KASPERSKY lab

AMAVIS UND KASPERSKY VS. MALWARE

Vortrag Linux Tag Chemnitz 2014

Roland Imme
Senior Technical Sales Engineer

THEMEN

3 Wo geht die Reise hin?

16 Infektionswege

19 AMaViS Projekt

22 Kaspersky Lab

28 AMaViS und Kaspersky vs. Malware und Spam

42 Mehr Lösungen

KASPERSKY lab

WO GEHT DIE REISE HIN?

Wir stellen die Trends der Malware-Strategien vor.

ALLGEMEINE BEDROHUNGSLAGE

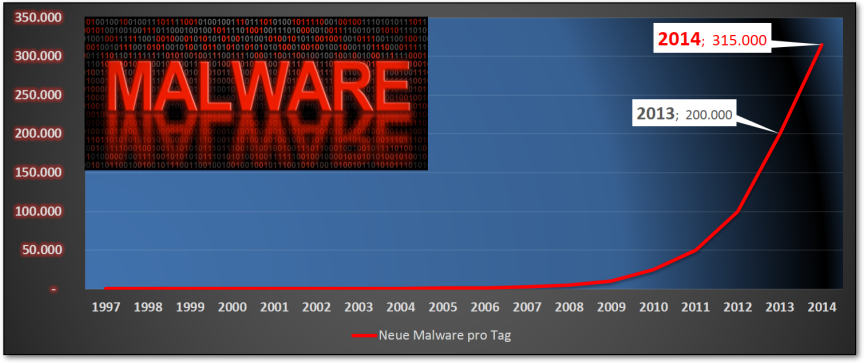
Zahlen und Fakten zur allgemeinen Bedrohungslage

BEDROHUNGEN FÜR ANWENDER

Copyright © 2014 Kaspersky Labs GmbH

EXPONENTIELLER ANSTIEG VON MALWARE …

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



Copyright © 2014 Kaspersky Labs GmbH

2013 IN ZAHLEN

- 5.188.740.554 durch Kaspersky Lab (Kaspersky Security Network) entdeckte Angriffe auf Computer und Mobile Geräte
- 104.427 neue Modifikationen von mobiler Malware
- 1.700.870.654 durch Kaspersky Lab neutralisierte Angriffe von Online Quellen
- …

Copyright © 2014 Kaspersky Labs GmbH

PROGNOSEN 2014

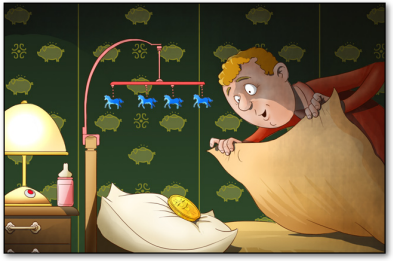
Wo geht die Reise hin?

MOBILE BEDROHUNGEN

- Weiterentwicklung von trojanischen Programmen für mobile Endgeräte
- Focus auf das Betriebssystem Android
- Verschlüsselung von Anwenderdaten auf dem Smartphone
- mobiles Phishing mit „Banking“-Trojaner
- Handel mit mobilen Botnetzen

Copyright © 2014 Kaspersky Labs GmbH

ATTACKEN AUF BITCOIN



- Attacken auf Bitcoin-Pools, Börsen und Nutzer von Bitcoins werden zunehmen
- Risiko von Attacken, die den Diebstahl der Wallets zum Ziel haben
- Angreifer können enorme Gewinne bei vollständiger Anonymität erzielen

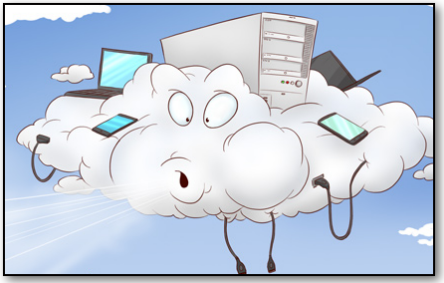
Copyright © 2014 Kaspersky Labs GmbH

PROBLEME BEIM SCHUTZ DES PRIVATLEBENS

- Anwender möchten ihr Privatleben vor den Geheimdiensten dieser Welt schützen
- Schutz kann nicht gewährleistet werden, wenn Internet-Dienste nicht die entsprechenden Maßnahmen ergreifen
- zum Beispiel Betreiber von Soziale Netzwerke, E-Mail-Provider und Cloud-Speicher
- verfügbare Schutzmethoden sind nicht ausreichend
- Anwender muss selbständig Maßnahmen ergreifen
  - Nutzung von VPN-Services, Tor-Anonymisierer und Verschlüsselungswerkzeugen

Copyright © 2014 Kaspersky Labs GmbH

ANGRIFFE AUF CLOUD-SPEICHER



- Vertrauen in Cloud-Speicherdienste wankt (Enthüllungen durch Edward Snowden)
- gespeicherte Daten sind zunehmend attraktives Ziel für Hacker
- Hacker werden zielgerichtet das schwächste Glied in der Kette angreifen (Mitarbeiter von Cloud-Services)

Copyright © 2014 Kaspersky Labs GmbH

ATTACKEN AUF SOFTWARE-ENTWICKLER

- Zunahme der Angriffe auf Software-Entwickler für den Zugang zu sensiblen Daten
- 2013 deckten wir eine Angriffsserie auf Spiele-Entwickler auf, denen serverseitige Quellcodes von Online-Games gestohlen wurden
- Opfer einer anderen Attacke wurde das Unternehmen Adobe
  - Quellcodes von Adobe Acrobat und ColdFusion wurden gestohlen
- Diebstahl von Quellcodes gängiger Produkte eröffnet Angreifern perfekte Möglichkeiten bei der Suche nach Sicherheitslücken

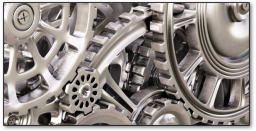
Copyright © 2014 Kaspersky Labs GmbH

CYBERSÖLDNER

- Enthüllungen von Edward Snowden haben gezeigt, dass der Staat Cyberspionage betreibt, um „seinen“ Unternehmen zu helfen
- drastische Mittel im Konkurrenzkampf der Geschäftswelt
- Umsetzen kann die Geschäftswelt derartige Aktivität allerdings nur mit Hilfe von Cybersöldnern
  - organisierte Gruppen von qualifizierten Hackern

Copyright © 2014 Kaspersky Labs GmbH

FRAGMENTIERUNG DES INTERNETS



- Experten, insbesondere Eugene Kaspersky, sprechen von der Notwendigkeit, ein paralleles, „sicheres Internet“ zu schaffen
- keine Möglichkeit, dort anonym Straftaten zu begehen
- Fragmentierungsprozess des Internets in nationale Segmente
  - Beispiel: China mit seiner „Great Firewall of China“
  - Deutschland plant, die gesamte interne Kommunikation zwischen deutschen Behörden vollständig innerhalb des Landes abzuwickeln
- Tendenzen haben sich besonders nach den Veröffentlichungen von Edward Snowden ergeben

Copyright © 2014 Kaspersky Labs GmbH

KASPERSKY lab

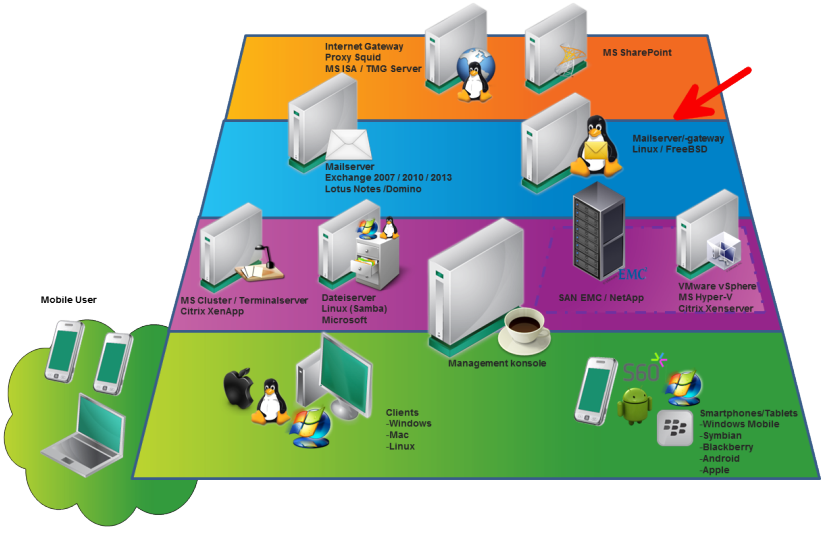
INFEKTIONSWEGE

Mögliche Wege einer Infektion mit Malware

INFORMATIONEN ZU INFEKTIONSWEGEN

Wie dringt Malware im Netz ein?

MÖGLICHE INFEKTIONSWEGE VON MALWARE



Copyright © 2014 Kaspersky Labs GmbH

KASPERSKY lab

AMAVIS PROJEKT

Kurze Beschreibung zum AMaViS Projekt

INFORMATIONEN ZU AMAVIS

Beschreibung zu AMaViS

AMAVIS

- AMaViS steht für A MAil Virus Scanner
- AMaViS ist kein Virenscanner in eigentlichen Sinne
- Software zur Einbindung von Virenscanner auf Mailserver
- Standardschnittstelle zwischen den Mail Transfer Agents (MTA) und den Contentfiltern (akuell 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/

Copyright © 2014 Kaspersky Labs GmbH

KASPERSKY LAB

Informationen zum Unternehmen Kaspersky LAB

KASPERSKY LAB FAKTEN IN KÜRZE

Allgemeine Informationen zum Unternehmen Kaspersky Lab

KASPERSKY LAB FAKTEN

Eugene Kaspersky

Copyright © 2014 Kaspersky Labs GmbH

KASPERSKY LABS GEOGRAFIE

> aktiv in fast 200 Ländern und Gebieten mit 30 Niederlassungen

Copyright © 2014 Kaspersky Labs GmbH

AUSZUG PARTNER

> viele Lösungen nutzen Kaspersky als Malware-Scanner

Copyright © 2014 Kaspersky Labs GmbH

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

Copyright © 2014 Kaspersky Labs GmbH

KASPERSKY lab

AMAVIS UND KASPERSKY VS. MALWARE UND SPAM

Vorgehensweise zur Integration beider Produkte

INTEGRATION AMAVIS UND KASPERSKY

Beispiel der Integration mit CentOS 6.5

INSTALLATION VON AMAVIS UNTER CENTOS

```
1 yum install clamav clamav-devel clamd spamassassin

3 gpasswd -a clamav amavis
```


Copyright © 2014 Kaspersky Labs GmbH

KONFIGURATION AMAVISD-NEW

```
1  vi /etc/amavisd.conf

3  ###http://www.clamav.net/
4  ['ClamAV-clamd',
5    \&ask_daemon, ["CONTSCAN {}\n", "/var/run/clamav/clamd.sock"
       ],
6    qr/\bOK$/, qr/\bFOUND$/,
7    qr/^.*?: (?!Infected Archive)(.*) FOUND$/ ],

9  freshclam

11 /etc/init.d/amavisd restart
```


Copyright © 2014 Kaspersky Labs GmbH

KONFIGURATION POSTFIX I

```
1 vi /etc/postfix/master.cf

3 amavisfeed unix    -       -       n       -       2       lmtp
4 -o lmtp_data_done_timeout=1200
5 -o lmtp_send_xforward_command=yes
6 -o disable_dns_lookups=yes
7 -o max_use=20
```


Copyright © 2014 Kaspersky Labs GmbH

KONFIGURATION POSTFIX II

```
127.0.0.1:10025 inet n    -       n       -       -     smtpd
    -o content_filter=
    -o smtpd_delay_reject=no
    -o smtpd_client_restrictions=permit_mynetworks,reject
    -o smtpd_helo_restrictions=
    -o smtpd_sender_restrictions=
    -o smtpd_recipient_restrictions=permit_mynetworks,reject
    -o smtpd_data_restrictions=reject_unauth_pipelining
    -o smtpd_end_of_data_restrictions=
    -o smtpd_restriction_classes=
    -o mynetworks=127.0.0.0/8
    -o smtpd_error_sleep_time=0
    -o smtpd_soft_error_limit=1001
    -o smtpd_hard_error_limit=1000
    -o smtpd_client_connection_count_limit=0
    -o smtpd_client_connection_rate_limit=0
    -o receive_override_options=no_header_body_checks,no_unknown_recipient_checks,no_milters,
        no_address_mappings
    -o local_header_rewrite_clients=
    -o smtpd_milters=
    -o local_recipient_maps=
    -o relay_recipient_maps=
```


Copyright © 2014 Kaspersky Labs GmbH

KONFIGURATION POSTFIX III

```
1 vi /etc/postfix/main.cf

3 content_filter=amavisfeed:[127.0.0.1]:10024

5 /etc/init.d/postfix reload
```


Copyright © 2014 Kaspersky Labs GmbH

INSTALLATION UND KONFIGURATION AMAVIS DOKU

> ...

- CentOS AMaViS HowTo
  http://wiki.centos.org/HowTos/Amavisd#head-c3a900408d68ddadef730bf8b540e13dcd9afae9

Copyright © 2014 Kaspersky Labs GmbH

INSTALLATION KLMS 8

```
1  rpm -i klms-8.0.1-705.i386.rpm

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


Copyright © 2014 Kaspersky Labs GmbH

KONFIGURATION KLMS 8 I

```
1  gpasswd -a kluser amavis

3  gpasswd -a amavis klusers

5  vi /usr/sbin/amavisd

7  ['SpamdClient', 'Amavis::SpamControl::SpamdClient' ]

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


Copyright © 2014 Kaspersky Labs GmbH

KONFIGURATION KLMS 8 II

```
vi /etc/amavisd.conf

$sa_mail_body_size_limit = 1500000;

  ### http://www.kaspersky.com/  (Kaspersky Security 8.0 for
      Linux Mail Server)
['Kaspersky Security 8.0 for Linux Mail Server',
\&ask_daemon, ["nCONTSCAN {}\n", "/var/run/klms/rds_av"],
qr/\bOK$/m, qr/\bFOUND$/m,
qr/^.*?: (?!Infected Archive)(.*) FOUND$/m ],


/etc/init.d/amavisd restart
```


Copyright © 2014 Kaspersky Labs GmbH

ÜBERPRÜFUNG DER KONFIGURATION

```
1 tail -f /var/log/maillog

3 Mar 15 16:28:14 centos65amavis amavis[3498]: (03498-03-10)
    Blocked INFECTED(Virus.DOS.KL-Demo) {DiscardedInbound,
    Quarantined}, <rimme@centos65amavis.fritz.box> -> <
    rimme@centos65amavis.fritz.box>, quarantine: virus-5
    aapE6ghTyzH, Message-ID: <20140315152812.
    GA21135@centos65amavis.fritz.box>, mail_id: 5aapE6ghTyzH,
    Hits: -, size: 1810, 343 ms
```


Copyright © 2014 Kaspersky Labs GmbH

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

Copyright © 2014 Kaspersky Labs GmbH

LIVE DEMO

Copyright © 2014 Kaspersky Labs GmbH

KASPERSKY lab

MEHR LÖSUNGEN

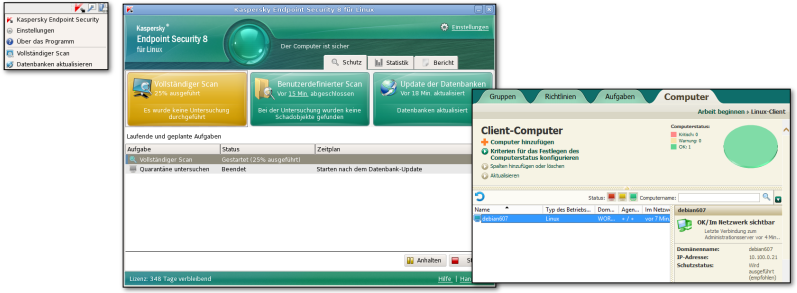
Weitere Lösungsansätze

WEITERE LINUXPRODUKTE VON KASPERSKY LAB

Übersicht über Linuxprodukte

KASPERSKY ENDPOINT SECURITY FÜR LINUX

- Echtzeit-Schutz auf Dateisystemebene und On Demand Scan

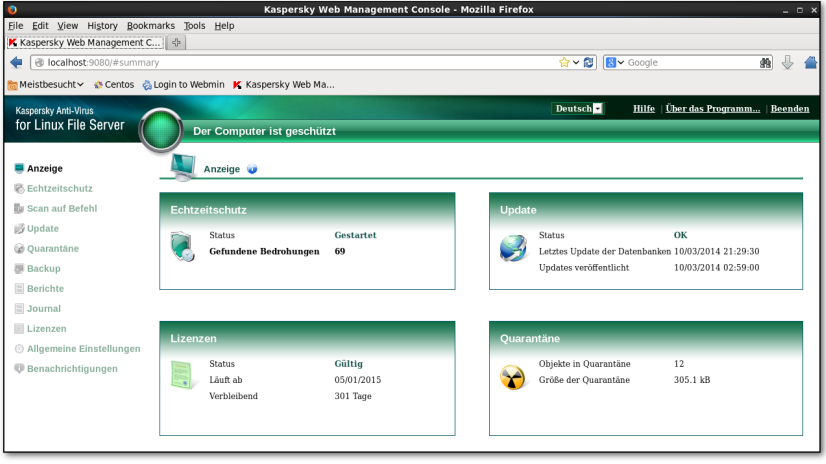


- komplette Virensignaturen (auch für Mac/Microsoft/Mobile/…)
- zentrale Verwaltung via Kaspersky Security Center

Informationen: `http://support.kaspersky.com/kes8linux`

Copyright © 2014 Kaspersky Labs GmbH

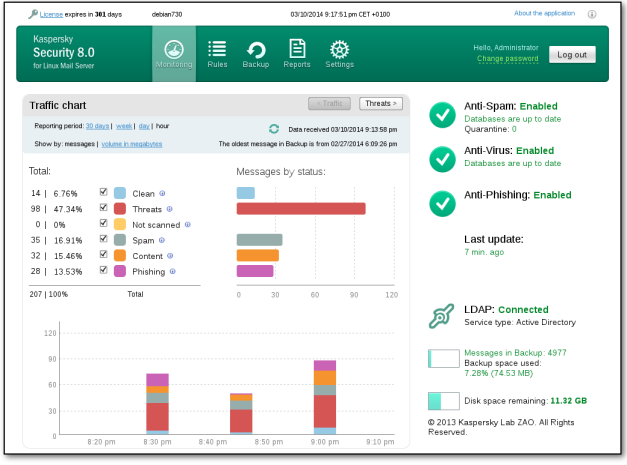
KASPERSKY ANTI-VIRUS FÜR LINUX FILE SERVER



- Informationen: http://support.kaspersky.com/linux_file80

Copyright © 2014 Kaspersky Labs GmbH

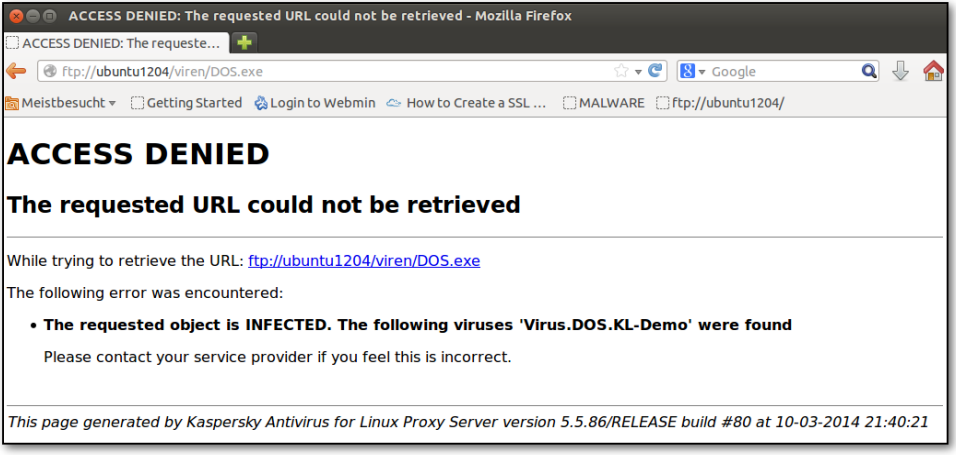
KASPERSKY SECURITY 8.0 FOR LINUX MAIL SERVER



- Informationen: http://support.kaspersky.com/klms8

Copyright © 2014 Kaspersky Labs GmbH

KASPERSKY ANTI-VIRUS 5.5 FOR PROXY SERVER



- Informationen: http://support.kaspersky.com/proxy5

Copyright © 2014 Kaspersky Labs GmbH

DANKE

KASPERSKY lab