The background of the slide features two Emperor penguins standing on a patch of ice. The penguin on the right is in the foreground, looking towards the right. The penguin on the left is slightly behind and to the side. The text is overlaid on the right side of the image.

ClamAV

Virensscanner für

ein Linux / Windows Umfeld

Situation

Viren, Trojaner, Würmer, Webbugs, Spyware, Dialer bedrohen die Netzwerke

nur wenige Sekunden ungeschützt
reichen



Situation Mailserver

Schnittstelle zum Internet, häufigste Verbreitungsart

Linux Mailserver (sendmail)
mit amavis und NAI Virusscan

scannt eingehende/ausgehende Mail

Updatezyklus langsam (1x pro Woche)



Situation Fileserver

Linux Fileserver
mit Samba und NFS

Domain-Controller
kein Virenskan
kein onAccess Scan



Situation Proxy

Schnittstelle zum Internet, häufigste Verbreitungsart

es gibt bisher keinen Content-Scanner

mit vscan-Modul für squid, dazuko und ClamAV besteht dahingehend die Möglichkeit

Situation Desktop 's

Windows NT, zunehmend XP

VirenScanner überwiegend proprietär
kein onAccess Scan möglich

Linux Desktops

Scans bislang kaum notwendig



Ziele

Einschleusen / Verbreiten von „Malware“
hemmen bzw. unterbinden

zusätzlicher bezahlbarer Virens Scanner

Verhinderung der Verbreitung über den
Fileserver

File Scan auf den Arbeitsplätzen



Maßnahmen

Virens Scanner ClamAV für Windows und Linux

Mailserver postfix mit RBL betreiben?

Spamassassin zur semantischen Kontrolle der Mails

Proxyserver squid mit Blacklists/vscan



ClamAV / Clamwin

freier Virens Scanner kurzen Update-
Zyklen www.clamav.net

Online-Update per http

Clamd mit onAccess Scanner für Linux
Kernel-Modul *dazuko* (H+B EDV)

Clamwin „klinkt“ sich in Taskleiste ein



Kernelmodul Dazuko

„Datenzugriffskontrolle“
www.dazuko.org

3rd-Party Schnittstelle für Virens Scanner

wird von Clamuko genutzt
prüft beim Öffnen/Schließen/Schreiben



zentrale VirenDB

mittels „freshclam“ als Daemon
zeitgesteuerte Aktualisierung

per http (tinyhttpd oder Apache) in das
Intranet publiziert

Einsparung Internet-Traffic



Clamwin

wird beim Hochfahren des PC gestartet
vom Benutzer manuell aktivierbar

kann von bestimmten PC des NW aus
mittels
RemoteClam gesteuert werden

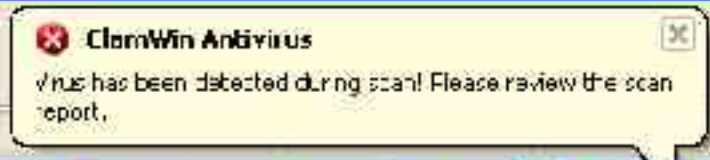


Clamwin

manuelles scannen von Dateien



Clamwin



RemoteClam

Dienst zum Übermitteln von Kommandos an Clamwin

startet Scripte aus Samba-Share

Rückmeldungen in Logdateien
(Samba-Share)

ausgeliefert als Setup-Exe



Virensan-Struktur

WinNT/XP



Clamwin
RemoteClam

Update
VirenDB

Kommandos
an Clamwin

Internet

Update
VirenDB



Linux

Fileserver
VirenDB für das Intranet
tinyhttp
Clamd onAccess Scan
postfix nutzt VirenDB

Admin-Console
Kommandos
Webinterface

zentrale Administration

1. Kommandos an ClamWin übermittelt
mittels RemoteClam

```
>telnet 192.168.20.11 5678  
scan
```

2. Web-Interface dazu (in Kürze)

Probleme

kein onAccess Scan
für Windows

Ressourcenverbrauch

- niedrige Prio für Clamwin
- ausgewählte Verzeichnisse scannen

Zusammenfassung

Clamav ist ein leistungsfähiger Scanner
für Linux & Windows

GPL Lizenz

Nutzung mit postfix/amavis

unter Linux auch onAccess Scan



A photograph of three Emperor penguins standing on a patch of ice. The penguins are shown in profile, facing right. They have dark grey heads and backs, and bright yellow-orange chests and bellies. The background is a plain, light color.

**Danke
für
Ihre
Aufmerksamkeit**