

# ***Mit Muscheln gegen Viren***

***Der freie Virens Scanner ClamAV und  
das Dazuko.ko***

# COMPUTERWOCHE

**“Einen guten Linux-  
Virens Scanner zu  
finden ist  
schwierig.”**



# *ist das auch nötig?*

ca. 33500 Signaturen

**Unix**      **58**

**Linux**      **87**

**Solaris**      **3**

**BSD**      **4**

**SunOS**      **2**

**Winux**      **1**

**+ Verantwortung durch Einsatz im Serverbereich**

# ***Virenscanner***

- **H+BEDV AntiVir**
- **Kaspersky**
- **McAfee/NAI**
- **Symantec**
- **Sophos**
- **ClamAV**

# *Security by Obscurity?*

**14. Feb 30665 Sigs**  
**14. Apr 32835 Sigs**  
**22. Apr 33426 Sigs**

- **The Cathedral and the Bazaar**
- **rasante Anpassung der Viren-DB und Engine**

# ClamAV

- ClamAV ist ein Antivirus-Toolkit für Unix, steht unter der GPL
- Hauptzweck war die Integration in Mailserver zum Attachment-Scanning.
- basiert auf libclamav



# ClamAV

- bietet einen flexiblen, skalierbaren multi-threaded Scandaemon
- milter interface für sendmail
- eingebaute Unterstützung für RAR2.0, Zip, Gzip, Bzip2, tar, MS OLE2, MS cabinet-Files, MS CHM, MS SZDD, mbox, maildir, RAW, UPX, FSG und Petite Formate.



# ***Kommandozeilentools***

- **clamd**
- **clamdscan**
- **clamscan**
- **freshclam**
- **sigtool**



The background features a group of penguins on a snowy or icy surface. A large, bright yellow thought bubble is superimposed over the scene, containing the main title. Several smaller yellow thought bubbles trail off from the bottom left of the main bubble.

# Kurze Vorführung

# Config/DB-Dateien

- **usr/local/etc/clamd.conf**
- **usr/local/etc/freshclam.conf**

basier(t)en auf der Viren-DB des OpenAntiVirus-Projekt/SignatureDB

- **main.cvd**
- **daily.cvd**



# 3<sup>rd</sup> Party-Software

- **KlamAV**
- **Klamaction**
- **INSERT**
- **ClamWin**
- **remoteClam**

**kleine Auswahl mehr bei clamav.net**



# ***OnAccess-Scanning***

- **ist die Möglichkeit Dateien beim Zugriff zu scannen**
- **ermöglicht Content-Scan**
- **schaltet die Unsicherheit Nutzer nahezu aus**

# Dazuko

- **Entwicklung H+BEDV, unter GPL**
- **ermöglicht Userland-Programmen, die Dateizugangskontrolle**
- **Linux 2.2 – 2.6., Linux-RSBAC und FreeBSD 4/5**
- **Entwickler wollen zukünftig MacOS X, Solaris und OpenBSD unterstützen**

The background features a group of penguins on a snowy or icy surface. A large, bright yellow thought bubble is superimposed over the scene, containing the main title. Several smaller yellow thought bubbles trail from the bottom left of the main bubble towards the penguins.

# Kurze Vorführung

# ***samba-vscan***

- **ermöglicht OnAccess-Scan von SMB-Shares**
- **nutzt (POSIX) VFS Samba 2.2 / 3.0**
- **original entwickelt für Sophie and Trophie**
- **ein Modul für verschiedene AV-Scanner**
- **Resultat-Caching -verbesserte Performance**



***Danke  
für  
Ihre  
Aufmerksamkeit***

**Fragen ???**