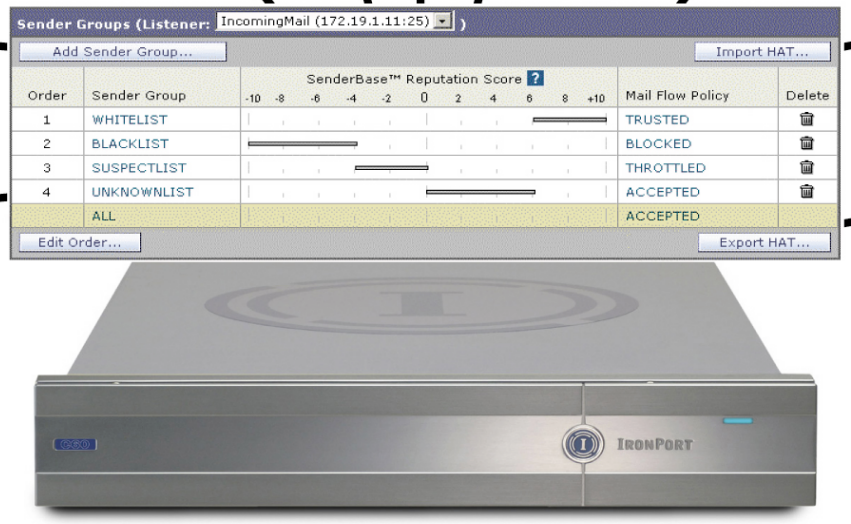
Spam Traps

Compromised Host Lists

SORBS, OPM, DSBL

Message size, attachment volume, attachment types, URLs, host names

Message Composition Data



Web site Composition Data

Downloaded files, linking URLs, threat heuristics

Global Volume Data

Over 100,000 organizations, email traffic, web traffic

Other Data

Fortune 1000, length of sending history, location, where the domain is hosted, how long has it been registered, how long has the site been up

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Reaktionen auf SB-Score

- Differenzierte Reaktionen in verschiedenen Gruppen möglich
  - Abblocken
  - Bandbreitenbegrenzung
  - Tests auf Empfängeranzahl, Header etc.
  - Mail Flow Policies individuell konfigurierbar
- Konfiguration über HostAccessTable (HAT)

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

HAT

Sender Groups (Listener: InOutMail (128.176.188.219:25) **)**

Add Sender Group... | Import HAT...

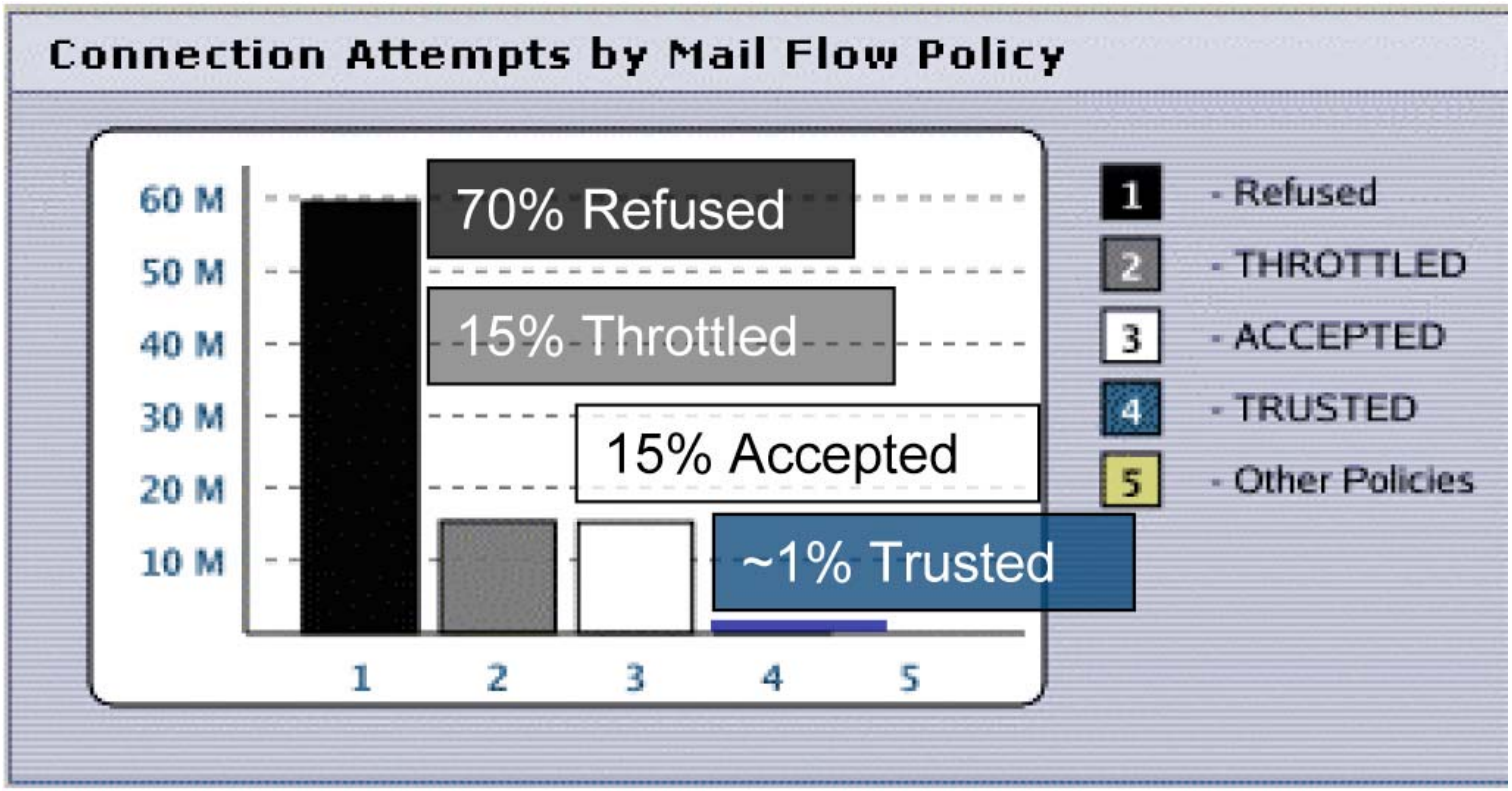
Order	Sender Group	SenderBase™ Reputation Score ? -10 -8 -6 -4 -2 0 2 4 6 8 +10	Mail Flow Policy	Delete
1	RELAYLIST		RELAYED	
2	WHITELIST		TRUSTED	
3	BLACKLIST		BLOCKED	
4	VERYSUSPECTLIST		HARDTHROTTLED	
5	SUSPECTLIST		THROTTLED	
6	UNKNOWNLIST		ACCEPTED	
	ALL		ACCEPTED	

Edit Order... | Export HAT...

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Effizienz

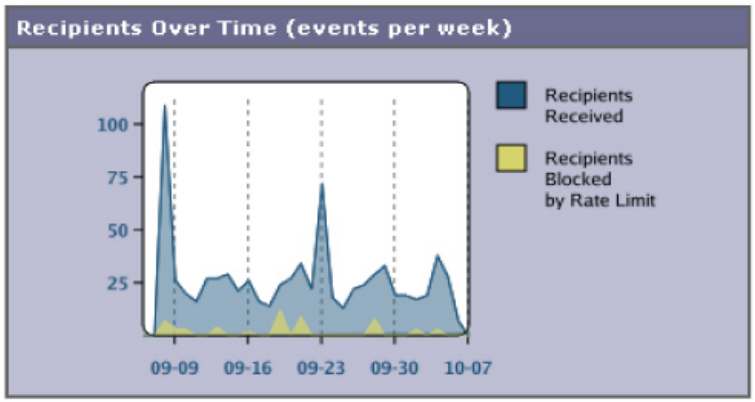
- Fallbeispiel ISP "Adelphia"

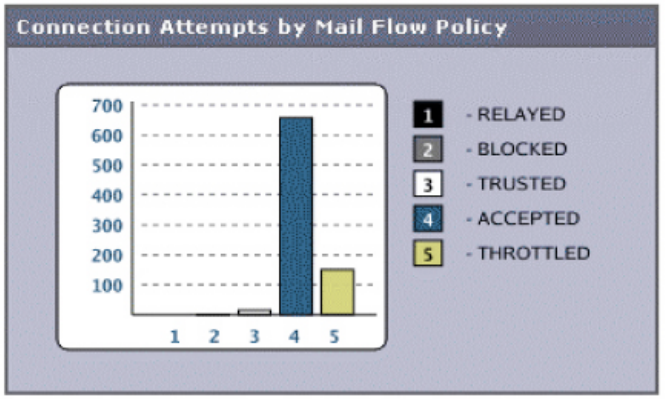


ZENTRUM FÜR
INFORMATIONS
VERARBEITUNG

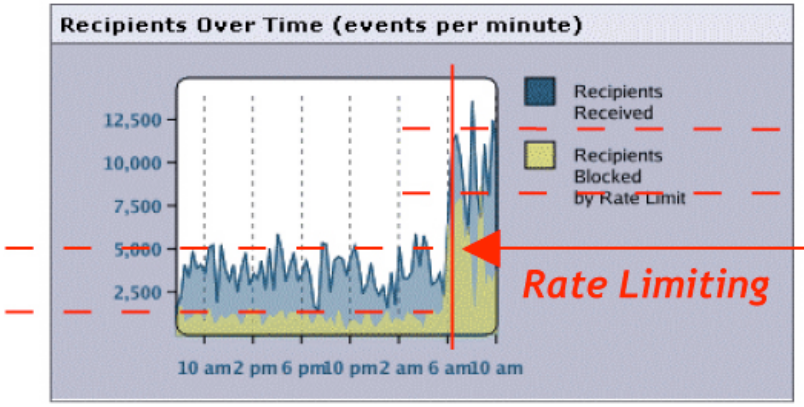
DOS-Schutz

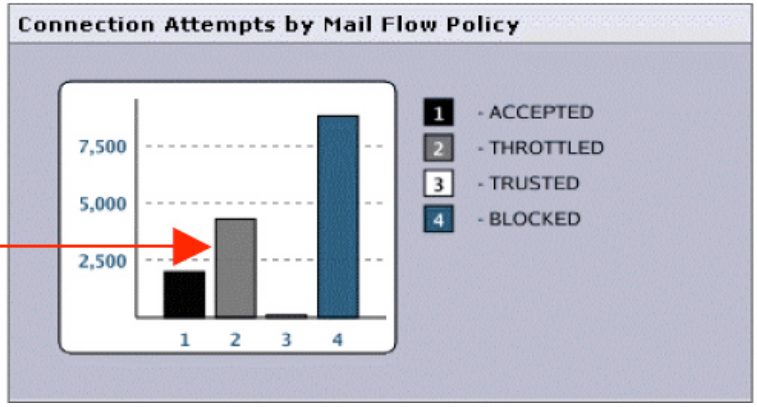
Standardbetrieb





Anomalie um 6:00 Uhr





ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Brightmail Antispam

- Setzt nach dem Empfang der Email ein
- Klassifiziert nach verschiedenen Verfahren
- gute Erkennungsrate (90-95%)
- extrem geringe Fehlerrate/ false Positive:

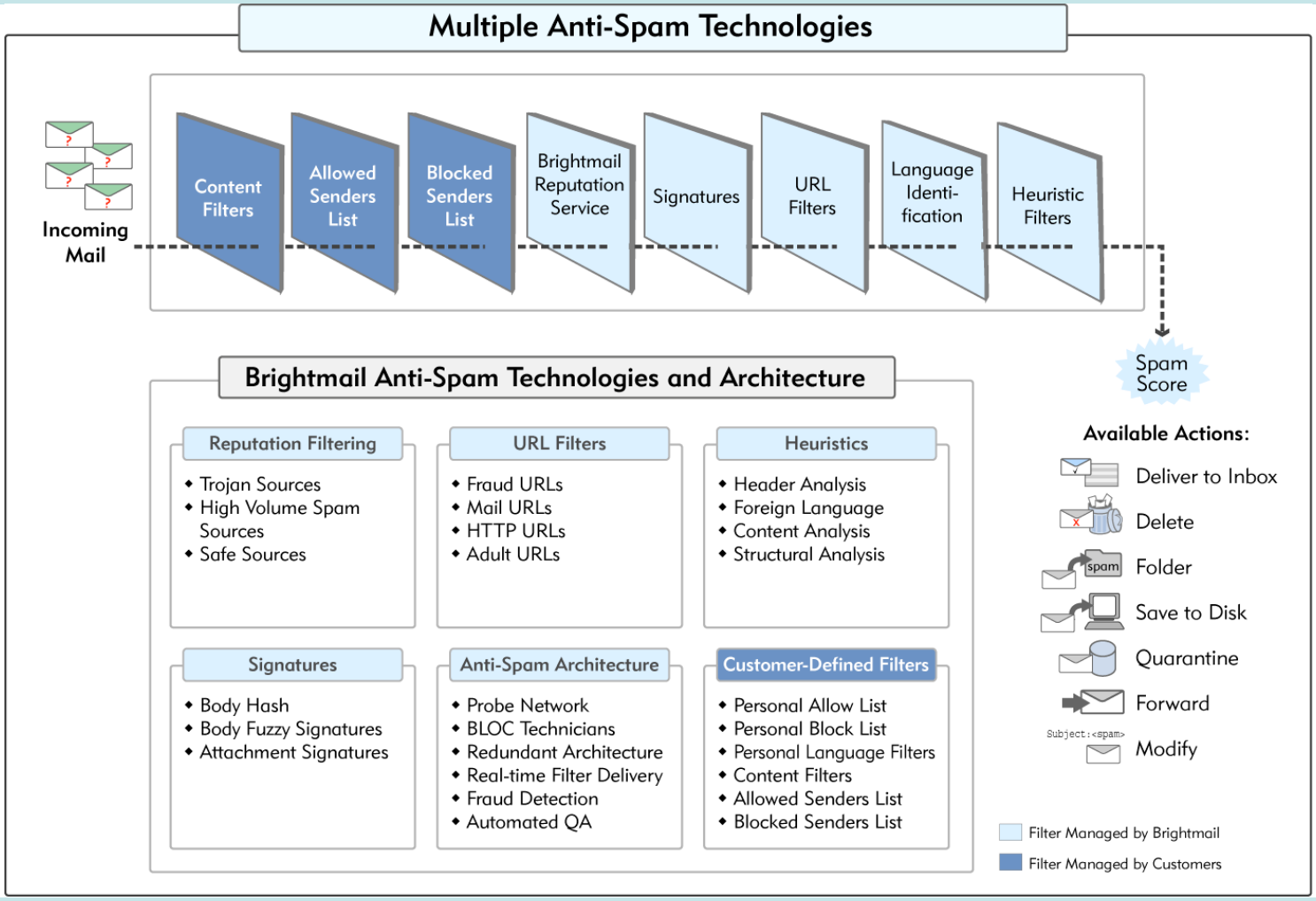
1:1.000.000 !!

d.h. 1 fälschlicherweise als SPAM erkannte Mail bei 1.000.000

Empfehlung an den Nutzer: SPAM ohne manuelle Kontrolle löschen !

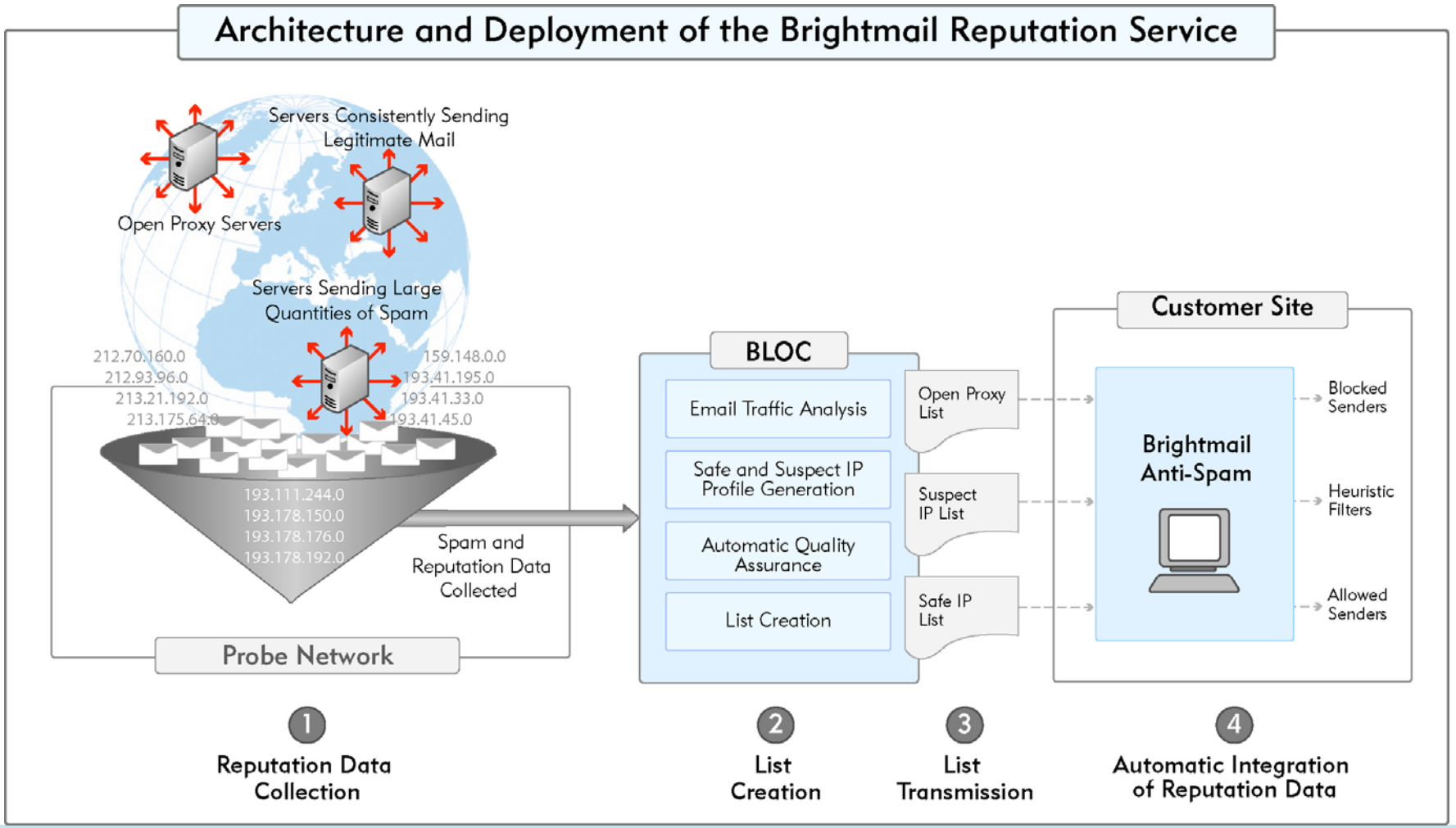
ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Details



ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Reputationsfilter



ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Rechtliches

- SBRS:
  - mögliche Effekte:
    - Verbindung wird abgebrochen
    - Mail wird nicht angenommen
    - Bandbreite wird begrenzt
  - Unbedenklich, da Mail nicht (vollständig) angenommen wurde
- Brigthmail Antispam
  - mögliche Effekte:
    - Markierung durch zusätzlichen Header
    - Löschung
  - Markierung unbedenklich, Löschung nur bei ausdrücklichem Nutzerwillen

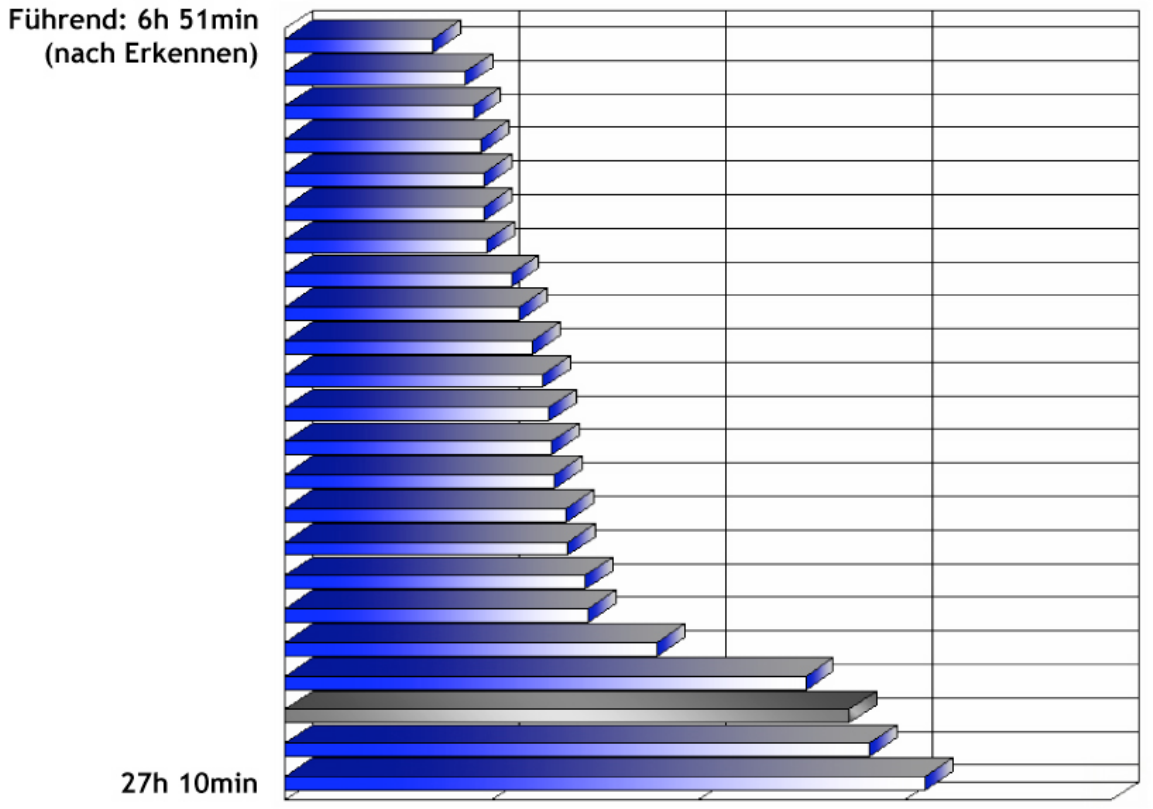
ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Zusätzliche Features

- Virenscanner (Sophos)
- "präventiver" Virenschutz
  - Virus Outbreak Filter (siehe nächste Folien)
- Verwaltung virtueller Domänen
  - Bsp.: Trennung von normaler Mail und Bounces zur Vermeidung von Blacklisting
- ...

Zeitproblem

durchschnittliche Dauer bis zur Verfügbarkeit einer Virus-Signatur



Quelle: AV-Test.org Research Group

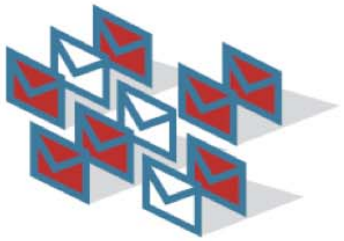
ZENTRUM FÜR
INFORMATIONS
VERARBEITUNG

Lösung

- "unscharfer" Virenfilter
  - basiert auf Beobachtung des Mailverkehrs und Erkennung von Anomalien und verdächtiger Mails
  - gesteuert durch Ironport Threat Operation Center
- Dynamische Quarantäne
  - Ausliefern unverdächtiger Mails bei neuen Informationen
  - kein Verwaltungsaufwand

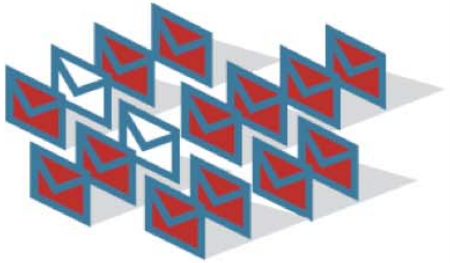
ZENTRUM FÜR INFORMATIONS VERARBEITUNG

VirusOutbreakFilter



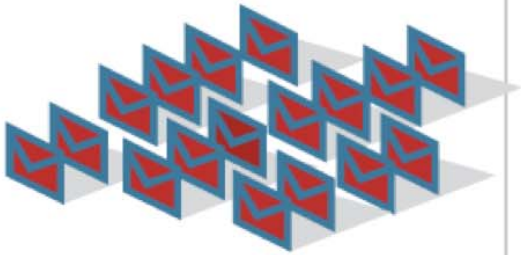
T = 0

> zip (exe) files



T = 5 Min.

> zip (exe) files
> Größe: 50 bis 55 KB



T = 10 Min.

> zip (exe) files
> Größe: 50 bis 55KB
> z.B. “Price” im
> Dateinamen

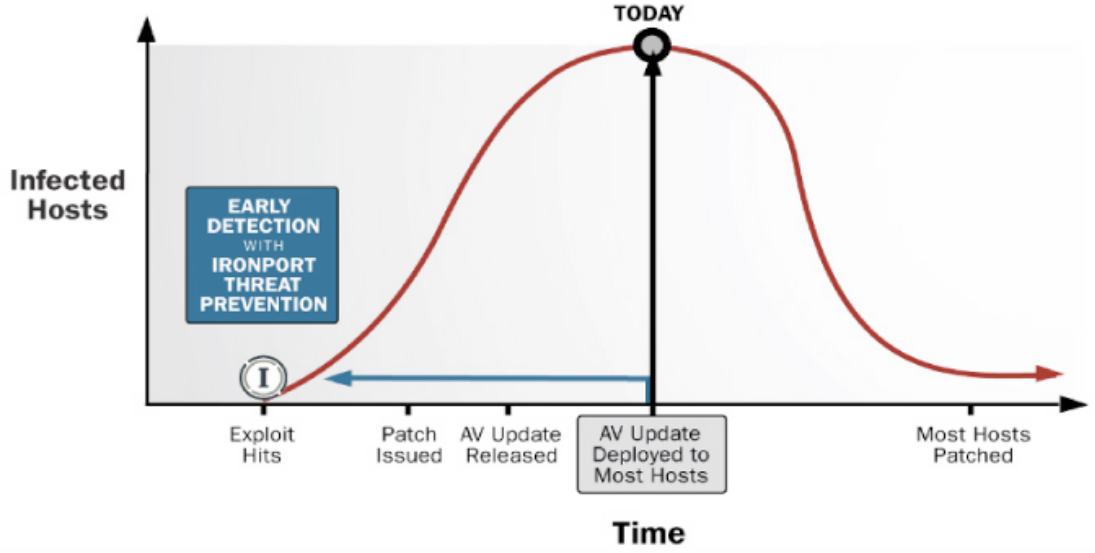
Nachrichten gescanned & gelöscht

T = 8 Std.

> Freigabe der Nachricht, sobald Signatur verfügbar

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Zeitvorteil



VIRUS NAME	IRONPORT'S EARLY DETECTION ADVANTAGE
Multiple "Bagle" Variants	DETECTED **41:43 hours** BEFORE ANY OTHER TECHNOLOGY
"MyTob.EC"	DETECTED **15:22 hours** BEFORE ANY OTHER TECHNOLOGY
"Sober.J"	DETECTED **10:23 hours** BEFORE ANY OTHER TECHNOLOGY
"Zotob-C"	DETECTED **2:51 hours** BEFORE ANY OTHER TECHNOLOGY

ZENTRUM FÜR INFORMATIONS VERARBEITUNG

Zusammenfassung/Ausblick

- Lösung/Entschärfung der SPAM-Problematik in Aussicht
  - Symantec 8260 in (Test-)Betrieb seit Mitte Mai
    - zwischen Frontend-MTA und lokalen Mailern
    - nur Markierung
    - positive Rückmeldungen
- Ironport als Lösung für Münster angestrebt
  - Frontend-MTA (löst die Scan-Mailer ab)
  - Anbindung an LDAP zur Mandantenfähigkeit
- Verhandlung bzgl. Landeslizenz Ironport
  - Uni Bonn führt die Verhandlungen