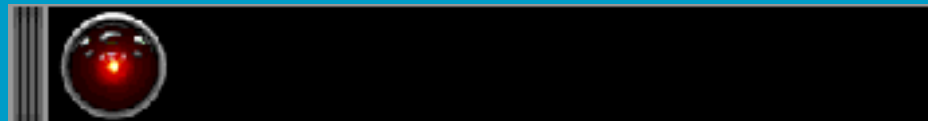




SPAMs, Viren, Trojaner - Möglichkeiten der Abwehr und Filterung mit OpenSource in Unternehmen

**Open Source Business Conference 2005
Wien, 21.1.2005**

Josef Bergmann <joe@bec.at>



Inhalt

- **Was sind SPAMs, Viren, Trojaner**
- **Spamassassin**
- **Clam Antivirus**
- **Typischer Praxiseinsatz**
- **Erfahrungen aus der Praxis**
- **Zusammenfassung**

Was sind SPAMs, Viren, Trojaner



Spam kommt aus einem Monty Python-Sketch (ursprünglich Dosenfleisch).

Exaktere Begriffe:

"UCE" (unsolicited commercial email)

"UBE" (unsolicited bulk email)

**In Österreich in TKG2003
§107 geregelt**

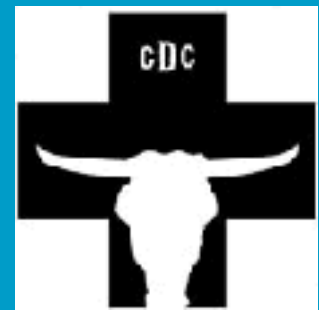
Was sind SPAMs, Viren, Trojaner ?

Trojanische Pferde: (manchmal nützliche) Programme, mit einer „schädlichen“ Funktion (Daten ausspähen, DoS, Spammer). „Back Orifice“, „Netbus“

Viren: Programme die Wirtsprogramme infizieren. „CIH-Virus“

Würmer: Viren die sich ohne Wirt selbst vermehren. „Sobig“

..., **Dialer = Malware**



Was ist an SPAMs schlecht?

Resourcendiebstahl: Kosten für Bandbreite, Verkehr, Speicherplatz, Arbeitszeit, ...

Unternehmen mit 300 Mitarbeiter: Zeitaufwand pro Spam 3s, jeder bekommt pro Tag 10 Spams, Kosten einer Arbeitsstunde 25,- ergibt **1400,- Euro/Monat**

Die Kosten für den „Spammer“ selbst sind minimal -> niedrige Hemmschwelle.

Spamassassin



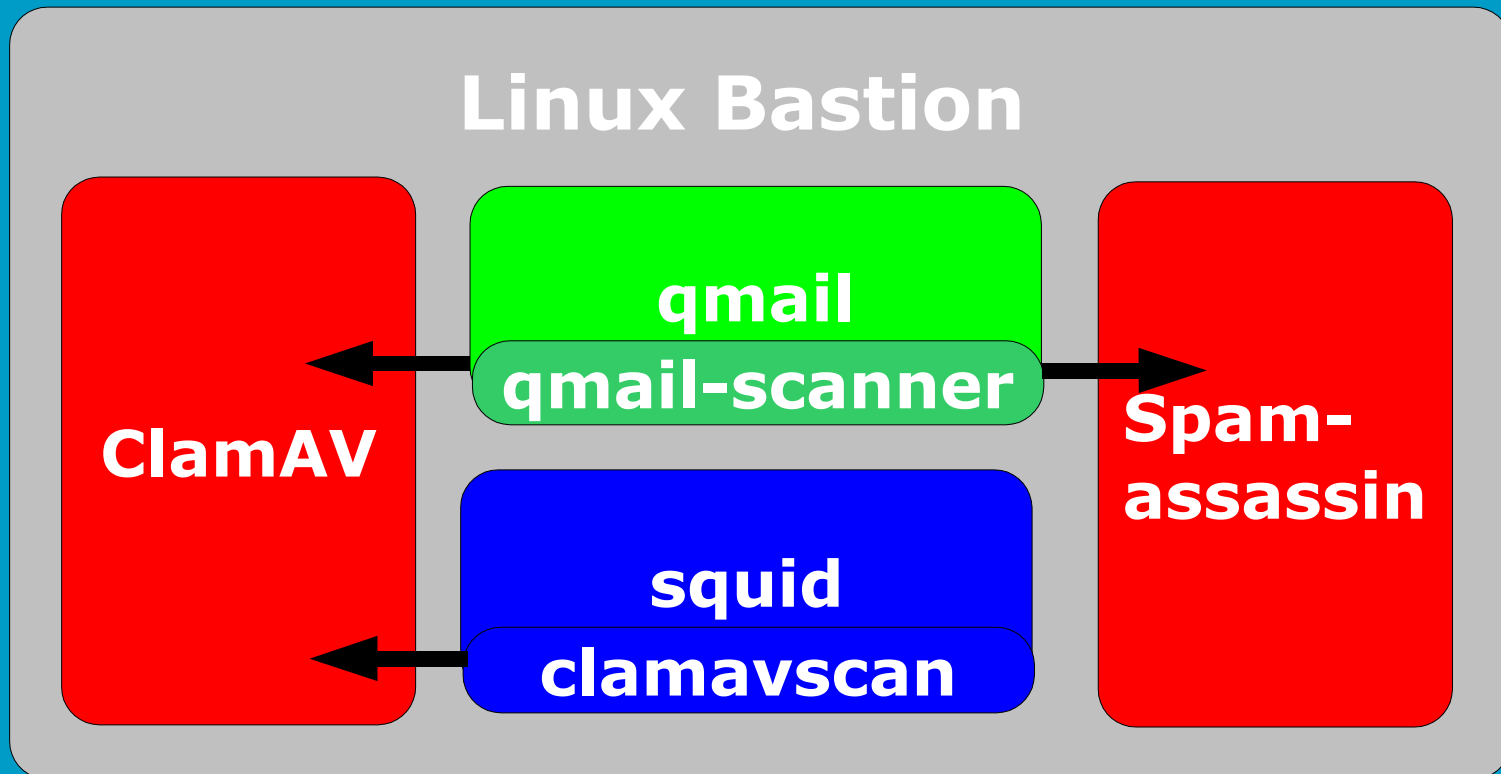
- **Quellenoffen (Apache Lizenz)**
- **verschiedene Portierungen (Linux ... Windows)**
- **Umfangreiches Regelwerk mit Scoring und Training (Bayes)**
- **Regeln mit „Onlinechecks“ (RBL, URIDNSBL, collab. Filterdatenbanken)**
- **verteilte Client/Server-Installation möglich**
- **weitreichende Unterstützung von MTAs**

Clam Antivirus (ClamAV)

- **Quellenoffen (GPL)**
- **verschiedene Portierungen (Linux ... Windows)**
- **schnelle multi-threaded Client/Server-Implementierung, sowie C-Library**
- **schnelles effizientes Onlineupdate**
- **erkennt derzeit über 29000 Viren, Würmer, Trojaner**
- **Erkennt sämtliche Archive (RAR ... OLDFORMATS)**
- **massig 3th party Software**



Typischer Praxiseinsatz



Typischer Praxiseinsatz

Abgesichert ist als M...

1) Prüft ei
öff...

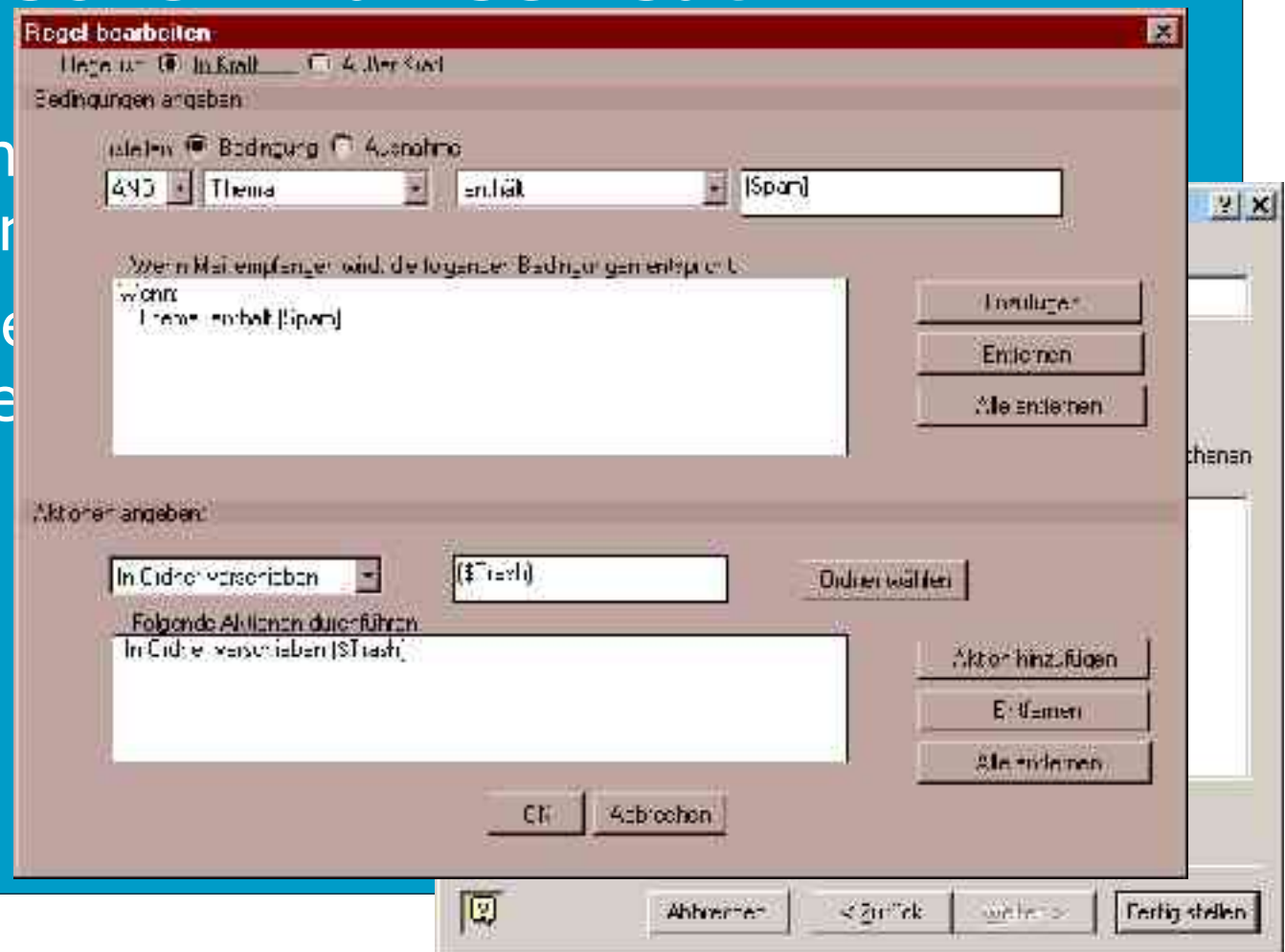
3) Prüft
geprüft (P...

```
Return-Path: <proof@richycraig.com>  
Delivered-To: YYYYYY@XXXXX.ZZZ  
Received: from proof@richycraig.com by fw by uid 64011 with mail-scanner-1.24  
(clamscan: 0.80. uvscan: v4.2.40/v4296. spamassassin: 3.0.2. Clear:RC:0:SA:1(27.5/5.0):.  
Processed in 1.54272 secs); 10 Jan 2005 06:02:29 -0000  
X-Spam-Status: Yes, hits=6.3 required=5.0  
Received: from unknown (HELO winme) (220.113.162.120)  
by fw.XXXXX.ZZZ with SMTP; 3 Oct 2003 06:02:22 -0000  
Message-ID: <1104...@winme>
```

Received: ... with mail-scanner-1.24
(clamscan: 0.80. ... spamassassin: 3.0.2. ...
Processed in 1.54272 secs); 10 Jan 2005 06:02:29 -0000
X-Spam-Status: Yes, hits=6.3 required=5.0

Typischer Praxiseinsatz –

Am Mail-Client
 Mail für Filter
 z.B. Regel „wenn
 vorkommt, verschieben
 Junk-Ordner



Abgesich
wird von

2005/01/14 11:55:47| mod_clamavscan: http://install.xxxtoolbar.com/ist/scripts/prompt.php?
contains virus Trojan.Downloader.Istbar-44, blocking 2292 bytes !
2005/01/14 11:55:47| mod_clamavscan: http://china.dalexcars.com/assassin-254.exe
contains virus Trojan.Downloader.DLex-3, blocking 1460 bytes !
2005/01/14 16:39:25| mod_clamavscan: http://69.50.166.212/counter/winxp/GetAccess.class
contains virus Java.ClassLoader.24564, blocking 1448 bytes !
2005/01/14 16:39:55| mod_clamavscan: http://69.50.191.68/eb/be/ass.html
contains virus Exploit.HTML.MHT-7, blocking 337 bytes !
2005/01/14 16:50:05| mod_clamavscan: http://69.50.191.68/eb/be/Dummy.class

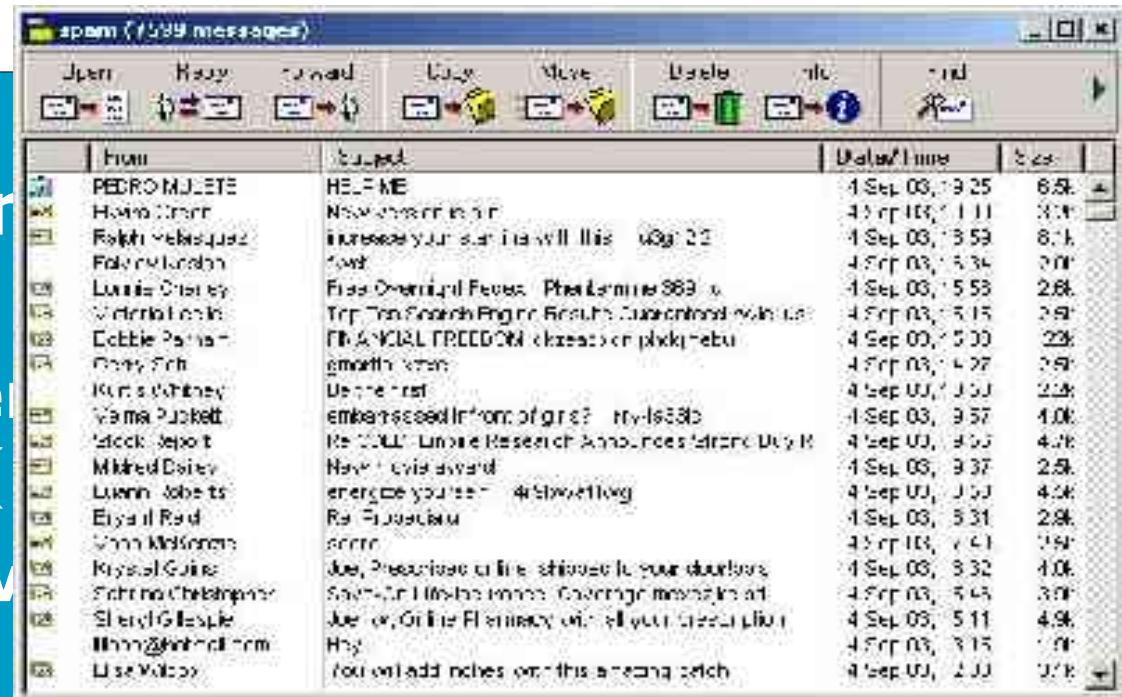
... mod_clamavscan: http://install.xxxtoolbar.com/ist/scripts/prompt.php?
contains virus Trojan.Downloader.Istbar-44, blocking 2292 bytes !

3) gefährl
gefährlich

2005/01/14 16:50:05| mod_clamavscan: http://69.50.191.68/eb/be/Dummy.class
contains virus Java.ClassLoader.240, blocking 240 bytes !
2005/01/14 16:50:29| mod_clamavscan: http://www.bulldog-stats.com/adv/10/index.html
contains virus Exploit.HTML.MHT-3, blocking 428 bytes !
2005/01/14 16:50:31| mod_clamavscan: http://myiframe.biz/acc1/exploit.htm
contains virus Trojan.VBS.Psyme.V, blocking 343 bytes !
2005/01/14 16:51:05| mod_clamavscan: http://69.50.191.68/eb/be/Dummy.class
contains virus Java.ClassLoader.240, blocking 240 bytes !
2005/01/14 18:54:52| mod_clamavscan: http://www.tv69.com/blur/all_launch_reg.htm
contains virus Trojan.NoClose.O, blocking 2035 bytes !

Erfahrungen

Typische SPAMs werden
 erst angenommen (10%)
 Rest wird zu 90 % von
 Antiviren erkannt



	From	Subject	Date/Time	Size
100	PEDRO MULETE	HELP ME	4 Sep 03, 19:25	6.5K
101	Helen O'neil	New research in your	4 Sep 03, 17:11	3.1K
102	Rafael Velascoquez	Increase your sales with this	4 Sep 03, 15:53	8.1K
103	Fakir London	Want	4 Sep 03, 15:34	2.0K
104	Louise O'neil	Free Chemical Fees - Phosphorus 889	4 Sep 03, 15:53	2.8K
105	Victoria Lewis	Top Ten Search Engine Results - Subcontractors	4 Sep 03, 15:15	2.9K
106	Cobbie Palmer	FINANCIAL FREEDOM (kreas) on pluck-hebu	4 Sep 03, 15:00	22K
107	Oliver Smith	smooth skin	4 Sep 03, 14:27	2.9K
108	Kurt Whitney	Use the first	4 Sep 03, 13:00	2.5K
109	Verna Puckett	embossed in front of girls? try-16386	4 Sep 03, 9:57	4.0K
110	Stock Report	RESEARCH - Unilever Research Announces Fat-Free Dairy B	4 Sep 03, 9:00	4.2K
111	Mikheil Davit	Have a great award	4 Sep 03, 9:37	2.5K
112	Lynn Roberts	energize yourself - 489wetting	4 Sep 03, 9:00	4.2K
113	Elysa Reid	Re: Prusaforum	4 Sep 03, 5:31	2.8K
114	Vinny McKeown	scrm	4 Sep 03, 4:41	3.9K
115	Kristal Guire	Joe, Prescription of line - shipped to your door	4 Sep 03, 3:32	4.0K
116	Richard Chelmsford	Save on Utilities - Green - Greening means in ad	4 Sep 03, 3:43	3.9K
117	Sheryl Gillespie	Joe or, Grille Flimsy with all your great plon	4 Sep 03, 5:11	4.9K
118	lham@hatfield.com	Hy	4 Sep 03, 3:15	1.9K
119	Lise Villoz	You will add notes on this amazing patch	4 Sep 03, 2:00	3.7K

Um „false positives“ aufzuspüren ist hin und
 wieder doch ein Blick in den Spamfolder
 erforderlich

Viren werden praktisch zu 100% abgeblockt.

Erfahrungen Squid-Contentscanner

Mit den Squid-Accessregeln lässt sich schon auf Contenttyp filtern.

Praktisch alle gängigen Viren und Trojaner werden vom Contentscanner erkannt. Auch Viren in Webmailsessions sind kein Problem.

Kein merkbarer Unterschied beim Surfverhalten (Content wird „inTime“ weitergeleitet).



Linkliste

Spamassassin <http://spamassassin.apache.org>

ClamAV <http://www.clamav.net>

Qmail <http://www.qmail.org>

Qmail-Scanner <http://qmail-scanner.sourceforge.net>

Squid <http://www.squid-cache.org>

Squid Filter

<http://sites.inka.de/sites/bigred/devel/squid-filter.html>

Squid clamavscan

<http://bec.at/support/squid/clamavscan>

WIFI Wien <http://www.wifiwien.at>

BERGMANN engineering & consulting <http://bec.at>



Zusammenfassung

Selbstbau mit Linux Know-How

WIFI: LTCP - LINUX Security Expert (LSX)

**Komplettlösungen mit abgesicherten Linux
Beratung, Setup, Wartung**

BERGMANN engineering & consulting

<http://www.firewall.at/help>