

KASPERSKY LAB MEETS OPEN-SOURCE

Vortrag Linux Tag
Chemnitz 2015

Roland Imme
Senior Technical Sales Engineer

THEMEN

- 3 **Bedrohungslage durch Malware**
- 12 **Infektionswege**
- 15 **Kaspersky Lab**
- 21 **Systeme mit Kaspersky absichern**
- 26 **AMaViS Projekt**
- 29 **AMaViS und Kaspersky vs. Malware und Spam**

BEDROHUNGSLAGE DURCH MALWARE

Besteht für Linux-Betriebssysteme eine Bedrohungslage durch Malware?

ALLGEMEINE BEDROHUNGSLAGE

Zahlen und Fakten zur allgemeinen Bedrohungslage

BEDROHUNGEN

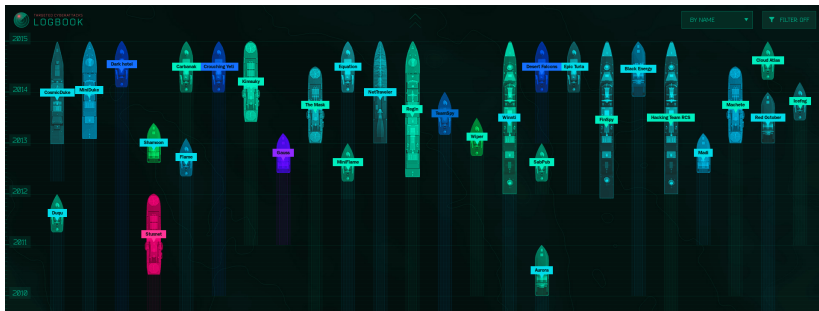


ANGRIFFE MIT MALWARE



Internetseite: <https://apt.securelist.com/#firstPage>

ÜBERBLICK ZU AKTUELLEN ANGRIFFSWERKZEUGEN



Internetseite: <https://apt.securelist.com/#firstPage>

BESCHREIBUNG CROUCHING YETI

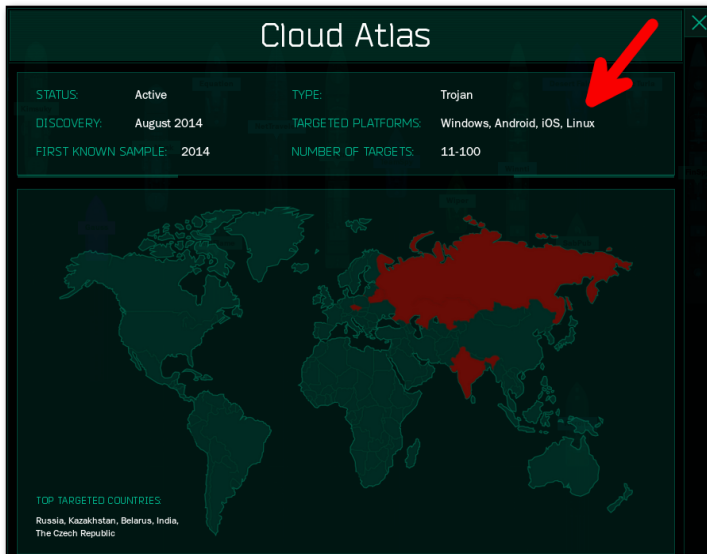
Crouching Yeti

STATUS:	Active	TYPE:	Backdoor, Remote administration tool
DISCOVERY:	January 2014	TARGETED PLATFORMS:	Windows
FIRST KNOWN SAMPLE:	2010	NUMBER OF TARGETS:	2,001-3,000

TOP TARGETED COUNTRIES:

United States, Spain, Japan,
Germany, France, Italy, Turkey, Ireland,
Poland, China

BESCHREIBUNG CLOUD ATLAS



EXPONENTIELLER ANSTIEG DER VERBREITUNG ...

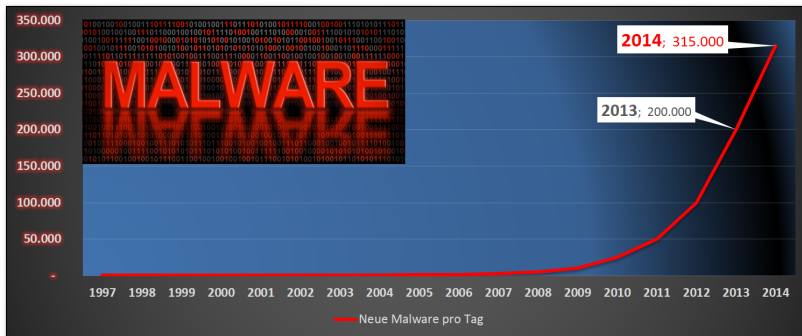
- > am Tag werden weltweit **ca. 325.000 neue Bedrohungen** in Umlauf gebracht
- > Bedrohungslage unverändert hoch

EXPONENTIELLER ANSTIEG DER VERBREITUNG ...

- > am Tag werden weltweit **ca. 325.000 neue Bedrohungen** in Umlauf gebracht
- > Bedrohungslage unverändert hoch

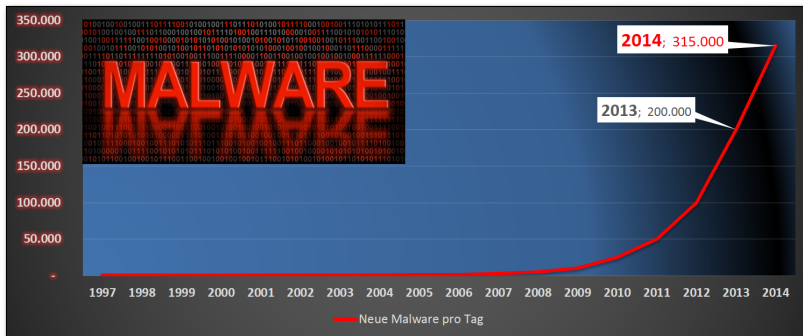
EXPONENTIELLER ANSTIEG ...(FOLIE 2014)

- > am Tag werden weltweit **ca. 315.000 neue Bedrohungen** in Umlauf gebracht
- > Bedrohungslage unverändert hoch



EXPONENTIELLER ANSTIEG ...(FOLIE 2014)

- > am Tag werden weltweit **ca. 315.000 neue Bedrohungen** in Umlauf gebracht
- > Bedrohungslage unverändert hoch



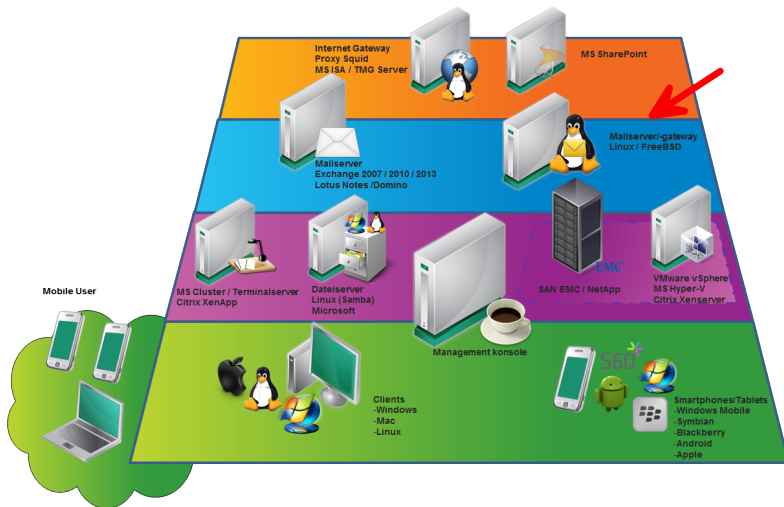
INFEKTIONSWEGE

Mögliche Wege einer Infektion mit Malware

INFORMATIONEN ZU INFEKTIONSWEGEN

Wie dringt Malware im Netz ein?

MÖGLICHE INFEKTIONSWEGE VON MALWARE



KASPERSKY LAB

Was steht hinter dem Unternehmen Kaspersky?

KASPERSKY LAB FAKTEN IN KÜRZE

Allgemeine Informationen zum Unternehmen Kaspersky Lab

KASPERSKY LAB FAKTEN

- > 1997 von einer Gruppe von IT-Sicherheitsexperten unter Führung von **Eugene Kaspersky** gegründet
- > bietet innovative Sicherheitssoftware und -lösungen für private und gewerbliche Nutzer
- > bietet mehr als 400 Millionen Menschen weltweit Schutz
- > beschäftigt mehr als 3.000 hochqualifizierte Spezialisten weltweit
- > ...



Kaspersky Lab Global <http://www.kaspersky.com/about>

KASPERSKY LAB FAKTEN

- > 1997 von einer Gruppe von IT-Sicherheitsexperten unter Führung von **Eugene Kaspersky** gegründet
- > bietet innovative Sicherheitssoftware und -lösungen für private und gewerbliche Nutzer
- > bietet mehr als 400 Millionen Menschen weltweit Schutz
- > beschäftigt mehr als 3.000 hochqualifizierte Spezialisten weltweit
- > ...



Kaspersky Lab Global <http://www.kaspersky.com/about>

KASPERSKY LAB FAKTEN

- > 1997 von einer Gruppe von IT-Sicherheitsexperten unter Führung von **Eugene Kaspersky** gegründet
- > bietet innovative Sicherheitssoftware und -lösungen für private und gewerbliche Nutzer
- > bietet mehr als 400 Millionen Menschen weltweit Schutz
- > beschäftigt mehr als 3.000 hochqualifizierte Spezialisten weltweit
- > ...



Kaspersky Lab Global <http://www.kaspersky.com/about>

KASPERSKY LAB FAKTEN

- > 1997 von einer Gruppe von IT-Sicherheitsexperten unter Führung von **Eugene Kaspersky** gegründet
- > bietet innovative Sicherheitssoftware und -lösungen für private und gewerbliche Nutzer
- > bietet mehr als 400 Millionen Menschen weltweit Schutz
- > beschäftigt mehr als 3.000 hochqualifizierte Spezialisten weltweit
- > ...



Kaspersky Lab Global <http://www.kaspersky.com/about>

KASPERSKY LAB FAKTEN

- > 1997 von einer Gruppe von IT-Sicherheitsexperten unter Führung von **Eugene Kaspersky** gegründet
- > bietet innovative Sicherheitssoftware und -lösungen für private und gewerbliche Nutzer
- > bietet mehr als 400 Millionen Menschen weltweit Schutz
- > beschäftigt mehr als 3.000 hochqualifizierte Spezialisten weltweit
- > ...



Kaspersky Lab Global <http://www.kaspersky.com/about>

KASPERSKY LAB FAKTEN

- > 1997 von einer Gruppe von IT-Sicherheitsexperten unter Führung von **Eugene Kaspersky** gegründet
- > bietet innovative Sicherheitssoftware und -lösungen für private und gewerbliche Nutzer
- > bietet mehr als 400 Millionen Menschen weltweit Schutz
- > beschäftigt mehr als 3.000 hochqualifizierte Spezialisten weltweit
- > ...



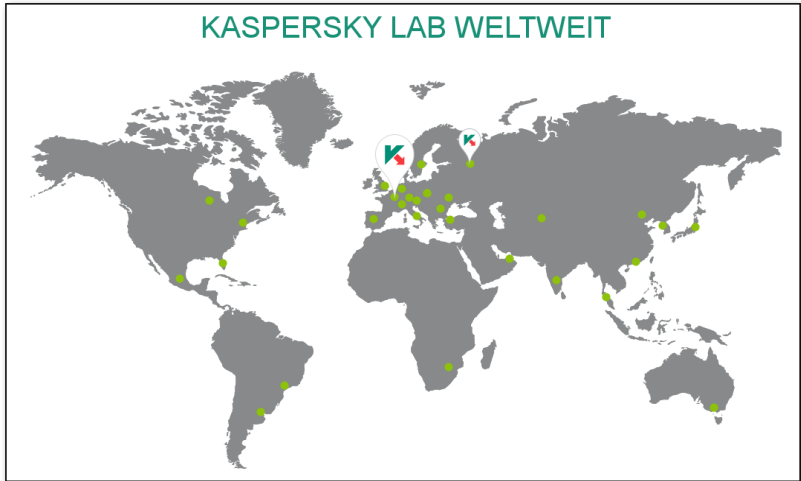
Kaspersky Lab Global <http://www.kaspersky.com/about>

KASPERSKY LAB FAKTEN



Eugene Kaspersky

KASPERSKY LABS GEOGRAFIE



> aktiv in 200 Ländern und Gebieten mit 33 Niederlassungen

AUSZUG PARTNER



> viele Lösungen nutzen Kaspersky als Malware-Scanner

KASPERSKY LABS GMBH

- > Sitz der Kaspersky Labs GmbH in Ingolstadt
- > ca. 150 Mitarbeiter
- > deutschsprachiger Support
- > ...

 Kaspersky Labs GmbH <http://www.kaspersky.com/de/?domain=www.kaspersky.de>

KASPERSKY LABS GMBH

- > Sitz der Kaspersky Labs GmbH in Ingolstadt
- > ca. 150 Mitarbeiter
- > deutschsprachiger Support
- > ...



Kaspersky Labs GmbH [http:](http://www.kaspersky.com/de/?domain=www.kaspersky.de)

[//www.kaspersky.com/de/?domain=www.kaspersky.de](http://www.kaspersky.com/de/?domain=www.kaspersky.de)

KASPERSKY LABS GMBH

- > Sitz der Kaspersky Labs GmbH in Ingolstadt
- > ca. 150 Mitarbeiter
- > deutschsprachiger Support
- > ...

 Kaspersky Labs GmbH <http://www.kaspersky.com/de/?domain=www.kaspersky.de>

KASPERSKY LABS GMBH

- > Sitz der Kaspersky Labs GmbH in Ingolstadt
- > ca. 150 Mitarbeiter
- > deutschsprachiger Support
- > ...



Kaspersky Labs GmbH [http:](http://www.kaspersky.com/de/?domain=www.kaspersky.de)

[//www.kaspersky.com/de/?domain=www.kaspersky.de](http://www.kaspersky.com/de/?domain=www.kaspersky.de)

KASPERSKY LABS GMBH

- > Sitz der Kaspersky Labs GmbH in Ingolstadt
- > ca. 150 Mitarbeiter
- > deutschsprachiger Support
- > ...



Kaspersky Labs GmbH [http:](http://www.kaspersky.com/de/?domain=www.kaspersky.de)

[//www.kaspersky.com/de/?domain=www.kaspersky.de](http://www.kaspersky.com/de/?domain=www.kaspersky.de)

SYSTEME MIT KASPERSKY ABSICHERN

Wie kann ich betroffene Systeme mit Kaspersky absichern?

WEITERE LINUXPRODUKTE VON KASPERSKY LAB

Übersicht über Linuxprodukte

KASPERSKY ANTI-VIRUS FÜR LINUX FILE SERVER

The screenshot shows the Kaspersky Web Management Console for Linux File Server in a Mozilla Firefox browser. The interface is in English and shows a 'Protected' status. A green circle highlights the 'Summary' link in the top navigation bar. The left sidebar contains a menu with the following items: Summary, Real-time protection, On-demand scan, Update, Quarantine, Backup, Reports, Log, License, General settings, and Notifications. The main content area displays four summary cards:

- Real-time protection**

Status	Running
Objects detected	356
- Update**

Status	OK
Last update	19/03/2015 00:18:03
Update published	18/03/2015 17:08:00
- License**

Status	License is valid
Expiration date	03/12/2015
Days left	260 days
- Quarantine**

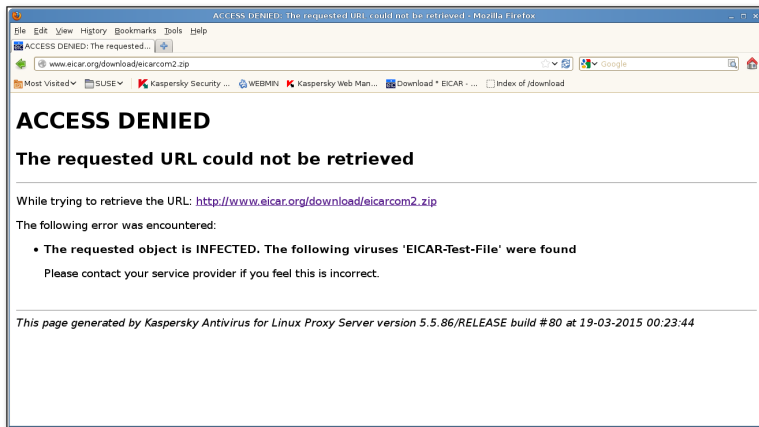
Objects	614
Quarantine size	15.05 MB



Informationen:

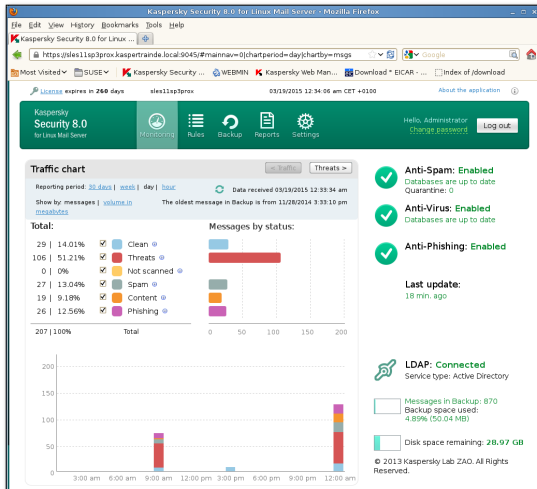
http://support.kaspersky.com/linux_file80

KASPERSKY ANTI-VIRUS 5.5 FOR PROXY SERVER



Informationen: <http://support.kaspersky.com/proxy5>

KASPERSKY SECURITY 8.0 FOR LINUX MAIL SERVER



Informationen: <http://support.kaspersky.com/klms8>

AMAVIS PROJEKT

Kurze Beschreibung zum AMaViS Projekt

INFORMATIONEN ZU AMAVIS

Beschreibung zu AMaViS

- > **AMaViS** steht für **A MAIL Virus Scanner**
- > **AMaViS** ist **kein Virens Scanner** in eigentlichen Sinne
- > Software zur Einbindung von Virens Scanner auf Mailserver
- > Standardschnittstelle zwischen den Mail Transfer Agents (MTA) und den Contentfiltern (aktuell in Perl geschrieben)
- > kompatibel mit Postfix, sendmail oder Exim
- > Einbindung ein oder mehrerer Antivirenprogramme
- > Anti-Spam-Software kann optional eingebunden werden

 Quelle <http://de.wikipedia.org/wiki/Amavis>

 Projekt <http://www.amavis.org/>

AMAVIS

- > **AMaViS** steht für **A MAIL Virus Scanner**
- > **AMaViS** ist **kein Virens Scanner** in eigentlichen Sinne
- > Software zur Einbindung von Virens Scanner auf Mailserver
- > Standardschnittstelle zwischen den Mail Transfer Agents (MTA) und den Contentfiltern (aktuell in Perl geschrieben)
- > kompatibel mit Postfix, sendmail oder Exim
- > Einbindung ein oder mehrerer Antivirenprogramme
- > Anti-Spam-Software kann optional eingebunden werden

🌐 Quelle <http://de.wikipedia.org/wiki/Amavis>

🌐 Projekt <http://www.amavis.org/>

AMAVIS

- > **AMaViS** steht für **A MAIL Virus Scanner**
- > **AMaViS** ist **kein Virens Scanner** in eigentlichen Sinne
- > Software zur Einbindung von Virens Scanner auf Mailserver
- > Standardschnittstelle zwischen den Mail Transfer Agents (MTA) und den Contentfiltern (aktuell in Perl geschrieben)
- > kompatibel mit Postfix, sendmail oder Exim
- > Einbindung ein oder mehrerer Antivirenprogramme
- > Anti-Spam-Software kann optional eingebunden werden

🌐 Quelle <http://de.wikipedia.org/wiki/Amavis>

🌐 Projekt <http://www.amavis.org/>

AMAVIS

- > **AMaViS** steht für **A MAil Virus Scanner**
- > **AMaViS** ist **kein Virens Scanner** in eigentlichen Sinne
- > Software zur Einbindung von Virens Scanner auf Mailserver
- > Standardschnittstelle zwischen den Mail Transfer Agents (MTA) und den Contentfiltern (aktuell in Perl geschrieben)
- > kompatibel mit Postfix, sendmail oder Exim
- > Einbindung ein oder mehrerer Antivirenprogramme
- > Anti-Spam-Software kann optional eingebunden werden

🌐 Quelle <http://de.wikipedia.org/wiki/Amavis>

🌐 Projekt <http://www.amavis.org/>

AMAVIS

- > **AMaViS** steht für **A MAIL Virus Scanner**
- > **AMaViS** ist **kein Virens Scanner** in eigentlichen Sinne
- > Software zur Einbindung von Virens Scanner auf Mailserver
- > Standardschnittstelle zwischen den Mail Transfer Agents (MTA) und den Contentfiltern (aktuell in Perl geschrieben)
- > kompatibel mit Postfix, sendmail oder Exim
- > Einbindung ein oder mehrerer Antivirenprogramme
- > Anti-Spam-Software kann optional eingebunden werden

🌐 Quelle <http://de.wikipedia.org/wiki/Amavis>

🌐 Projekt <http://www.amavis.org/>

AMAVIS

- > **AMaViS** steht für **A MAil Virus Scanner**
- > **AMaViS** ist **kein Virens Scanner** in eigentlichen Sinne
- > Software zur Einbindung von Virens Scanner auf Mailserver
- > Standardschnittstelle zwischen den Mail Transfer Agents (MTA) und den Contentfiltern (aktuell in Perl geschrieben)
- > kompatibel mit Postfix, sendmail oder Exim
- > Einbindung ein oder mehrerer Antivirenprogramme
- > Anti-Spam-Software kann optional eingebunden werden

🌐 Quelle <http://de.wikipedia.org/wiki/Amavis>

🌐 Projekt <http://www.amavis.org/>

AMAVIS

- > **AMaViS** steht für **A MAil Virus Scanner**
- > **AMaViS** ist **kein Virens Scanner** in eigentlichen Sinne
- > Software zur Einbindung von Virens Scanner auf Mailserver
- > Standardschnittstelle zwischen den Mail Transfer Agents (MTA) und den Contentfiltern (aktuell in Perl geschrieben)
- > kompatibel mit Postfix, sendmail oder Exim
- > Einbindung ein oder mehrerer Antivirenprogramme
- > Anti-Spam-Software kann optional eingebunden werden

🌐 Quelle <http://de.wikipedia.org/wiki/Amavis>

🌐 Projekt <http://www.amavis.org/>

AMAVIS

- > **AMaViS** steht für **A MAIL Virus Scanner**
- > **AMaViS** ist **kein Virens Scanner** in eigentlichen Sinne
- > Software zur Einbindung von Virens Scanner auf Mailserver
- > Standardschnittstelle zwischen den Mail Transfer Agents (MTA) und den Contentfiltern (aktuell in Perl geschrieben)
- > kompatibel mit Postfix, sendmail oder Exim
- > Einbindung ein oder mehrerer Antivirenprogramme
- > Anti-Spam-Software kann optional eingebunden werden

 Quelle <http://de.wikipedia.org/wiki/Amavis>

 Projekt <http://www.amavis.org/>

- > **AMaViS** steht für **A MAIL Virus Scanner**
- > **AMaViS** ist **kein Virens scanner** in eigentlichen Sinne
- > Software zur Einbindung von Virens scanner auf Mailserver
- > Standardschnittstelle zwischen den Mail Transfer Agents (MTA) und den Contentfiltern (aktuell in Perl geschrieben)
- > kompatibel mit Postfix, sendmail oder Exim
- > Einbindung ein oder mehrerer Antivirenprogramme
- > Anti-Spam-Software kann optional eingebunden werden

 Quelle <http://de.wikipedia.org/wiki/Amavis>

 Projekt <http://www.amavis.org/>

AMAVIS UND KASPERSKY VS. MALWARE

Der Einsatz von AMaViS und Kaspersky zum Schutz gegen Malware

INTEGRATION AMAVIS UND KASPERSKY

Beispiel der Integration mit CentOS 7.0.1406

INSTALLATION VON AMAVIS UNTER CENTOS 7

1 Installation Epel:

2 `yum install epel-release`

4 Repository Epel aktivieren:

5 `yum --enablerepo=epel`

7 Installation Amavis und ClamAV:

8 `yum -y install amavisd-new clamav-server clamav-server-systemd`

EINRICHTUNG VON AMAVIS UNTER CENTOS 7 TEIL I

```
1  Kopieren der Datei clamd.amavisd:
2  cp /usr/share/doc/clamav-server*/clamd.sysconfig /etc/sysconfig.)
   /clamd.amavisd

4  vi /etc/sysconfig/clamd.amavisd
5  2 Zeilen hinzufügen:
6  CLAMD_CONFIGFILE=/etc/clamd.d/amavisd.conf
7  CLAMD_SOCKET=/var/run/clamd.amavisd/clamd.sock

9  vi /etc/tmpfiles.d/clamd.amavisd.conf
10 1 Zeile hinzufügen:
11 d /var/run/clamd.amavisd 0755 amavis amavis -

13 vi /usr/lib/systemd/system/clamd@.service
14 2 Zeilen hinzufügen:
15 [Install]
16 WantedBy=multi-user.target

18 Dienst starten und aktivieren:
19 systemctl start clamd@amavisd
20 systemctl enable clamd@amavisd
```

EINRICHTUNG VON AMAVIS UNTER CENTOS 7 TEIL II

```
1 vi /etc/amavisd/amavisd.conf
2   Name der Domäne anpassen:
3   $mydomain = 'server.world';

4
5   Name vom Rechner anpassen:
6   $myhostname = 'mail.server.world';

7
8   2 Zeilen auskommentieren:
9   $notify_method = 'smtp:[127.0.0.1]:10025';
10  $forward_method = 'smtp:[127.0.0.1]:10025';

11
12  Dienst starten und aktivieren:
13  systemctl start amavisd
14  systemctl enable amavisd
15  systemctl start spamassassin
16  systemctl enable spamassassin
```

EINRICHTUNG POSTFIX TEIL I

```
1 vi /etc/postfix/master.cf
2   Zeilen am Ende hinzufügen:
3 smtp-amavis unix      -      n      -      2 smtp
4     -o smtp_data_done_timeout=1200
5     -o smtp_send_xforward_command=yes
6     -o disable_dns_lookups=yes
7 127.0.0.1:10025 inet    n      -      n      -      - smtpd
8     -o content_filter=
9     -o local_recipient_maps=
10    -o relay_recipient_maps=
11    -o smtpd_restriction_classes=
12    -o smtpd_client_restrictions=
13    -o smtpd_helo_restrictions=
14    -o smtpd_sender_restrictions=
15    -o smtpd_recipient_restrictions=permit_mynetworks,reject
16    -o mynetworks=127.0.0.0/8
17    -o strict_rfc821_envelopes=yes
18    -o smtpd_error_sleep_time=0
19    -o smtpd_soft_error_limit=1001
20    -o smtpd_hard_error_limit=1000
```

EINRICHTUNG POSTFIX TEIL II

```
1 vi /etc/postfix/main.cf
2   1 Zeile hinzufügen:
3   content_filter=smtp-amavis:[127.0.0.1]:10024
4
5   Dienst neustarten:
6   systemctl restart postfix
```

INSTALLATION UND KONFIGURATION AMAVIS DOKU

- > ...
- > Bitte selber testen!
- > Für die Richtigkeit der Angaben ...

 CentOS 7 AMaViS HowTo

http://www.server-world.info/en/note?os=CentOS_7&p=mail&f=6

INSTALLATION UND KONFIGURATION AMAVIS DOKU

- > ...
- > Bitte selber testen!
- > Für die Richtigkeit der Angaben ...

 CentOS 7 AMaViS HowTo

http://www.server-world.info/en/note?os=CentOS_7&p=mail&f=6

INSTALLATION UND KONFIGURATION AMAVIS DOKU

- > ...
- > Bitte selber testen!
- > Für die Richtigkeit der Angaben ...

 CentOS 7 AMaViS HowTo

http://www.server-world.info/en/note?os=CentOS_7&p=mail&f=6

INSTALLATION UND KONFIGURATION AMAVIS DOKU

- > ...
- > Bitte selber testen!
- > Für die Richtigkeit der Angaben ...



CentOS 7 AMaViS HowTo

http://www.server-world.info/en/note?os=CentOS_7&p=mail&f=6

INSTALLATION KLMS 8

- > Sie können die Standardinstallation verwenden.
- > Bei der Integration vom MTA unbedingt „Manual integration“ verwenden!

```
1  Installation von KLMS durchführen:
2  rpm -i klms-8.0.1-705.i386.rpm
3
4  Konfiguration von KLMS durchführen:
5  /opt/kaspersky/klms/bin/klms-setup.pl
6  ...
7  Configuration script has found following MTA on this host:
8  1) Postfix
9  2) Manual integration
10 Please select MTA to integrate with, manual integration, or ↵
    Ctrl+C to abort
11 installation, or press Enter to use default [1]:
12 2
13 ...
```

INSTALLATION KLMS 8

- > Sie können die Standardinstallation verwenden.
- > Bei der Integration vom MTA unbedingt „**Manual integration**“ verwenden!

```
1  Installation von KLMS durchführen:
2  rpm -i klms-8.0.1-705.i386.rpm
3
4  Konfiguration von KLMS durchführen:
5  /opt/kaspersky/klms/bin/klms-setup.pl
6  ...
7  Configuration script has found following MTA on this host:
8  1) Postfix
9  2) Manual integration
10 Please select MTA to integrate with, manual integration, or ↵
    Ctrl+C to abort
11 installation, or press Enter to use default [1]:
12 2
13 ...
```

KONFIGURATION KLMS 8 (AMAVIS)

```
1  Benutzer den Gruppen hinzufügen:
2  gpasswd -a kluser amavis
3  gpasswd -a amavis klusers

4
5  vi /usr/sbin/amavisd
6  Einstellungen für den Anti-Spam-Filter anpassen:
7  ['SpamdClient', 'Amavis::SpamControl::SpamdClient' ]

8
9  my($spamd_handle) = Amavis::IO::RW->new(
10  [ '/var/run/klms/rds_asp' ], Eol => "\015\012", Timeout => 30);

11
12  vi /etc/amavisd/amavisd.conf
13  Das bestehende Limit erhöhen:
14  $sa_mail_body_size_limit = 1500000;
15  Eintrag für den Virens Scanner hinzufügen:
16  ### http://www.kaspersky.com/ (Kaspersky Security 8.0 for
    Linux Mail Server)
17  ['Kaspersky Security 8.0 for Linux Mail Server',
18  \&ask_daemon, ["nCONTSCAN {} \n", "/var/run/klms/rds_av"],
19  qr/\bOK$/m, qr/\bFOUND$/m,
20  qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],

21
22  Dienst neustarten:
23  systemctl restart amavisd
```

ÜBERPRÜFUNG DER KONFIGURATION

```
1 vi /etc/amavisd/amavisd.conf
2   Loglevel anpassen (Nur für den Test!):
3   $log_level = 5;                # verbosity 0..5, -d
4
5   Datei /var/log/maillog mitschneiden:
6   tail -f /var/log/maillog
7
8   Mar 18 18:24:48 centos701 amavis[20577]: (20577-03) Blocked  ↵
9   INFECTED
10  (UDS: DangerousObject.Multi.Generic) {DiscardedInternal, ↵
11   Quarantined}, MYNETS
12  LOCAL [::1]:36690 <rimme@centos701.kaspertrainde.local> ->
13  <rimme@localhost.kaspertrainde.local>, quarantine: virus- ↵
14  vKFs8lNsYWpe,
15  Queue-ID: 88D274300D2D, Message-ID: <20150318172447. ↵
16  GA21399@centos701.kaspertrainde.local>, mail_id: ↵
17  vKFs8lNsYWpe, Hits: -, size: 316585, 564 ms
```

DARSTELLUNG EINER E-MAIL



```

Von: Content-filter at centos701.kaspertrainsde.local <postmaster@centos701.kaspertrainsde.local>
Betreff: VIRUS [UDS: DangerousObject.Multi.Generic] in mail FROM LOCAL [::1]:36690 <romeo@centos701.kaspertrainsde.local>
An: romeo@centos701.kaspertrainsde.local

A virus was found: UDS: DangerousObject.Multi.Generic
Banned name: application/octet-stream,.exe,.exe-ms,ksn.exe
Scanner detecting a virus: Kaspersky Security 8.0 for Linux Mail Server
Content type: Virus
Internal reference code for the message is 20577-03/vKFs8lNoYqpe
First upstream SMTP client IP address: [::1]:36690 localhost
Received from: ::1

Return-Path: <romeo@centos701.kaspertrainsde.local>
From: Roland Issee <romeo@centos701.kaspertrainsde.local>
Message-ID: <20150318172447.6A21399@centos701.kaspertrainsde.local>
Subject: KSN-Test
The message has been quarantined-as-virus-03Fs8lNoYqpe

The message WAS NOT relayed to:
<romeo@localhost.kaspertrainsde.local>:
 250 2.7.0 Ok, discarded, id=20577-03 - INFECTED: UDS: DangerousObject.Multi.Generic

Virus scanner output:
p002: UDS: DangerousObject.Multi.Generic FOUND
p004: UDS: DangerousObject.Multi.Generic FOUND

--header--

Return-Path: <romeo@centos701.kaspertrainsde.local>
Received: from localhost (localhost [IPv6::1])
@ 5 Antivirus Scanner 1015 Status

```


INSTALLATION KLMS 8 DOKU

- > Einstellungen können über Kommandozeile angepasst werden

```
1 /opt/kaspersky/klms/bin/klms-control --help
```

> ...



Handbuch KLMS

http://docs.kaspersky-labs.com/english/klms8.0_linux_adminguide_en.pdf

INSTALLATION KLMS 8 DOKU

- > Einstellungen können über Kommandozeile angepasst werden

```
1 /opt/kaspersky/klms/bin/klms-control --help
```

> ...



Handbuch KLMS

http://docs.kaspersky-labs.com/english/klms8.0_linux_adminguide_en.pdf

INSTALLATION KLMS 8 DOKU

- > Einstellungen können über Kommandozeile angepasst werden

```
1 /opt/kaspersky/klms/bin/klms-control --help
```

- > ...



Handbuch KLMS

http://docs.kaspersky-labs.com/english/klms8.0_linux_adminguide_en.pdf

INSTALLATION KLMS 8 DOKU

- > Einstellungen können über Kommandozeile angepasst werden

```
1 /opt/kaspersky/klms/bin/klms-control --help
```

- > ...



Handbuch KLMS

http://docs.kaspersky-labs.com/english/klms8.0_linux_adminguide_en.pdf

LIVE DEMO



FRAGEN



DANKE