

# Emailfilter

**Schutz vor unerwünschten Emails**  
**(Unix, MS-Windows, Outlook, gmx.de, procmail, ...)**

Bert Schöneich

Februar 2002

## Inhalt (I)

1. Erklärung zur Verwendung realer Beispiele
2. Zweck des Filterns
  1. Beispiele unerwünschter Emails
  2. SPAM Emails - möglicher Inhalt
  3. Was ist "SPAM"?
3. Was bedeutet "Filtern von Emails"?
4. Wo wird gefiltert?
5. DESY Zeuthen - zentrales Filtern für alle?
  1. DESY Zeuthen
  2. CERN
6. DESY Zeuthen – der einzelne Nutzer

## Inhalt (II)

7. **procmail - das Filterprogramm unter UNIX**
  1. procmail – Beispiele
  2. Erfahrungen mit .procmail
  3. Einrichten von .procmail
  4. procmail und AFS
8. **Filtern auf dem eigenen PC**
  1. Anwendung am Beispiel von Outlook Express
  2. Möglichkeiten (Bedingungen, Aktionen)
  3. Erfahrungen
9. **Provider – private Anbieter von Emaildiensten**
  1. Provider – Beispiel gmx.de
  2. Erfahrungen mit Providern



## Inhalt (III)

10. **Erfahrungen**
  1. Gefahren beim Filtern
  2. Wohin mit dem Abfall?
  3. Wie und wann filtern?
  4. Wie mit dem Filtern beginnen?
  5. Signaturen unerwünschter Emails
  6. Reaktion auf unerwünschte Emails
11. **Zusammenfassung:**
  1. Vorteile
  2. Nachteile
12. **Literatur**



# 1. Erklärung zur Verwendung realer Beispiele

## 1. Erklärung zur Verwendung realer Beispiele

In dem folgenden Vortrag werden reale Beispiele verwendet, um das Filtern von Emails praxisnah erläutern zu können.

Diese Beispiele sollen es ermöglichen, schnell und sicher eigene Filter einzusetzen.

Diese Beispiele und die in ihnen notwendigerweise auftauchenden Begriffe solle in keiner Weise einzelne Personen oder Gruppen beleidigen oder anderweitig angreifen.

## 2. Zweck des Filterns

### 2.0 Zweck des Filterns

- Vermeiden des Empfanges unerwünschter Emails
    - Absender
    - Inhalt (Werbung, unerwünschte Angebote)
    - Massensendung (Kettenbriefe) } **SPAM**
  - Kostenreduzierung
    - Übertragung großer Emails im privaten Bereich (online Kosten)
  - Schutz des PC's / der eigenen Daten
    - Infektionsverdacht der Email (Viren, trojanische Pferde)
- 
- Sortieren erwünschter Emails
    - sofortige Ablage in gewünschte Ordner
  - Weiterleiten ausgewählter Emails
    - andere Empfänger, FAX, Programme

## 2.1.1 Beispiele unerwünschter Emails

(an bert.schoeneich@ifh.de vom 1.2.2002 – 11.2.2002)

!	📧	📧	From	Subject	Received
			ashcraft@hino	We Guarantee to add 1 to 3 inches to Peri...	01.02.02 04:05
			Serapion	Can you measure up?	01.02.02 12:31
			turtledpv@mailhub.smar...	Exciting New Home Based Business for Y...	02.02.02 10:25
			alphonso69	SUPER BOWL SUPER CASH GIVEAWAY!	02.02.02 11:15
			PROwSE	Seems like old times!!!FSFQEE	03.02.02 03:24
			netcashfreedom@yahoo...	The little guy gets screwed again	04.02.02 21:39
			safelyvideo@hotmail.com	*Kid's AntiAbduction/AntiBully/SelfDfense ...	05.02.02 22:51
			safelyvideo@hotmail.com	*Kid's AntiAbduction/AntiBully/SelfDfense ...	06.02.02 02:51
			541231@art.com.br	The greatest risk is not taking on...	07.02.02 15:30
			alphonso69	FREE CASH & TICKETS TO TH...	07.02.02 17:01
			Jan A. Loeffler	Dringend benötigte Rückenmarksp...	07.02.02 23:21
			Oydsqmqsyf@rubiko...	MAKE FREE DVD MOVIES!!!	08.02.02 00:03
			Enlighten yourself	ADV: INTENSE ERECTIONS, SA...	08.02.02 08:18
			hfluiah52@yahoo.com	Start a \$5000/mon home biz by fil...	08.02.02 13:37
			cucumberman@gmx.de	Lose 30 Pounds In 30 Days, Guar...	08.02.02 15:17
			Bob	I'll give you \$100 to read this em...	08.02.02 15:19
			427851@iway.net	Work From Home - Email Broadca...	09.02.02 04:46
			photoboo702261@m...	2001 Statistics Revealed	10.02.02 06:09
			bassnfool411217@al...	2001 Statistics Revealed	10.02.02 07:25
			Cynthiena@yahoo.com	Please confirm Your order# ...	10.02.02 11:12
			intertuben@manage...	ok	11.02.02 01:37
			admin@chancellorsvillem...	Be a part of history	11.02.02 02:59
			best.defense101@la...	RE: We Are Now Accepting Posit...	11.02.02 03:13
			best.defense101@la...	RE: We Are Now Accepting Posit...	11.02.02 03:13
			246810@ev1.net	Fire Your Boss and Work For Yourself	11.02.02 05:42
			gtabsott724387@aol...	Accept Credit Cards	11.02.02 08:39
			gtac30463345@aol....	Ecommerce Exposition	11.02.02 08:45

26/10/2007

Bert Schöneich DESY Zeuthen



9

## 2.1.2 Beispiele unerwünschter Emails

(an bert.schoeneich@gmx.de vom 1.2.2002 – 15.2.2002)

!	📧	📧	From	Subject	Received
			Bert Schoeneich	test, bleibt im junk-folder	15.12.01 12:25
			tamara-24@onlinehome.de	Wie nun treffen ?	12.02.02 07:57
			free-sms.de Newsletter	--> I Love You - Valentins-Special bei free-sms.de <--	12.02.02 15:49
			FUN-News	Schon wieder Sport im Fernsehen?	13.02.02 13:32
			Fischabenteurer	Treffpunkt für Sportangler!	14.02.02 09:26
			tamara-26@onlinehome.de	Wie nun treffen ?	15.02.02 09:26

Gleicher Inhalt, andere Adresse, um Filter zu umgehen!

26/10/2007

Bert Schöneich DESY Zeuthen



10

## 2.2 SPAM Emails - möglicher Inhalt

**Wikinger** Spam, Spam, Spam, Spam, Spam ... lovely Spam, wonderful Spam ...



**Kellnerin** Ruhe! Ruhe!

## (2.2 SPAM Emails - möglicher Inhalt)

- Medikamente (wirkungsvolle)
- Geld / Kredite (hoch und runter)
- Mietwagen (preiswerte)
- Handy (kostenlose)
- Immobilien (günstige)
- Haar (volles)
- Körpergewicht (geringes)
- Emaillisten (lange)
- Online Geschäfte (einträgliche)
- Geld verdienen von zu Hause (schnell und viel)
- Kodierung Kabelfernsehen umgehen (einfach)
- Ein- und Auswanderung (sofort)
- ...
- Pornografie (...)

## 2.3 Was ist "SPAM"?

Anti-Spam

### Virtuelles Dosenfleisch

**"SPAM": Spiced Pork and Ham**

Noch sind es wenige schwarze Schafe, die unverlangt Werbung per E-Mail versenden, doch bald soll die schöne neue Werbewelt allen Werbetreibenden offenstehen.



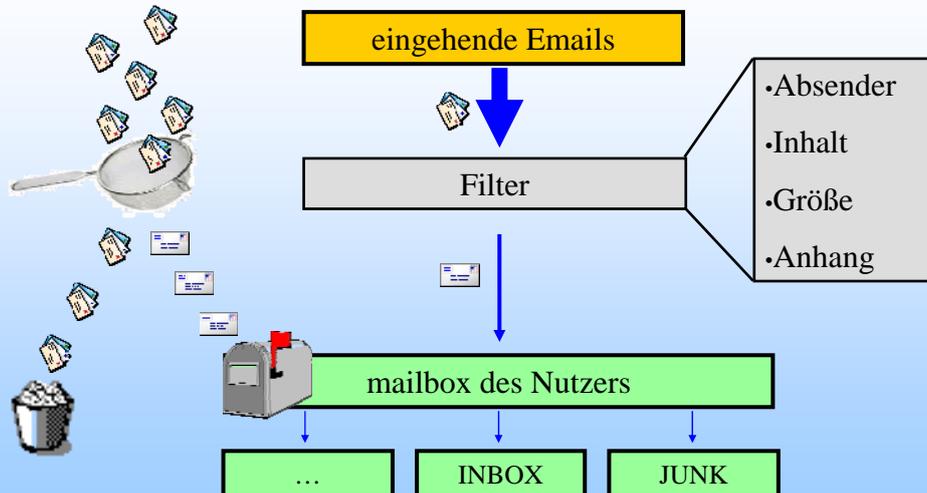
Davon träumt eine ganze Branche: **Werbung per E-Mail**. Einmal geschrieben, läßt sich die Kaufbotschaft millionenfach mit einem Knopfdruck versenden. Den User erreicht E-Post schnell und preiswert, und vor allen Dingen: Er kann sich gegen den Erhalt beim Abrufen der Post nicht wehren.

#### Was heißt Spam?

"SPAM" ist der Fachausdruck für die Überflutung mit Neuigkeiten, die Keinen interessieren, benannt nach einem Dosenfleisch, das vornehmlich in den USA und Großbritannien verkauft wird. Das Fleisch spielte in vielen **Monty-Python-Sketchen** eine Rolle. In einem Film sang eine Gruppe Wikinger "Spam, Spam, Spam,...", wodurch sämtliche Konversation im Raum erstickt wurde. Ähnlich sehen Experten die Gefahr durch Werbemails; durch die Unmenge an Post könnten die Mailserver im Internet **vollkommen überlastet** werden und die wichtigen Nachrichten ihre Empfänger nur mit Mühe erreichen.

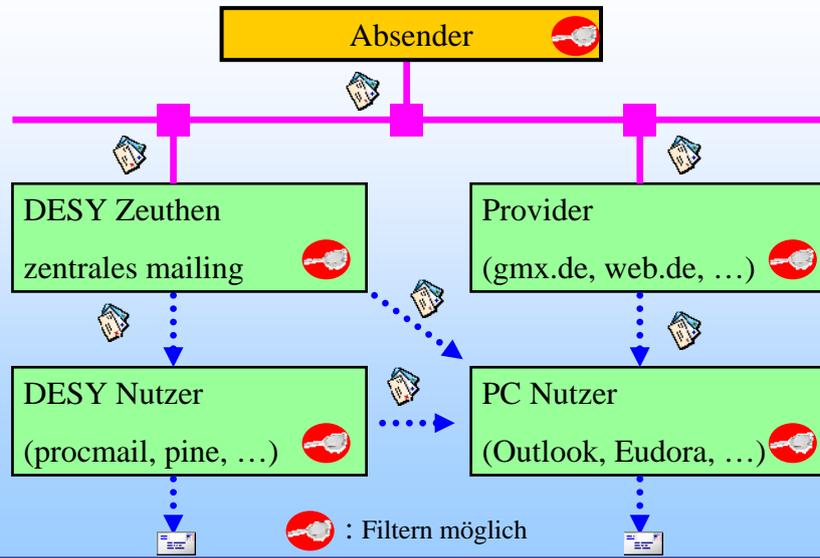
## 3. Was bedeutet "Filtern von Emails"?

### 3. Was bedeutet "Filtern von Emails"?



### 4. Wo wird gefiltert?

## 4. Wo wird gefiltert?



26/10/2007

Bert Schöneich DESY Zeuthen



17

## 5. DESY Zeuthen zentrales Filtern?

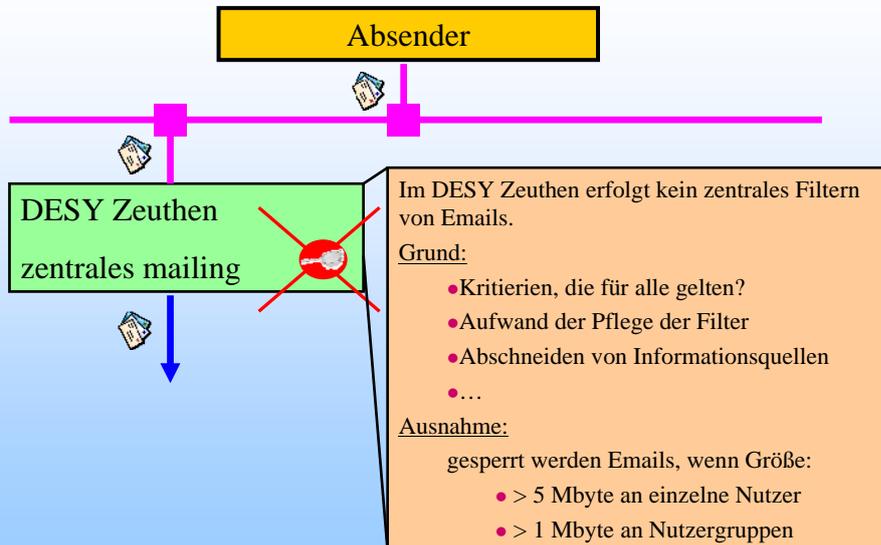
26/10/2007

Bert Schöneich DESY Zeuthen



18

## 5.1 DESY Zeuthen



## 5.1 DESY Zeuthen

notwendige Ergänzung nach dem Vortrag vom 26.2.2002 im DESY Zeuthen:

### **DESY Zeuthen zentrales Filtern:**

Die Emails des Nutzers, die über den Microsoft Exchange-Server (NTMail) kommen, werden gefiltert:

- auf Viren  
(Folgende Attachments werden durch den Virenschanner geblockt: .com, .scr, .lnk, .pif, das heißt, die Email kommt durch, allerdings ohne Anhang. Der Nutzer erhält eine Mitteilung darüber.)
- an Hand einer SPAM-Liste

Es ist allerdings weder auf dem web-Seiten noch an anderer Stelle eine Information darüber zu finden, weder über die Tatsache das gefiltert wird, noch worauf gefiltert wird (auch keine Liste der "überwachten" SPAM-Absender).

## 5.2 CERN

### **CERN:**

Es werden alle (!) Emails mit einer Absenderadresse aus der folgenden Liste (insgesamt zur Zeit 945 Einträge) abgewiesen:

123-computer.com  
13net.com  
141.com  
163.net  
18andhorny.com  
1adultsextoystore.com  
1mallonline.com  
1stinternet.net  
2-cool.com  
centurymarketing.net  
2ndincome.com  
2sexy.com  
411forsex.com  
...

funmail.co.uk  
funtv.com  
gln.com  
gadens.com.au  
garlock.com  
gatenet.net  
generalmedia.com  
genie.com  
geocities.com  
get.topica.com  
getbuzy.com  
getnet.it  
giddyupwoe.com  
...

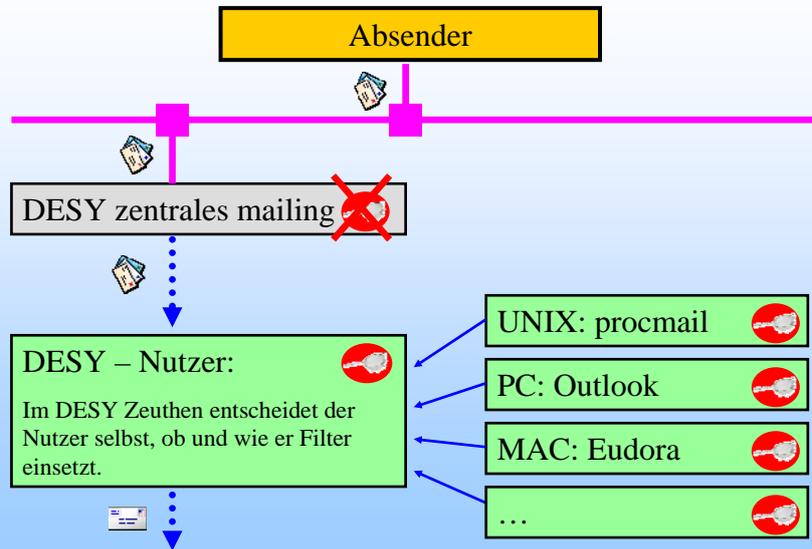
netblast.com  
netcene.com  
netexecutive.com  
netland.com.br  
netlane.com  
netlimit.com  
netpix.com  
netroplex.com  
netsvoice.com  
netvigator.com  
newwest.com  
neworleans.org  
newsround.com  
...



# 6. DESY Zeuthen der einzelne Nutzer



## 6. DESY Zeuthen – der einzelne Nutzer



26/10/2007

Bert Schöneich DESY Zeuthen



23

## 7. procmail das Filterprogramm unter UNIX

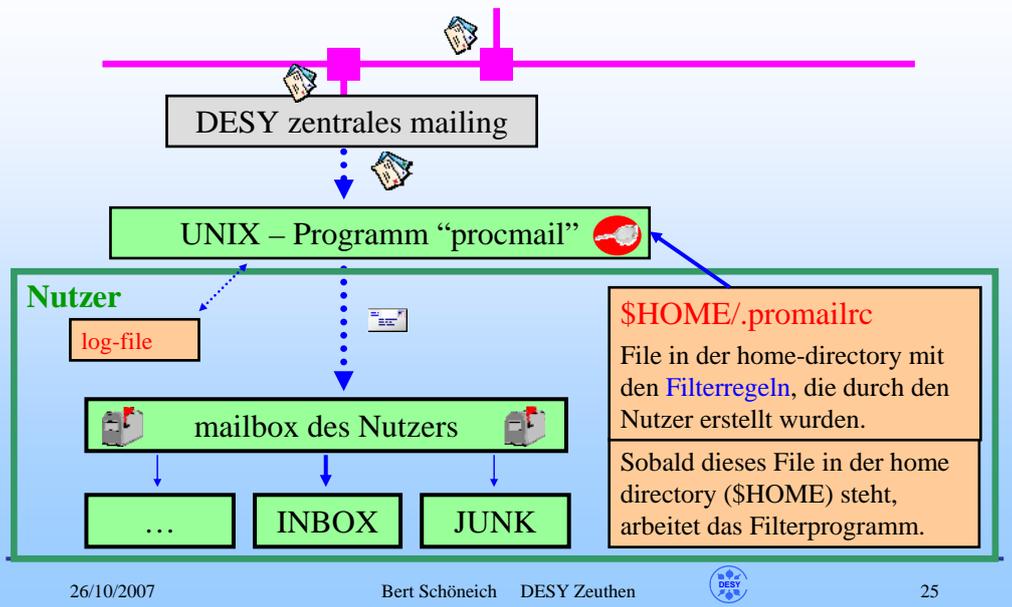
26/10/2007

Bert Schöneich DESY Zeuthen

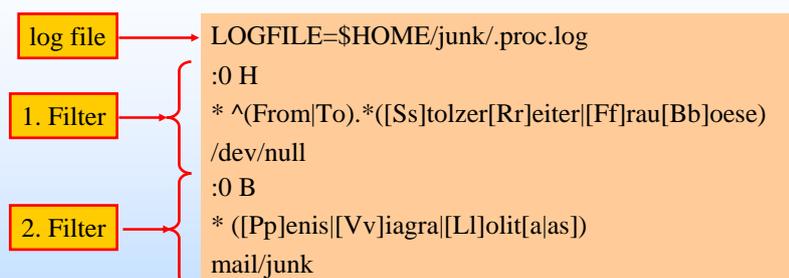


24

## 7. procmail - das Filterprogramm unter UNIX

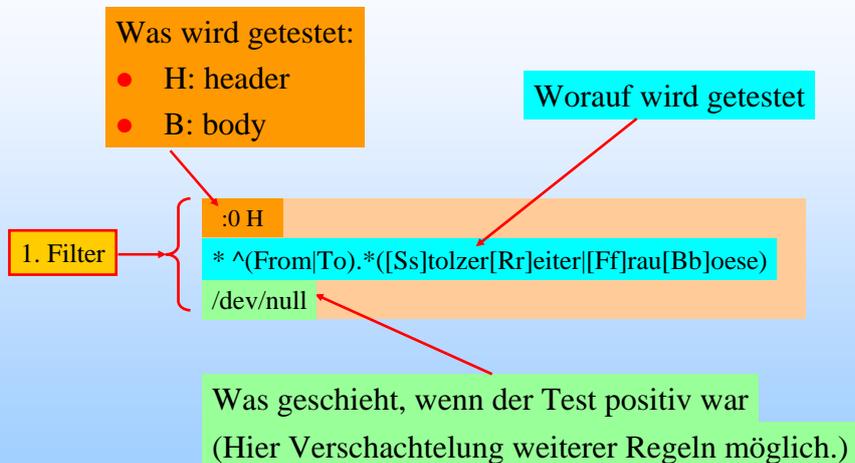


### 7.1.1 procmail – Beispiele



**ACHTUNG:**  
 Die Reihenfolge der Regeln (Filter) ist wichtig!  
 Eine Email, die durch die erste Regel verworfen wurde, wird in den folgenden Regeln nicht mehr bearbeitet!

## 7.1.2 procmail – Beispiele



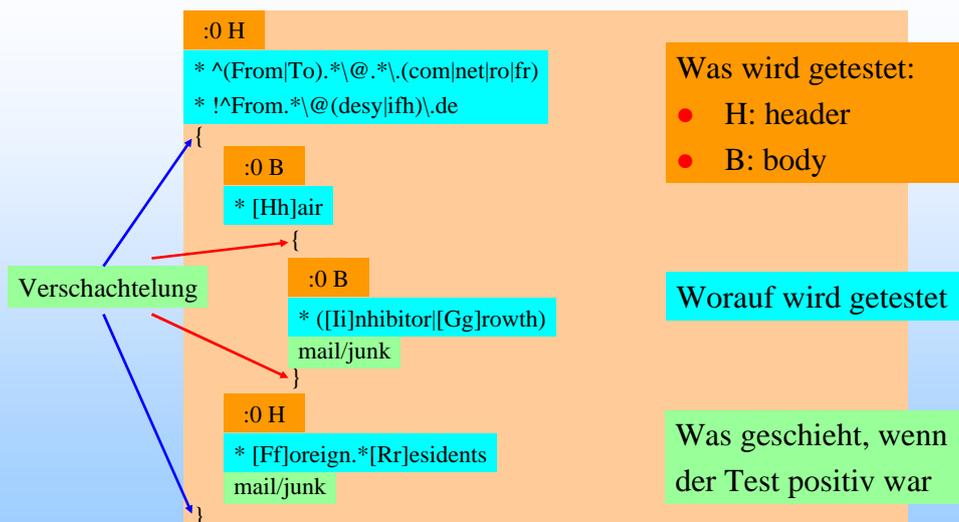
26/10/2007

Bert Schöneich DESY Zeuthen



27

## 7.1.3 procmail – Beispiele



26/10/2007

Bert Schöneich DESY Zeuthen



28

## 7.2.1 Erfahrungen mit procmail

### Vorteile:

- sehr mächtiges Werkzeug
- sehr fein abstimmbare Filterregeln
- “alles möglich” – Vorteil (“Briefverteileramt”)
- arbeitet problemlos im Hintergrund (“set it and forget it”)

### Nachteile:

- Programmiererfahrung allgemeiner Art notwendig - nichts für Laien
- “alles möglich” – Nachteil
- empfindlich gegen Fehlprogrammierung
- keine Fehlermeldung bei falscher Programmierung
- intensives Testen neuer Filterregeln notwendig (gilt immer!)

## 7.2.2 Erfahrungen mit procmail

### Empfehlung 1:

- procmail sollte der erste Emailfilter eines erfahrenen Nutzers am DESY Zeuthen sein. (Achtung bei AFS!)

### Empfehlung 2:

Das File ‘.promailrc’ gegen alle (!) lese/schreib schützen:

```
-rw----- 1 schoene rz      1280 Dec 21 15:17 .procmailrc
```

### Empfehlung 3:

```
~schoene/.procmailrc.example
```

## 7.3 Einrichten von procmail

mit dem Beispielfile: `~schoene/.procmailrc.example`

1. pine: mailfolder "junk" anlegen (mail/junk)
2. `>cp ~schoene/.procmailrc.example .procmailrc`
3. `>chmod 600 .procmailrc`

**Das funktioniert so nur, wenn die eigene home-Directory im NFS-Filespace ist!**  
(Nicht im AFS, siehe nächste Folie.)

**Auf eigene Gefahr!**

## 7.4 procmail und AFS

**Wolfgang Friebe** hat unter

<http://www-zeuthen.desy.de/computing/services/Mail/mailservice.html>

alles zu mail zusammengefaßt.

### Mail filtering und AFS:

If your home directory is in AFS space (starts with /afs/) then the usage of .procmailrc is more complicated.

This config file has then to be in the ~/public directory and a link from your homedir has to be made to this file.

This is achieved by:

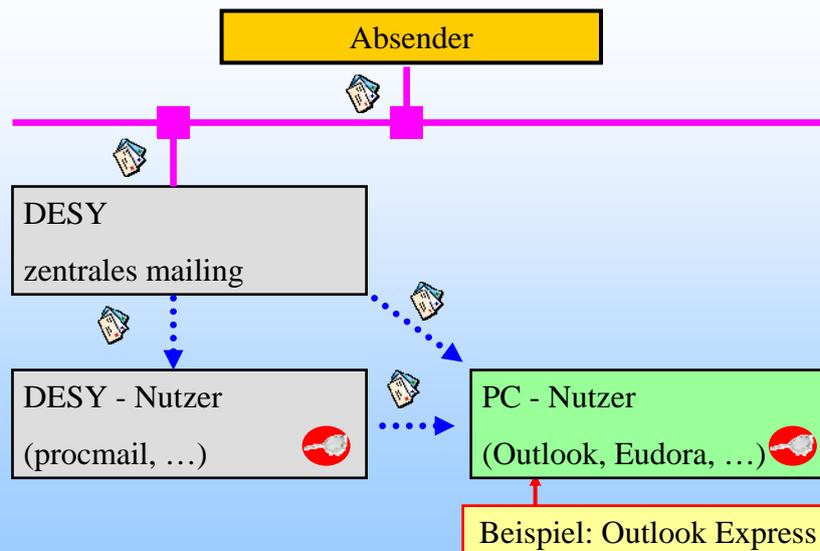
```
mv ~/.procmailrc ~/public
```

```
ln -s ~/public/.procmailrc ~/
```

In addition you have to ensure that all write operations are not using AFS file space. That is most easily achieved by moving the directory containing your mail folders into NFS space.

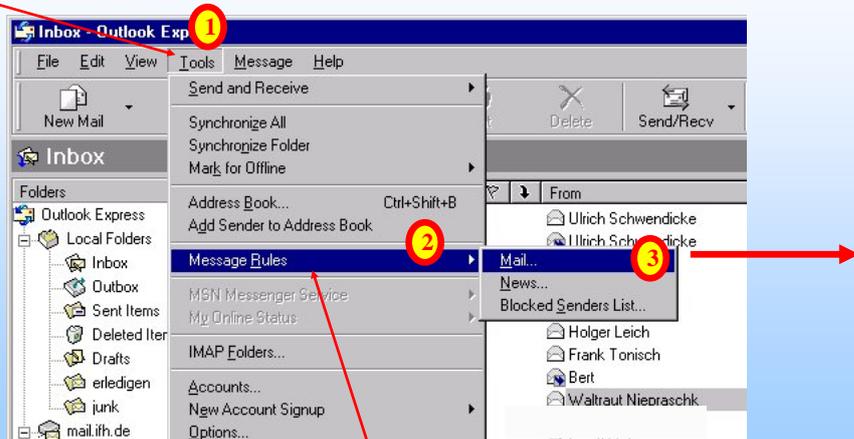
# 8. Filtern auf dem eigenen PC (Outlook Express)

## (4.) Wo wird gefiltert?



## 8. Filtern auf dem eigenen PC (Outlook Express)

“Extras”



“Regel-Assistent” (ein Emailordner muß geöffnet sein)

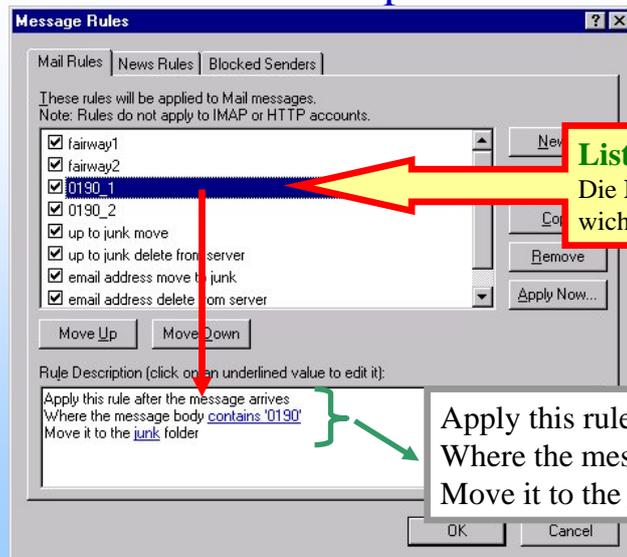
26/10/2007

Bert Schöneich DESY Zeuthen



35

### 8.1.1 Beispiel Outlook Express



Liste der Regeln

Die Reihenfolge der Regeln ist wichtig!

Apply this rule after the message arrives  
Where the message body contains '0190'  
Move it to the junk folder

26/10/2007

Bert Schöneich DESY Zeuthen



36

## 8.1.2 Beispiel Outlook Express

Message Rules

These rules will be applied to Mail messages.  
Note: Rules do not apply to IMAP or HTTP accounts.

- fairway1
- fairway2
- 0190\_1
- 0190\_2**
- up to junk move
- up to junk delete from server
- email address move to junk
- email address delete from server

Rule Description (click on an underlined value to edit it):

Apply this rule after the message arrives  
Where the message body contains '0190'  
Delete it from server

Apply this rule after the message arrives  
Where the message body contains '0190'  
Delete it from server

26/10/2007 Bert Schöneich DESY Zeuthen 37

## 8.1.3 Beispiel Outlook Express

Edit Mail Rule

Select your Conditions and Actions first, then specify the values in the Description.

1. Select the Conditions for your rule:

- Where the From line contains people
- Where the Subject line contains specific words
- Where the message body contains specific words**
- Where the To line contains people

2. Select the Actions for your rule:

- Stop processing more rules
- Do not Download it from the server
- Delete it from server**

3. Rule Description (click on an underlined value to edit it):

Apply this rule after the message arrives  
Where the message body contains '0190'  
Delete it from server

4. Name of the rule:

0190\_2

Auswahl der Bedingung:  
Where the message body contains specific words

Auswahl der Aktion:  
Delete it from server

Apply this rule after the message arrives  
Where the message body contains '0190'  
Delete it from server

Name der Regel

26/10/2007 Bert Schöneich DESY Zeuthen 38

## 8.1.4 Beispiel Outlook Express

The screenshot shows the 'Edit Mail Rule' dialog box in Outlook Express. It is divided into four numbered sections:

- 1. Select the Conditions for your rule:** The option 'Where the message body contains specific words' is selected. A red arrow points to this option from a yellow callout box.
- 2. Select the Actions for your rule:** The option 'Delete it from server' is selected.
- 3. Rule Description (click on an underlined value to edit it):** The description is 'Apply this rule after the message arrives Where the message body contains Delete it from server'. A red arrow points from the underlined word 'contains' to a yellow callout box.
- 4. Name of the rule:** The name is '0190\_2'.

A secondary dialog box titled 'Type Specific Words' is open, showing the text 'Where the message body contains' entered in the 'Words:' field. A red arrow points from the yellow callout box to this dialog box.

**Auswahl der Bedingung:**  
Where the message body contains specific words

26/10/2007 Bert Schöneich DESY Zeuthen

## 8.1.5 Beispiel Outlook Express

The screenshot shows the 'New Mail Rule' dialog box in Outlook Express, overlaid on the 'junk - Outlook Express' window. The 'New Mail Rule' dialog box is divided into four numbered sections:

- 1. Select the Conditions for your rule:** The option 'Where the From line contains specific words' is selected. A red arrow points from a yellow callout box to this option.
- 2. Select the Actions for your rule:** The option 'Forward it to people' is selected.
- 3. Rule Description (click on an underlined value to edit it):** The description is 'Apply this rule after the message arrives Where the From line contains 'alice@onlinehome.de''. A green arrow points from the underlined word 'contains' to a yellow callout box.
- 4. Name of the rule:** The name is 'New Mail Rule #1'.

A yellow callout box points to the 'Create Rule From Message...' option in the 'Message' menu.

**Auswahl der Email:**

**Auswahl der Bedingung:**  
Apply this rule after the message arrives  
Where the From line contains 'alice@onlinehome.de'

26/10/2007 Bert Schöneich DESY Zeuthen

## 8.2.1 Möglichkeiten Outlook Express - Bedingungen

1. Select the Conditions for your rule:

- Where the From line contains people
- Where the Subject line contains specific words
- Where the message body contains specific words
- Where the To line contains people

---

- Where the CC line contains people
- Where the To or CC line contains people
- Where the message is marked as priority
- Where the message is from the specified account
- Where the message size is more than size
- Where the message has an attachment
- Where the message is secure
- For all messages

## 8.2.2 Möglichkeiten Outlook Express - Aktionen

2. Select the Actions for your rule:

- Move it to the specified folder
- Copy it to the specified folder
- Delete it
- Forward it to people

---

- Highlight it with color
- Flag it
- Mark it as read
- Mark the message as watched or ignored
- Reply with message
- Stop processing more rules
- Do not Download it from the server
- Delete it from server

## 8.3 Erfahrungen mit Outlook Express

### Vorteile:

- gut bedienbar auch für Laien
- schnelles Erstellen / Bearbeiten der Filterregeln durch den Nutzer
- keine Online-Kosten beim Erstellen / Bearbeiten der Regeln

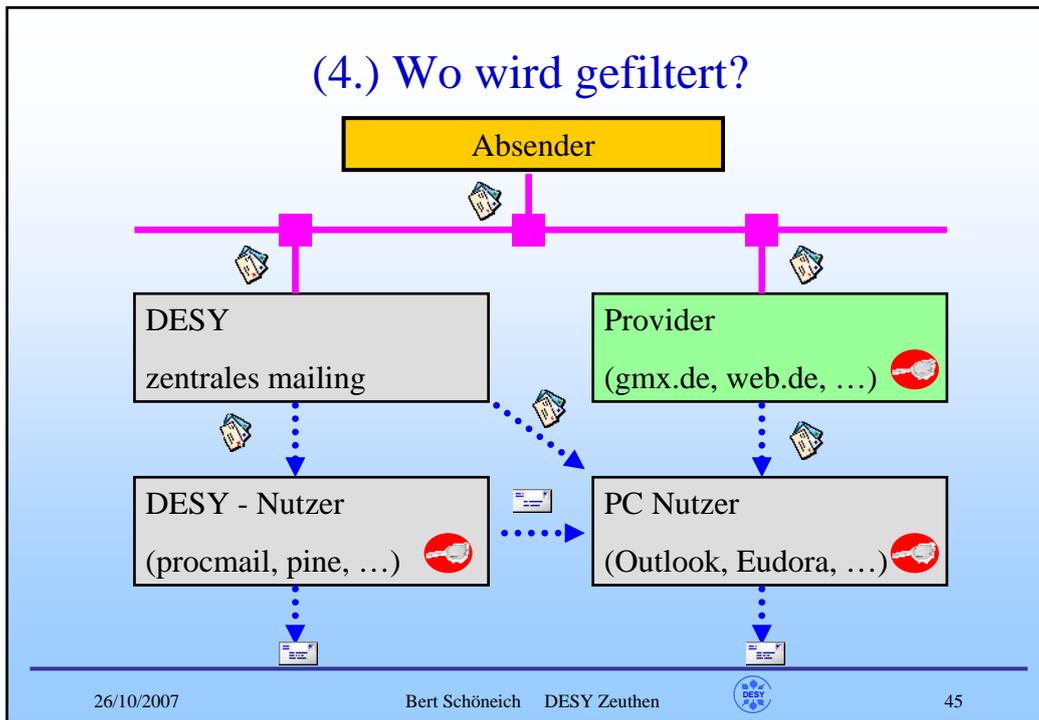
### Nachteile:

- eingeschränkte Filtermöglichkeiten
- Filtern geschieht auf dem eigenen PC
  - zunächst Belastung des PC's, da alle Emails auf dem PC ankommen
  - Onlinekosten bei großen Emails oder Massensendungen
  - Gefahr des Einschleppens von Viren und "Trojanischer Pferde"

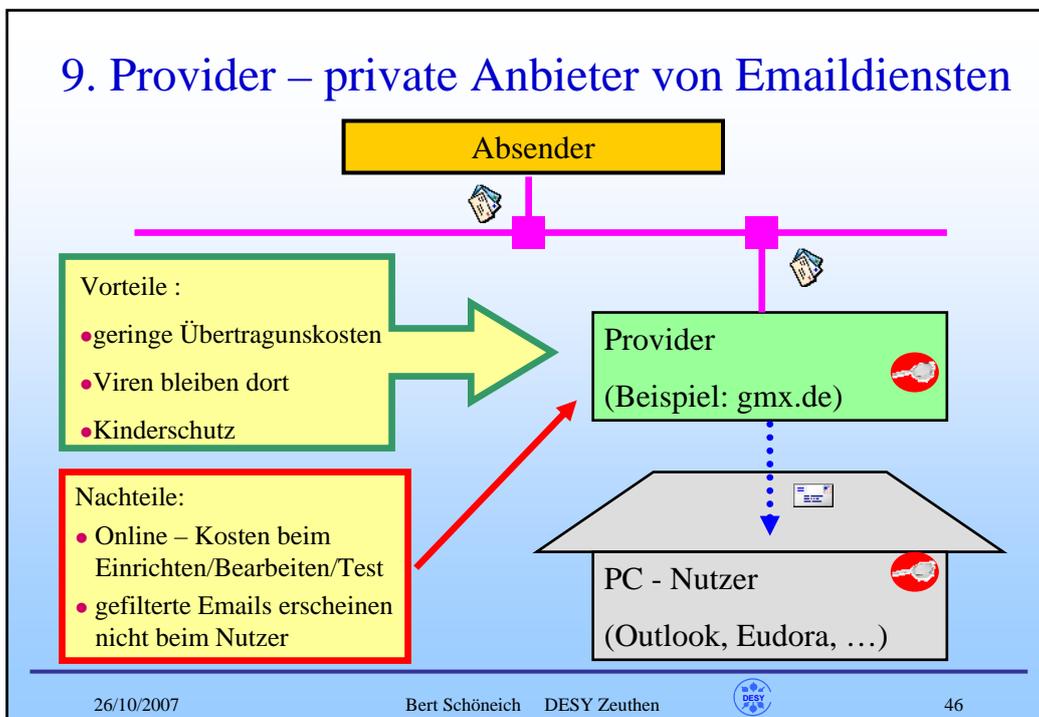
Einsatz eines Virens scanners und eines Firewalls

# 9. Provider private Anbieter von Emaildiensten

#### (4.) Wo wird gefiltert?



#### 9. Provider – private Anbieter von Emailldiensten



## 9.1.1 Provider – Beispiel gmx.de

The screenshot shows the GMX webmail interface. The main content area displays the 'FILTERREGELN' (Filter Rules) configuration page. The page title is 'Aktion: GMX ProMail bestellen und 100 webmailes kassieren!'. The left sidebar contains navigation options like 'Allgemein', 'e-mail-Adressen', 'Signaturen', 'AntiSpam', 'Filterregeln', 'Ordnerverwaltung', 'Abwesenheit', 'Sicherheit', 'Sammeldienst', 'GMX FEATURES', and 'BENUTZERDATEN'. The main content area shows a list of filter rules with the following details:

- Regel 1: "junk"**: Bedingungen: Absender enthält "standalones"; Aktion(en): Ablegen in: Unerwünschte Nachrichten - Bearbeitung hier beenden.
- Regel 2: "to big"**: Bedingungen: Mail größer als 1 Megabyte; Aktion(en): Nachricht an: bert@bert-schoeneich.de - Bearbeitung hier beenden.
- (Standard)**: Bedingungen: keine; Aktion(en): Ablegen in: Posteingang -

Red arrows point to the 'Filter aufrufen' button at the top right, the 'Liste der Filterregeln' section, and the specific rule entries. A 'Standard' rule is also highlighted.

26/10/2007 Bert Schöneich DESY Zeuthen 47

## 9.1.2 Provider – Beispiel gmx.de

The screenshot shows the 'FILTERREGELN / NEUE FILTERREGEL DEFINIEREN' configuration page. The form is filled out for a rule named 'Junk'. The configuration details are as follows:

- Regel 1: "junk"**: Name: Junk
- Bedingung:** Absender enthält das Wort "standalones" (Field: Absender, Operator: enthält, Value: standalones)
- Aktion:** Ablegen in Unerwünschte Nachrichten (wird regelmäßig geleert)
- Regel 1 aktivieren**: The 'Übernehmen' button is highlighted.

Red arrows point to the rule name, the condition field, the action dropdown, and the 'Übernehmen' button.

26/10/2007 Bert Schöneich DESY Zeuthen 48

### 9.1.3 Provider – Beispiel gmx.de

FILTERREGELN / NEUE FILTERREGEL DEFINIEREN ?

Name to big

Ans Ende stellen  Einfügen vor to big

Bedingungen

Feld Absender ist gleich

Mail ist größer als 1 MByte

Groß-/Kleinschreibung beachten  
 Leerzeichen ignorieren

(Keine weitere Bedingung)

Feld Absender ist gleich

Mail ist kleiner als 0 Byte

Groß-/Kleinschreibung beachten  
 Leerzeichen ignorieren

Aktionen

Ablegen in Unerwünschte Nachrichten

Weiterleiten an

Mail löschen - VORSICHT!

Nur benachrichtigen

Benachrichtigung an bert@bert-schoeneich.de

Regelbearbeitung hier beenden

--> übernehmen

**Regel 2: "to big"**

**Bedingung: Email > 1 MByte**

**Aktion: benachrichtigen**

**Regel 2 aktivieren**

26/10/2007 Bert Schöneich DESY Zeuthen 49

### 9.1.4 Provider – Beispiel gmx.de

ANTISPAM-HOTLIST (AUSSCHLUSSLISTE) ?

GMX-AntiSpam-Liste aktivieren  
GMX verwaltet eine interne Liste von E-Mail-Adressen, die für den Versand von E-Mail-Werbung auch an Personen bekannt sind, die dem Empfang dieser Werbung nicht ausdrücklich zugestimmt haben. Wenn Sie diese Funktion aktivieren, erhalten Sie von diesen Adressen keine Werbung mehr zugesandt.

Spam-Schutz für Massendomains aktivieren  
Aus Sicherheitsgründen empfängt GMX Mails aus den Domains aol.com, aol.de, hotmail.com, yahoo.com, yahoo.com und msn.com standardmäßig nur von Mailservern dieser Domains. Sollten Sie diesen Schutzmechanismus ausschalten, rechnen Sie bitte mit einem erhöhten Aufkommen von Spam und/oder UCE in Ihrem Postfach.

Mailbombenschutz aktivieren  
Um Sie vor Mailbomben zu schützen, besitzt GMX einen Mechanismus, der die Mails gleicher Absender an Sie automatisch ablehnt, sollte eine auffallend große Anzahl pro Zeiteinheit eintreffen. Diesen Schutzmechanismus sollten Sie nur ausschalten, wenn das unbedingt notwendig ist!

26/10/2007 Bert Schöneich DESY Zeuthen 50

## 9.1.5 Provider – Beispiel gmx.de

erwünschte Absender

schnuffel@aol.de

Beispiel:  
name@domain erlaubt den betreffenden Absender  
%@domain erlaubt alle Mailabsender aus "domain"  
%domain erlaubt alle Absender und Subdomains aus "domain"

unerwünschte Absender

esistmir@altavista.de  
contech@ares.agmasys.com  
%@aol.de

Beispiel:  
name@domain blockt den betreffenden Absender  
%@domain blockt alle Mailabsender aus "domain"  
%domain blockt alle Absender und Subdomains aus "domain"

--> übernehmen --> abbrechen

Liste erwünschter Absender  
(z.B.: schnuffel@aol.de)

Liste unerwünschter Absender

Namenskonventionen  
%@domain  
(z.B.: %@aol.de)

26/10/2007 Bert Schöneich DESY Zeuthen 51

## 9.2 Erfahrungen mit Providern

### Vorteile:

- gut bedienbar
- sehr gut bei Spam- und andere Massenmails
- Senkung der Übertragungskosten
- Viren / Trojanische Pferde u.ä. bleiben dort
- Kinderschutz

### Nachteile:

- eingeschränkte Filtermöglichkeiten
- Online – Kosten beim Einrichten/Bearbeiten/Test
- gefilterte Emails erscheinen nicht beim Nutzer

# 10. Erfahrungen

26/10/2007

Bert Schöneich DESY Zeuthen



53

## 10.1 Erfahrungen - Gefahren

**1** Frank Stephan  
 Dienstag, 5. Dezember 2000 17:39

**To:** Alexander Donat; Axel Kretzschmann; Bert Schöneich; Brian Long; Herbert Schulze; Volker Leich; Ilja Bohnet; Ingo Wil; Jörg Rossbach; Philippe Piot; Qiang Zhao; Rainer Wernsdorff; Reinhold Heide

**Subject:** Entwurf grober Zeitplan für PITZ-Installation

**Attach:** ZeitplanPITZ.mpp (127 KB)

**2** donat@ifh.de, ..., ..., joerg.rossbach@desy.de

**3** \* !^From.\*@(desy|ifh)\.de

**Abhilfe**

**4** \* [Ce]ll

**5** \* ([Pp]hone)

mail/junk

Liebe Kollegen,  
 im Anhang erhalten Sie einen groben Entwurf des Zeitplanes zur Inbetriebnahme von PITZ (im Wesentlichen nur bis zur Erzeugung Photoelektronen).  
 Es sind nur grobe Punkte aufgeführt und das Ganze ist nur als Entwurf zu verstehen, der zu diskutieren ist.  
 Ich erbitte Rückmeldungen bis 11.12. an mich.  
 Viele Grüße,  
 Frank

Dr. Frank Stephan Email: frank.stephan@desy.de  
 spokesman for the PITZ project

DESY Zeuthen Phone: +49 (0)33762-77338  
 Platanenallee 6 Fax: +49 (0)33762-77330  
 15738 Zeuthen cellular phone: +49 (0170)-7807438  
 Germany

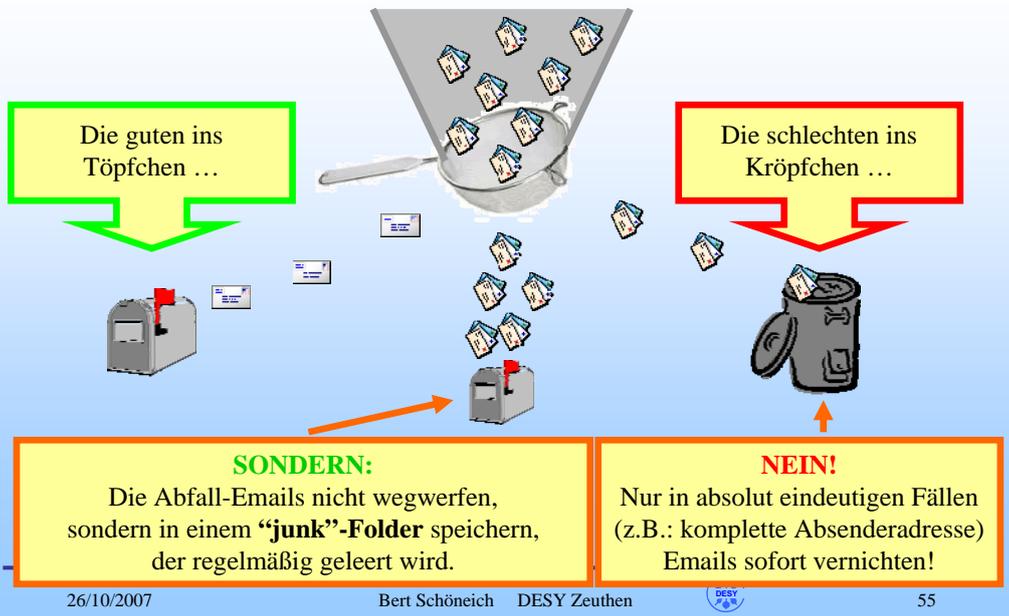
26/10/2007

Bert Schöneich DESY Zeuthen



54

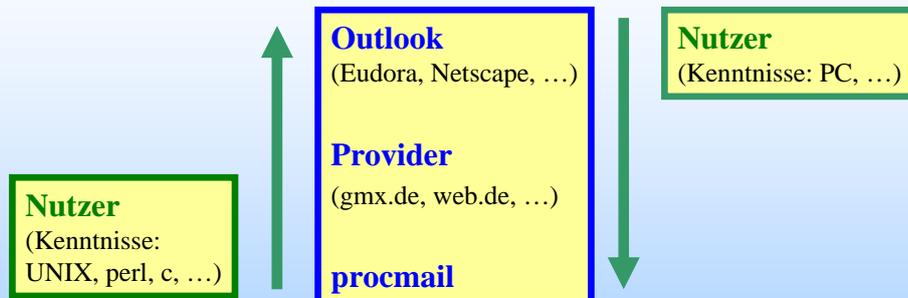
## 10.2 Erfahrungen - Wohin mit dem Abfall?



## 10.3 Erfahrungen - Wie und wann filtern?

- “nachsorgend”, nicht “vorausgehend”:  
Erst, wenn es anfängt zu stören, gibt es eine neue Regel.
- Den Umfang und die Präzision der Filter schrittweise (auch zeitlich!) erhöhen.
- Lieber ein Dutzend unerwünschter E-mails in der Mailbox, als eine erwünschte E-mail im Nichts.
- Filtern möglichst nah am Absender:
  - zuerst procmail / Provider
  - danach Outlook auf dem eigenen PC
- möglichst **nicht** auf dem eigenen PC, sondern **“davor”**
  - Virenschutz
  - senken der Online-Kosten
  - nur gute und kleine E-mails werden übertragen

## 10.4 Erfahrungen - Wie mit dem Filtern beginnen?



1. Keine Email sofort vernichten!
2. TESTEN TESTEN TESTEN!

## 10.5.1 Erfahrungen - Signatur unerwünschter Emails

- Absender
  - bin ich selbst, weiß aber nichts davon
  - unbekannter Name, ungewohnte Domain, ungewohntes Land
  - Schläfer, der aufwacht
    - mit diesem Absender über lange Zeit keinen Kontakt gehabt
    - unbekannt, warum er sich wieder meldet
- Betreff /Subject-Zeile:
  - leer
  - nur **Re:**
  - unpersönlich, unzutreffend
  - kündigt Unerwünschtes an, vorzugsweise in Englisch

## 10.5.2 Erfahrungen - Signatur unerwünschter Emails

- Inhalt
  - unerwartet
  - unpersönlich
  - nicht angefordert
  - “Text im Anhang/Attachment, bitte lesen”
- Anhang/Attachment
  - Titel des Anhanges unbekannt
  - unerwartet, nicht angefordert
  - groß
  - Typ kritisch (z.B. \*.EXE)
- Massensendung (SPAM)
- Kettenmail, egal (!) welchen Inhaltes

## 10.6.1 Erfahrungen - Reaktion auf unerwünschte Emails

Treffen mehrere (eventuell auch nur einer) der Signaturpunkte unerwünschter Emails zu, dann:

- Email nicht öffnen
- Anhang
  - nicht öffnen
  - nicht speichern/save
- **Email aus der Liste heraus im ungeöffneten Zustand streichen**  
(rechte Maustaste)
- **Ordner der gestrichenen Emails sofort leeren**

## 10.6.2 Erfahrungen - Reaktion auf unerwünschte Emails

- **NIE auf eine SPAM – Email reagieren!**
- **NIE** eine SPAM - Email beantworten oder zurückschicken, weder freundlich, noch unfreundlich, noch wütend.
- Die Folge wären möglicherweise ein deutlich erhöhtes Aufkommen an solchen Emails.
- **Email wegwerfen**
- **Filter programmieren, wenn viele gleichartige Emails kommen.**

## 10.6.3 Erfahrungen - Reaktion auf unerwünschte Emails

- DFÜ (Internetverbindung)
  - trennen
  - überprüfen auf neue DFÜ-Verbindungs-Einträge (z.B. andere als das gewohnte t-online)
- Virens Scanner
  - über alle Platten und alle Files (!) laufen lassen
  - neueste Virensignaturen herunterladen

## 10.6.4 Erfahrungen - Reaktion auf unerwünschte Emails

- überprüfen
  - 0190 – Warner und seine Einstellungen
  - Firewall und seine Einstellungen
- Absender, falls bekannt
  - anrufen
  - klären, ob die Email
    - von ihm kam
    - sinnvoll war

**Email noch einmal schicken lassen**

# 11. Zusammenfassung

## 11. Zusammenfassung

### 11.1 Vorteile:

- Mit dem Einsatz von Emailfiltern gelingt es, das Aufkommen an unsinnigen, störenden Emails deutlich zu senken.
- Emailfilter senken die Bedrohung durch Viren, Trojanische Pferde u. ä..
- Emailfilter senken die Onlinekosten.

### 11.2 Nachteile:

- Ein 100 % - iger Schutz vor unerwünschten Emails ist nicht möglich.
- Es ist nicht vollkommen auszuschließen, das in Einzelfällen auch erwünschte Emails verschwinden.
- Der Einsatz von Emailfiltern verlangt je nach Umfang und Präzision des Filters in steigendem Maße Programmierkenntnisse.

## 12. Literatur

## 12.1 Literatur

- man pages für procmail:
  - procmail - autonomous mail processor
  - procmailrc - procmail rcfile
  - procmailex - procmail rcfile examples
  - procmailsc - procmail weighted scoring technique
- alles zu Email am DESY Zeuthen (Wolfgang Friebe)  
<http://www-zeuthen.desy.de/computing/services/Mail/mailservice.html>
- Empfehlungen des CERN an seine Email-Nutzer:  
<http://security.web.cern.ch/security/Recommendations/Default.htm>
- Provider:
  - “test”, Stiftung Warentest, August 2001, S. 25 ff.
  - “Gratis, aber unsicher – 27 E-Mail-Dienste, gut sind nur vier”
- “Hilfe” – Button der privaten Anbieter
- Beispiel - Regelfile unter .procmail  
~schoene/.procmailrc.example



## 12.2 Literatur

- Informationen und Erklärungen zu SPAM u.ä. :  
<http://www.cityweb.de/free/3.spam100499.inhalt-000.html#top>  
[http://www.uni-koeln.de/RRZK/kompass/76/wmwork/www/k76\\_15.html](http://www.uni-koeln.de/RRZK/kompass/76/wmwork/www/k76_15.html)  
<http://www.trash.net/sam/spam/>  
<http://www.jobpilot.de/content/journal/thema/kw09-02.html>
- Monty Python's SPAM-Sketch  
<http://www.pythonsite.de/55.htm>
- SPAM-Behandlung am CERN (einschließlich der Sperrliste)  
<http://consult.cern.ch/service/mail/problems/spams.html>



## 12.3 Literatur

### Dialer Problem:

- “Wider die Dialer-Mafia”  
Protest gegen 0190-Abzocker wächst  
c’t 6/02, S.74 f.
- “Abzocke abblocken, Tipps gegen ungewollte 0190-Dialer”  
c’t 1/02, S. 180
- “Umstöpseln und abkassieren, Heimliche Umstellung auf 0190-Nummern”  
c’t 26/01, S.216
- <http://www.regtp.de>
- <http://www.dialerschutz.de>
- <http://www.polizei.bayern.de/ppmuc/schutz/text10.htm>

## 12.4 Literatur

- Rechtslage :  
“Hausfriedensbruch per FAX, Mail oder SMS”  
Verbraucherschützer fordern härteres Durchgreifen gegen Absender  
MAZ 16.3./17.3.2002