Aufgabenstellung SN-Labor Versuch 1: Viren

Nachdem in den vorhergehenden Kapiteln Grundlagen zur sogenannten Malware, zu Techniken zum Schutz und die Funktionsweise der Programme erläutert wurden, werdet ihr während des Laborversuchs mit dem Virenscanner der Firma Kaspersky experimentieren, mit dem Anti-Trojaner-Programm Anti-Trojan, und der Firewall ZoneAlarm bekannt gemacht und arbeiten.
Screenshots sollten sofort gespeichert werden, damit im Falle eines Crashes nichts verloren geht.

Im Laufe des Labors sollen folgende Aufgaben gelöst werden:
1. Installieren des Virenscanners der Firma Kaspersky.
2. Einstellen des Virenscanners.
3. Scannen von Dateien / Untersuchung auf Infektionen.
4. Isolieren von Viren.
5. Suchen von Informationen über gefundenen Viren und Gefahreneinschätzung via Webrecherche (von zu Hause).
6. Einstellen und scannen mit einem Trojaner-Suchprogramm.
7. Welche Ports werden gescannt, für welche Dienste werden diese Ports verwendet? Warum werden gerade diese Ports gescannt?
8. Wie findet man Dateien mit doppelter Dateiendung, und wofür ist das wichtig?
9. Installieren und einstellen der Firewall.
10. Anpingen des Rechners anhand seiner IP-Nummer, einmal mit aktivierter Firewall des Nachbarrechners und einmal mit deaktivierter Firewall des Nachbarrechners.
11. Nun ist das kleine Virenquiz auszufüllen, welches im Ordner „Viren Know How“ auf dem Server zu finden ist.
12. Installieren weiterer Virenscanner (bitDefender, Sophos) und gleichzeitiges Scannen mit mehreren Virenscannern. Was passiert?

1. Installieren des Virenscanners der Firma Kaspersky

Um den Kaspersky Virenscanner zu installieren, wird das Installationsprogramm gestartet. Es können jeweils die vorgegebenen Einstellungen bestätigt werden. Nach der Installation erfolgt das Einstellen des Virenscanners.

2. Einstellen des Virenscanners

Hierzu wird der Kaspersky Virenscanner gestartet. Zum Einstellen des Scanners auf die Registerkarte „Einstellungen“ (siehe Abbildung 1) klicken.

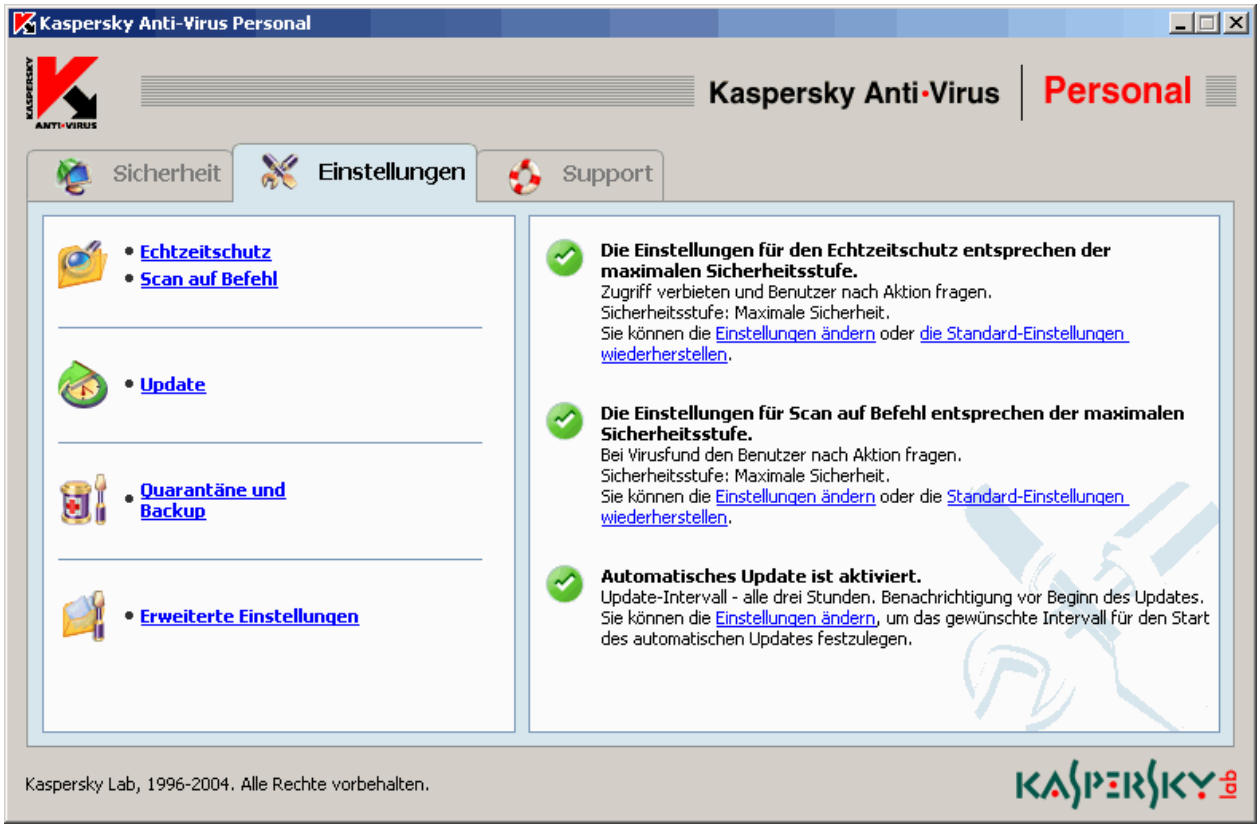

Abbildung 1 – Kaspersky Virenscanner „Registerkarte“ - Einstellungen

Im Bereich Einstellungen finden sich verschiedene Möglichkeiten um den Virenscanner bestmöglich zu konfigurieren.

Unter dem Punkt „Echtzeitschutz“ (siehe Abbildung 2) lässt sich der im Hintergrund laufende Virenscanner einstellen, der das System während der gesamten Laufzeit überwacht bzw. nach Viren scannt. Um zu erreichen, das der Virenscanner nicht nur für Viren besonders anfällige Dateitypen prüft, sondern auch „gepackte“ Dateien und Emails, wird die Sicherheitsstufe auf „Maximale Sicherheit“ gestellt. Um über jede Aktion des Virenscanners informiert zu werden sollte man noch die Einstellung „Zugriff verbieten und Benutzer nach Aktion fragen“ tätigen.
Bei den Einstellungen für „Scan auf Befehl“ (siehe Abbildung 3) sollte die gleiche Sicherheitsstufe (Maximale Sicherheit) gewählt werden, auch hier sollte der Benutzer über jede Aktion des Virenscanner informiert werden.

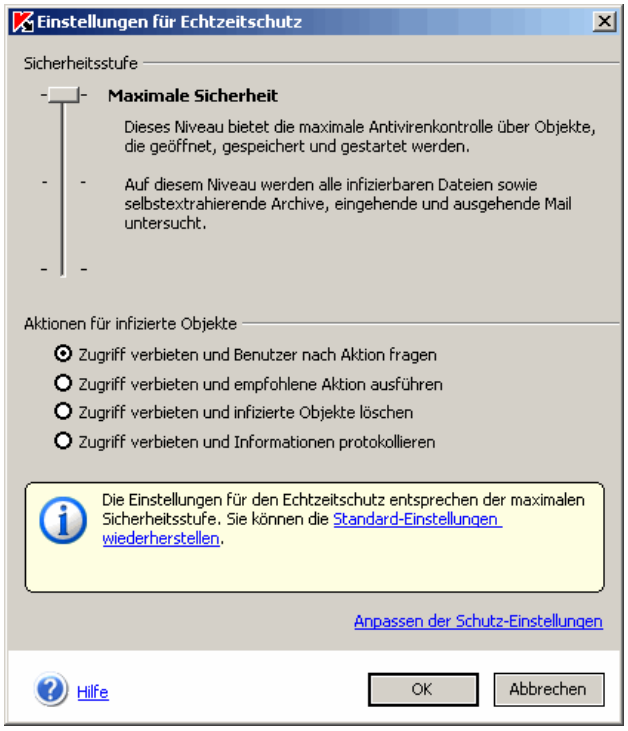

Abbildung 2 – Einstellungen für Echtzeitschutz

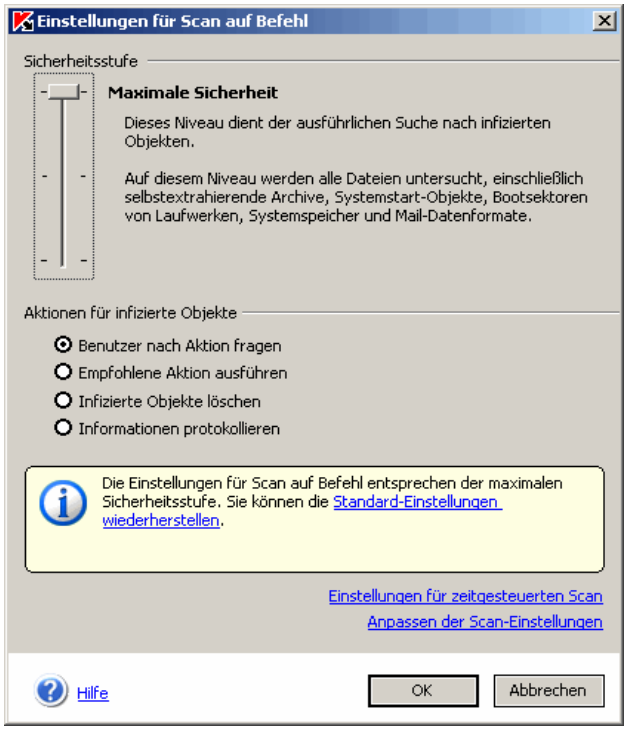

Abbildung 3 – Einstellungen für Scan auf Befehl

Der nächste Konfigurationspunkt sind die Einstellungen für die Update-Eigenschaften des Virenscanners (siehe Abbildung 4).
Die Update-Frequenz sollte auf mind. 3 Std. stehen, so wird gewährleistet dass die Virendefinition zumindest einmal am Tag aktualisiert wird. Auch das „Häkchen“ zur Benachrichtigung eines Updates sollte gesetzt werden, so wird der Benutzer vor einem neuem Update benachrichtigt.

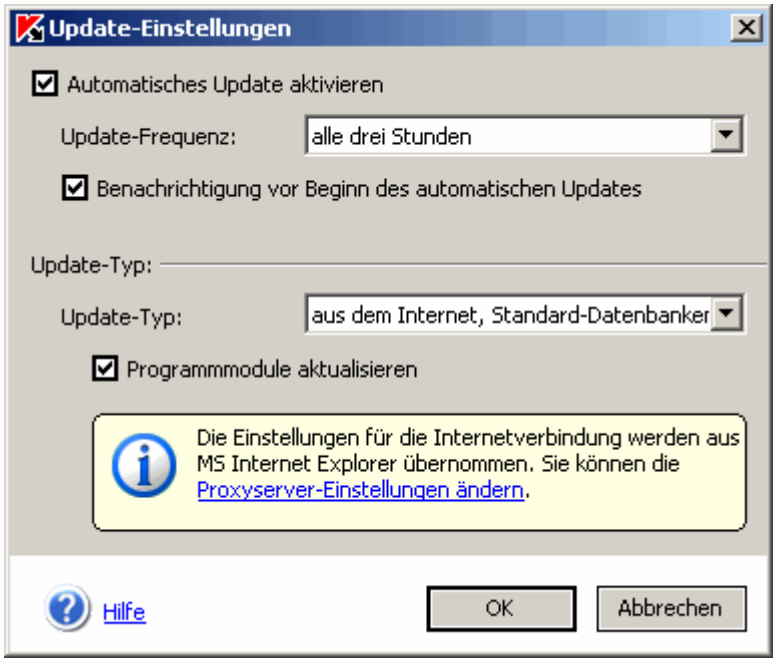

Abbildung 4 – Update-Einstellungen

Der nächste Einstellungspunkt des Virenscanners sind die Quarantäne Eigenschaften. Diese Funktion ist dafür da, infizierte Dateien in den so genannten „Quarantäne Ordner“ schieben zu können. Dies ist sinnvoll, wenn man die befallene Datei nicht reparieren kann, sie aber weiter benutzen möchte. Der Virenscanner koppelt die Datei von anderen Programmen ab bzw. der Zugriff wird verweigert, somit kann sich der Virus nicht weiter ausbreiten.
Das Häkchen sollte bei „Objekte in Quarantäne nach jedem Update der Antiviren-Datenbank automatisch untersuchen“ gesetzt werden.

Der letzte Einstellungspunkt des Virenscanners sind die „Erweiterten Einstellungen“ (siehe Abbildung 5). Hier sollte das Häkchen bei „Kaspersky Anti-Virus Personal bei Systemstart starten“ gesetzt werden. Somit wird gewährleistet, dass der „Echtzeitschutz“ des Virenscanners immer im Einsatz ist.
Die restlichen Einstellungen liegen im Ermessen des Benutzers, ob er z.B. „Akustische Signale verwenden“ will.

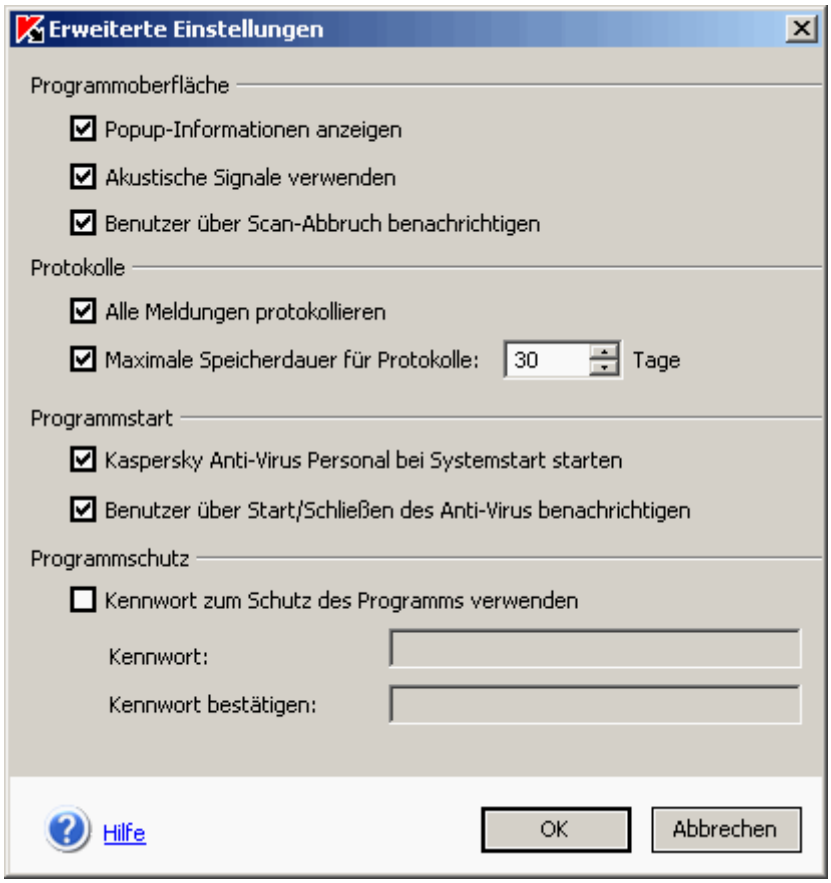

Abbildung 5 – Erweiterte Einstellungen

Jetzt ist die Konfiguration des Virenscanners abgeschlossen. Das System sollte nun nach Viren gescannt werden!

3. Scannen von Dateien / Untersuchung auf Infektionen

Das Scannen von Dateien geschieht auf zwei Arten:
Einmal gibt es die Möglichkeit, den Scanner im Hintergrund zu aktivieren (siehe Einstellungen für Echtzeitschutz). Alle Dateien und Programme, auf die auf dem Rechner zugegriffen werden, auf Viren geprüft (on access).

Die zweite Möglichkeit ist ein gezieltes Durchsuchen von Dateien, Ordnern oder Datenträgern. Diese Möglichkeit wird von Hand gestartet (on demand).
Möchte man das System, ein Laufwerk oder andere Objekte nach Viren durchsuchen, so findet man unter der Registerkarte „Sicherheit“ verschiedene Möglichkeiten.
Nachdem der Virenscanner zum ersten Mal auf dem Rechner installiert wurde, sollte man sich für das Scannen der gesamten Festplatte entscheiden.
Der Scannvorgang wird nun durch klicken auf „Untersuchen“ gestartet (siehe Abbildung 6 und Abbildung 7).

Abbildung 6 – Objekte untersuchen

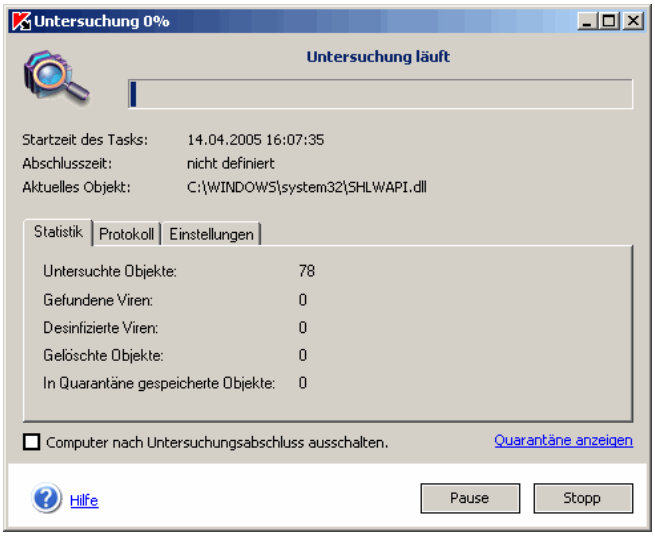

Abbildung 7 – Untersuchung läuft

Der Virenscanner durchsucht nun alle Dateien im angegebenen Ziel anhand einer Liste mit Beispielen aller ihm bekannten Viren und anderer schädlicher Software („Virensignaturen” oder „Virendefinitionen”), mit der er die zu überprüfende Software vergleicht.
Findet der Scanner dann schädliche Software, sendet Kaspersky eine Warnung, mit der Frage, was als nächstes geschehen soll.

Abbildung 8 – Viren Meldung

Die möglichen Optionen reichen da von Löschen der infizierten Datei über einen Reparaturversuch bis hin zur Quarantäne der Datei (siehe Abbildung 8).
Ist eine Desinfektion der Datei nicht möglich, so kann die Datei gelöscht werden oder es soll keine Aktion ausgeführt werden. Für Benutzer mit weniger Erfahrung, bietet das Programm eine empfohlene Aktion an.
Nach der abgeschlossenen Untersuchung erhält der Anwender einen Untersuchungsbericht (siehe Abbildung 9). Hier erhält man eine Übersicht über alle gefundenen Schädlinge im System.

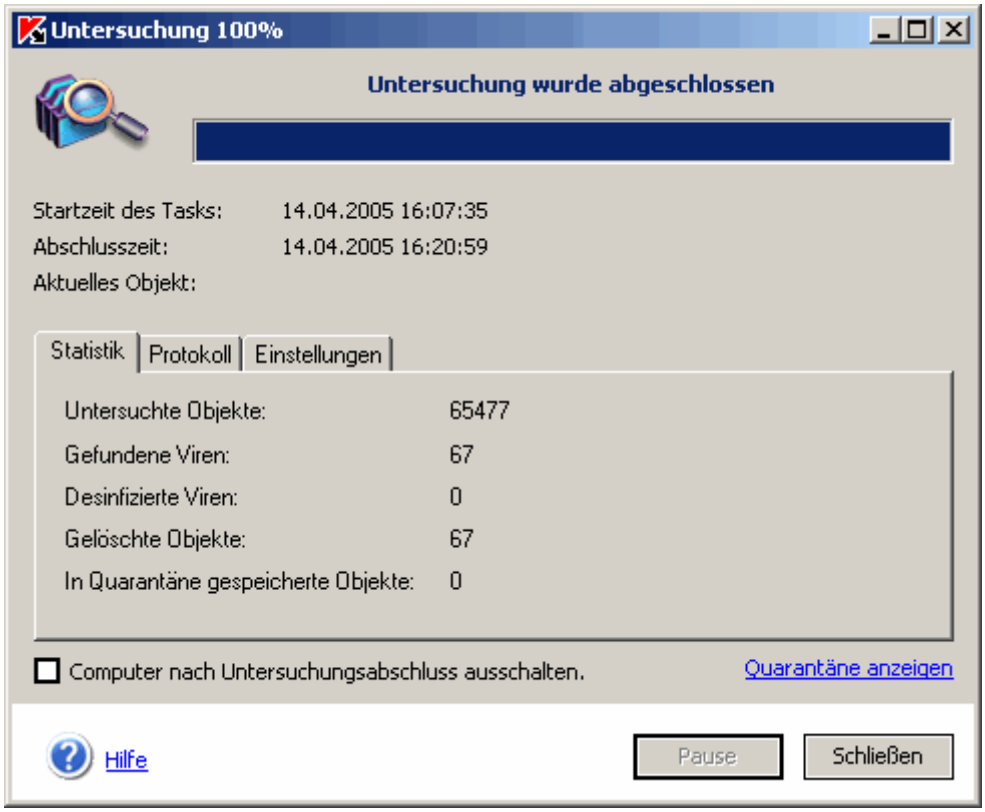

Abbildung 9 – Untersuchung wurde abgeschlossen

Einen Überblick, welche Aktion das Programm ausgeführt hat, erhält man unter der Registerkarte „Protokoll“ (siehe Abbildung 10).

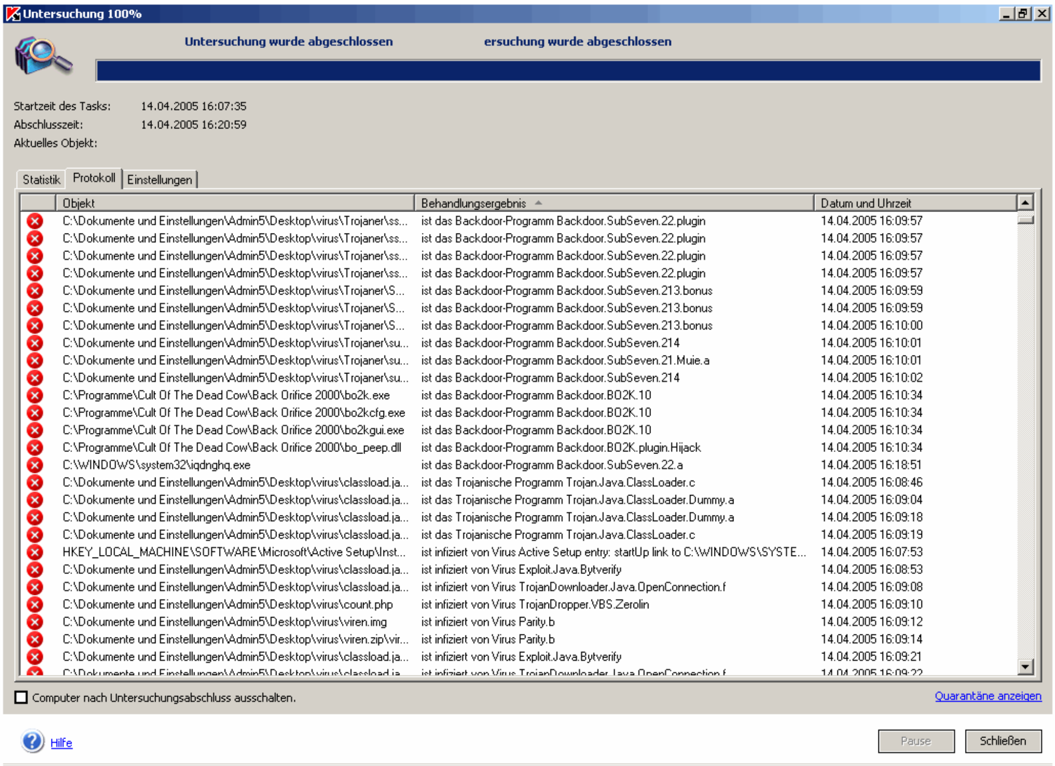

Abbildung 10 – Ansicht Protokoll

4. Isolieren von Viren

Kaspersky versucht die befallenen Dateien zu reparieren, wenn dies nicht gelingt zu isolieren (siehe Abbildung 11). Isolierte Dateien können keinen Schaden mehr anrichten (s. o. „3 - Erweiterte Einstellungen“).

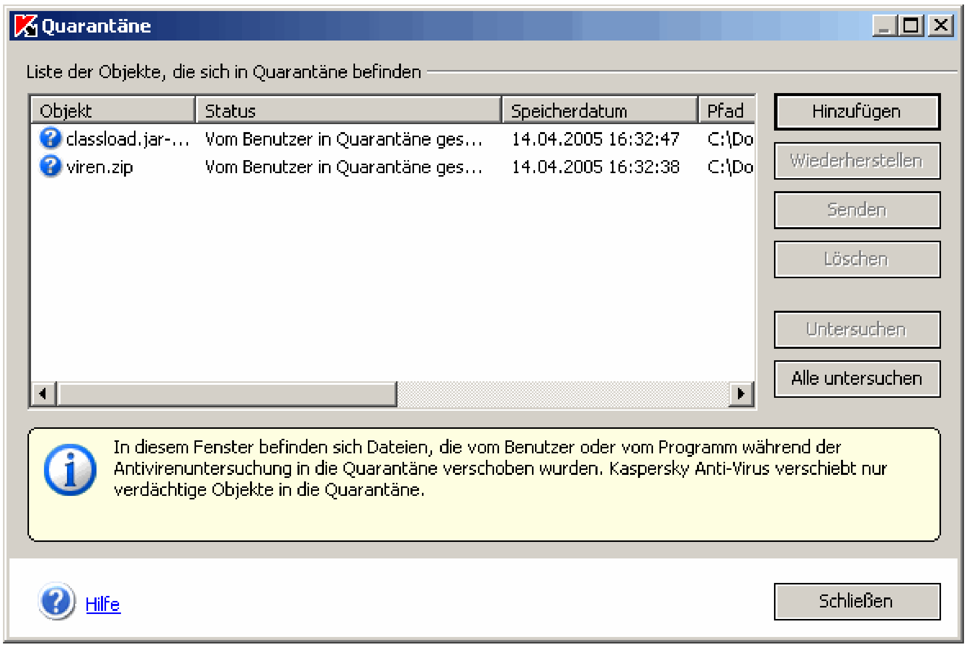

Abbildung 11 – Quarantäne

5. Suchen von Informationen über gefundene Viren und Gefahreneinschätzung via Webrecherche (von zu Hause)

BackOrifice2K.Trojan
BackOrifice2000 ist eine neue Version von BackOrifice.Trojan. Einmal auf einem MS Windows System installiert, erlaubt der Trojaner anderen Nutzern vollen Zugriff auf das System via Netzwerkverbindung zu erlangen. Ähnlich dem originalen BackOrifice besteht das Programm aus zwei Teilen: einem Server- und einem Client-Programm (Beide Programme laufen nun aber auch unter Windows NT). Durch das auf einem System installierte Client-Programm ist es möglich, ein anderes System mit laufendem Server-Programm zu überwachen und zu kontrollieren.
Die Portnummer, über die der Client den Server kontrolliert, ist frei konfigurierbar. Solange jedoch der Port durch eine Firewall blockiert wird, ist es dem Trojaner nicht möglich zum Server durchzudringen. Es macht dabei keinen Unterschied, ob das TCP- oder UDP-Protokoll verwendet wird. Bisher gab es noch keine Hinweise, dass das Programm eine Firewall durchbrechen konnte.
Der Trojaner ist als gefährlich einzustufen, da er sehr frei konfigurierbar ist und somit kein einheitliches Auftreten hat. Der Angreifer kann vom einfachen Neustart des Serverrechners über das Nachladen von Plug-Ins mit eventuell neuen Schadfunktionen bis zum Ausspionieren von Daten und Passwörtern auf eine breite Palette Schadfunktionen zugreifen.
Typ: Trojanisches Pferd, bekannt seit Juli 1999
Quelle: http://securityresponse.symantec.com/avcenter/venc/data/back.orifice.2000.trojan.html

6. Einstellen und scannen mit einem Trojaner-Suchprogramm
Anti-Trojan 5.5 installieren. Die vom Programm vorgegebenen Einstellungen wurden übernommen. Ledigleich bei der Suche wurde nach „Trojaner in der Registry“ und auf alle „Festplatten-Partitionen“ ausgewählt
(siehe Abbildung 12).

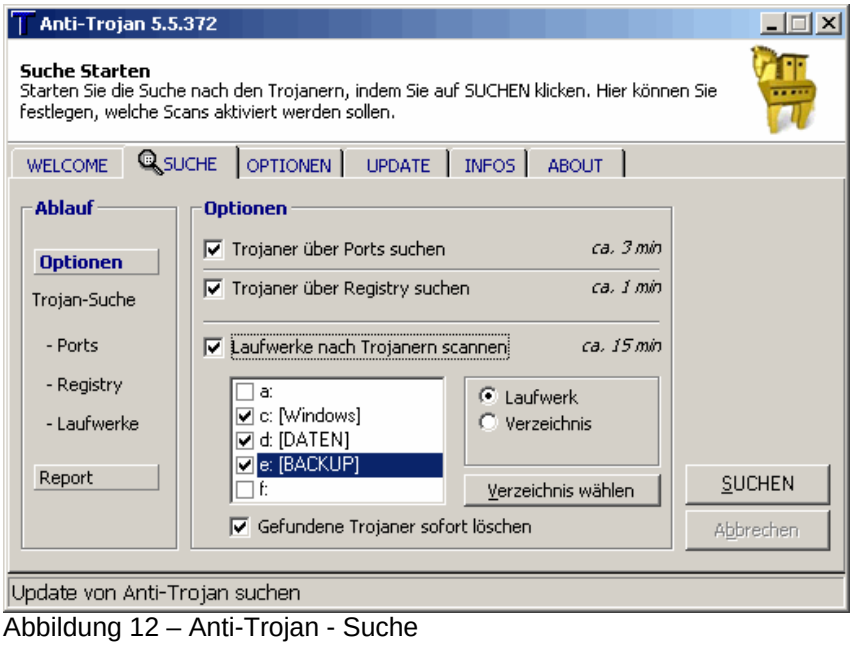

Abbildung 12 – Anti-Trojan - Suche

Nach den oben genannten Einstellungen kann die Suche gestartet werden (siehe Abbildung 13).

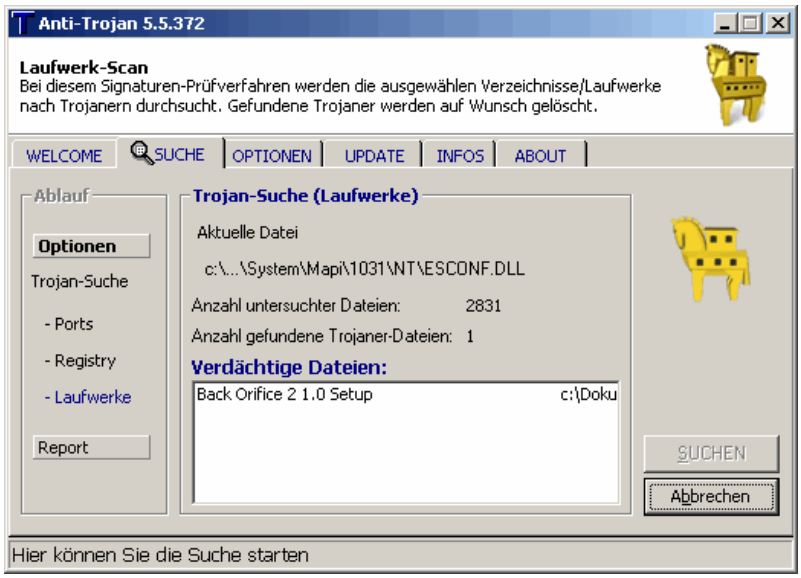

Abbildung 13 – Anti-Trojan - Suchen

Ist die Suche abgeschlossen, zeigt Anti-Trojan im Report die Anzahl der gefunden Trojaner und die weitere Vorgehensweise an (siehe Abbildung 14).

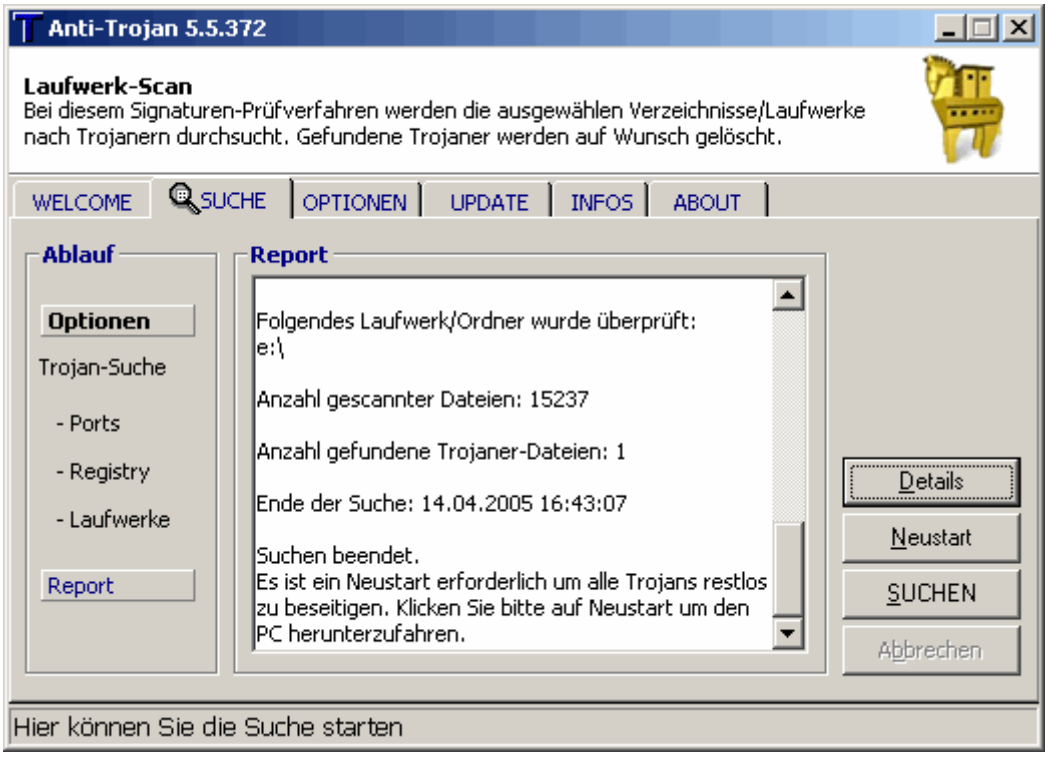

Abbildung 14 – Anti-Trojan - Report

7. Welche Ports werden gescannt, für welche Dienste werden diese Ports verwendet? Warum werden gerade diese Ports gescannt?
Es werden alle (65535) Ports des Rechners geprüft, ob ein Trojaner aktiv ist. Beim Port-Scan werden keine Trojaner entfernt, es werden lediglich alle "Löcher" im System angezeigt.

Anti-Trojan hat folgende offenen Ports entdeckt (siehe Abbildung 15 u. 16):

Abbildung 15 – Anti-Trojan – Port-Scan

Abbildung 16 – Anti-Trojan – Port-Scan

Die Ports werden für folgende Dienste verwendet:

Port 135 (Dienst: epmap)
Port 139 (Dienst: netbios-ssn)
Port 445 (Dienst: microsoft-ds)
Port 1110 (Dienst: nfsd-status & nfsd-keepalive)
Port 1125 (Dienst: hpvmmagent)
Port 5000 (Dienst: commplex-main, Trojaner Sockets de Troie, Blazer 5)

Damit der Computer Daten empfangen kann, müssen Ports geöffnet werden. Hinter jedem Port kann eine Anwendung laufen. Es gibt einige Ports die man braucht, also ist nicht jeder offene Port schlimm.
Die Trojaner benutzten meist einen bestimmten Port sagen wir mal z.B. 2500, wenn der Port 2500 nun offen ist würde uns Anti-Trojan warnen.

Bekannte System-Ports sind unter anderem:

Dienst	**Port**	**Transportprotokoll**
ping (Echo Service)	7	TCP/UDP
FTP Data Channel	20	TCP

FTP Control Channel	21	TCP
Telnet	23	TCP
SMTP	25	TCP
DNS	53	TCP
TFTP	69	UDP
GOPHER	70	TCP
HTTP (WWW)	80	TCP
POP3	110	TCP
MNTP (news)	119	TCP
SNMP	161	UDP

8. Wie findet man Dateien mit doppelter Dateiendung, und wofür ist das wichtig?

Eine weitere wichtige Vorgehensweise im Vermeiden einer Vireninfektion ist das Anzeigen der Dateiendung. Durch die Standardvoreinstellungen in Windows kann sich ein Virus mit zwei Dateianhängen, wie zum Beispiel dateiname.txt.exe oder AnnaKournikova.jpg.vbs (VBS.SST@mm, ein weit verbreiteter Virus Anfang 2001), leicht im System verbergen, da er beispielsweise im Windows-Explorer nur als dateiname.txt oder AnnaKournikova.jpg angezeigt wird. Sobald der Anwender nun die Datei anklickt, wird nicht etwa wie vermutet der Texteditor oder ein Bildbetrachtungsprogramm gestartet sondern stattdessen der Virus (also bei AnnaKournikova.jpg das VB-Skript) ausgeführt.

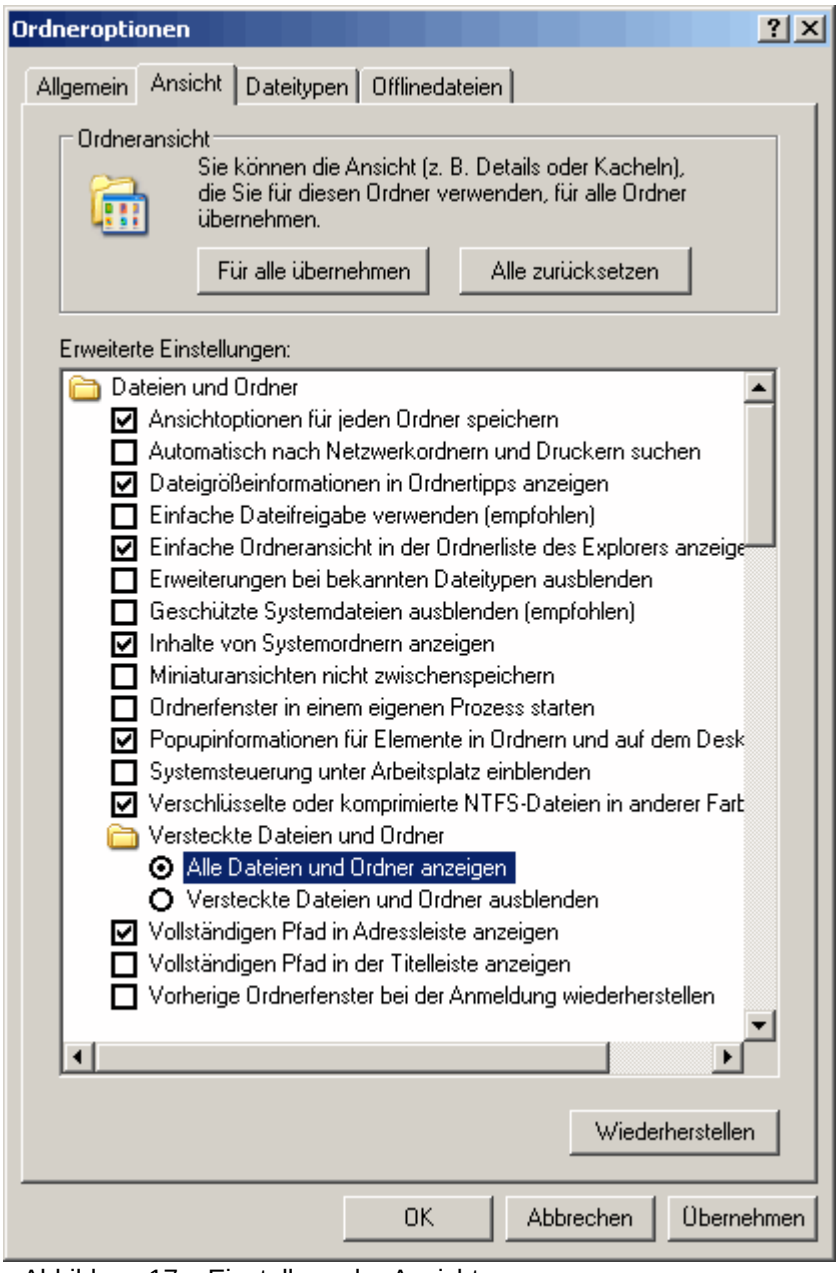

Abbildung 17 – Einstellung der Ansicht

Um dies zu vermeiden und die Dateiendungen anzeigen zu lassen, sollten folgende Einstellungen (siehe Abbildung 17) im Windows-Explorer unter „Extras“ >

„Ordneroptionen“ in der Registerkarte „Ansicht“ verändert werden:

- Häkchen entfernen bei „Erweiterungen bei bekannten Dateitypen ausblenden“
- Häkchen entfernen bei „Geschützte Systemdateien ausblenden (empfohlen)“
- Häkchen setzen bei „Inhalte von Systemordnern anzeigen“
- Option setzen bei „Alle Dateien und Ordner anzeigen“

9. Installieren und einstellen der Firewall

Um die ZoneAlarm Firewall zu installieren, wird das Installationsprogramm gestartet. Es können jeweils die vorgegebenen Einstellungen bestätigt werden. Nach der abgeschlossenen Installation und dem Starten des Programms wird man zunächst von einem Übersichtsbildschirm begrüßt (siehe Abbildung 18).

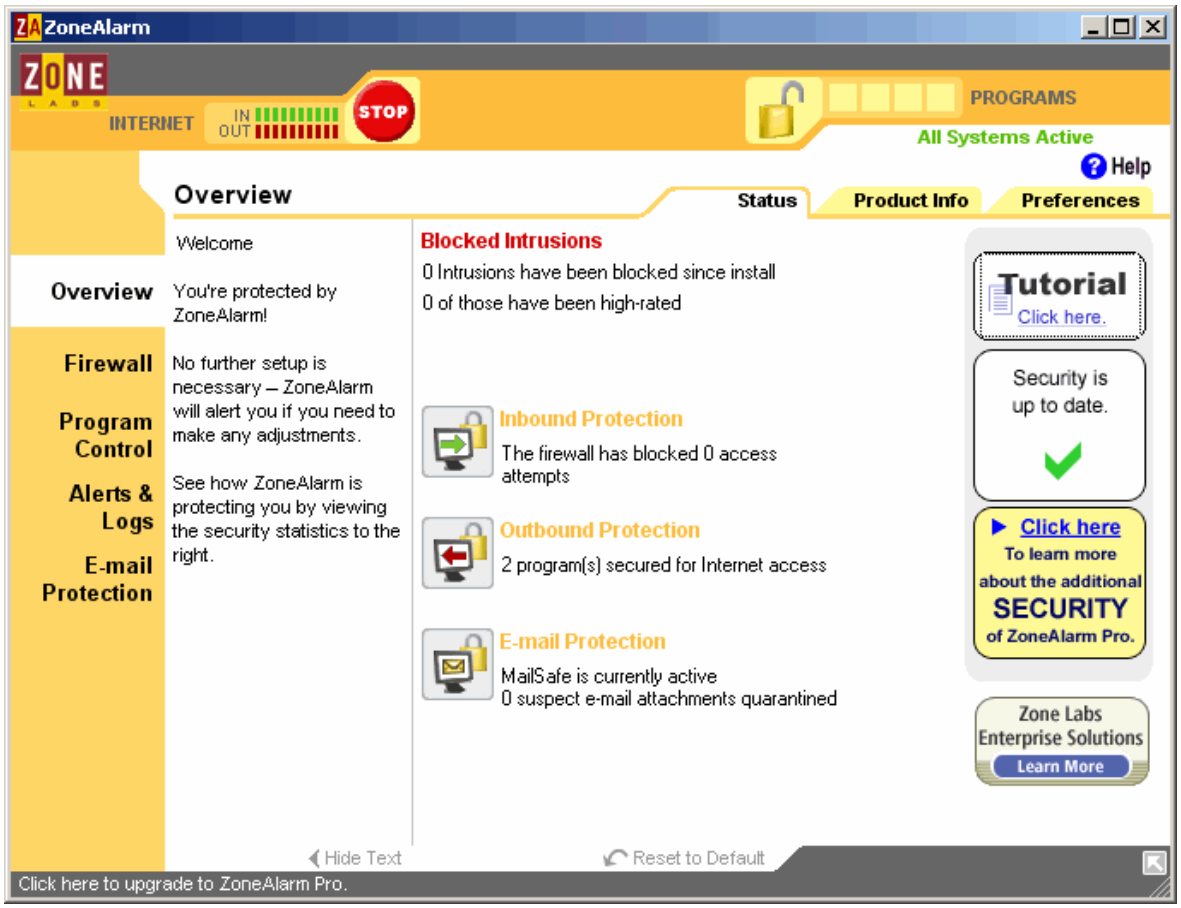

Abbildung 18 – Übersichtsbildschirm von ZoneAlarm

Durch einen Klick auf „Preferences“ kommt man zu den generellen Einstellungen des Programms (siehe Abbildung 19).
Hier sollte ein Häkchen bei „Load ZoneAlarm at startup“ gesetzt werden, damit der Computer bei jedem Neustart von Anfang an geschützt ist. Dadurch wird verhindert, dass z.B. vergessen wird, die Firewall zum Websurfen oder E-Mails abholen einzuschalten.
Noch dazu sollte man mit einem Häkchen bei „Hide my IP-address when applicable“ die eigene IP-Adresse verstecken.

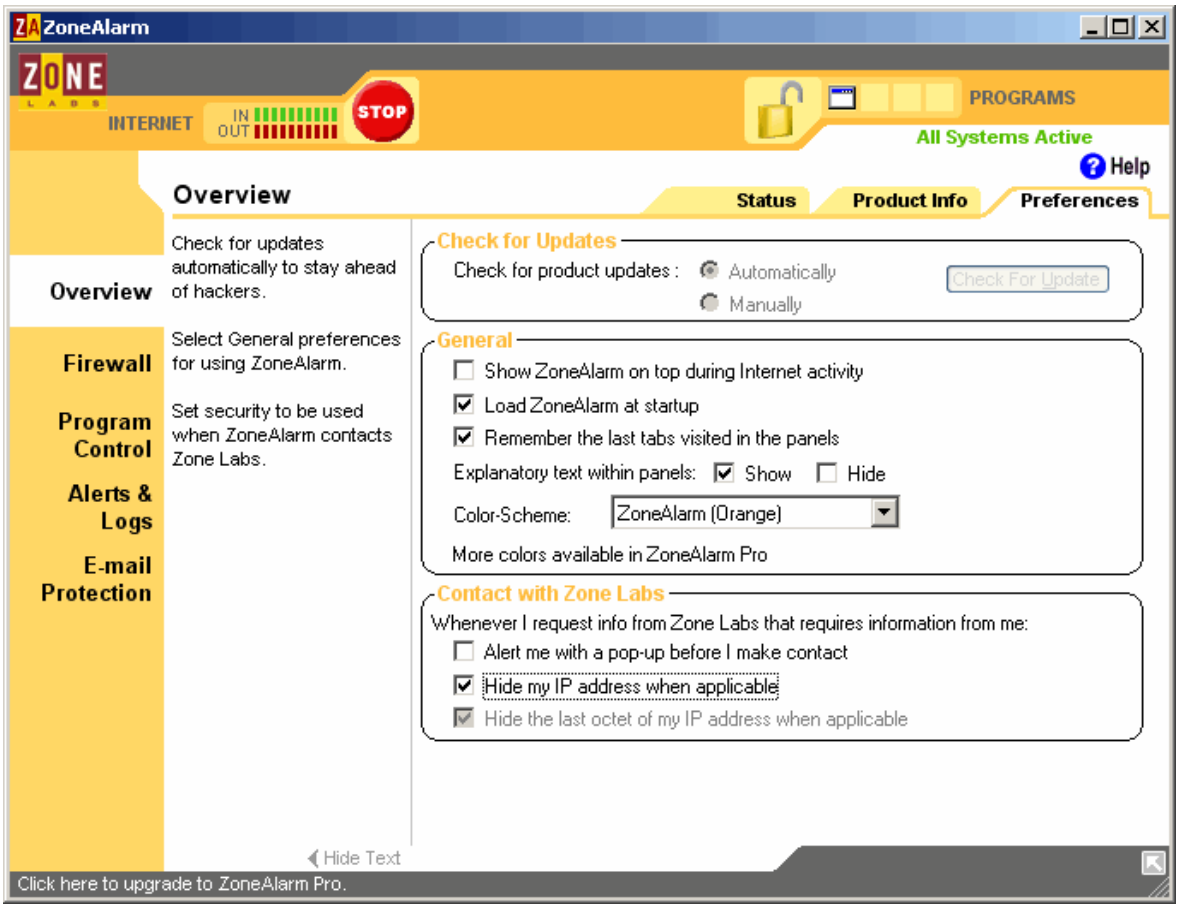

Abbildung 19 – Generelle Einstellungsmöglichkeiten

Nach Auswahl des Punktes „Firewall“ im linken Menü kommt man zu den Einstellungsmöglichkeiten der Firewall. Hier sollten beide Regler auf „High“ gestellt werden. Dies bewirkt, dass der Computer im Rahmen des möglichen am Besten gegen Angreifer von Aussen gesichert ist. Allerdings leidet dadurch ein wenig der Komfort, da eventuell einige gewünschte Effekte nicht mehr ausgeführt werden.

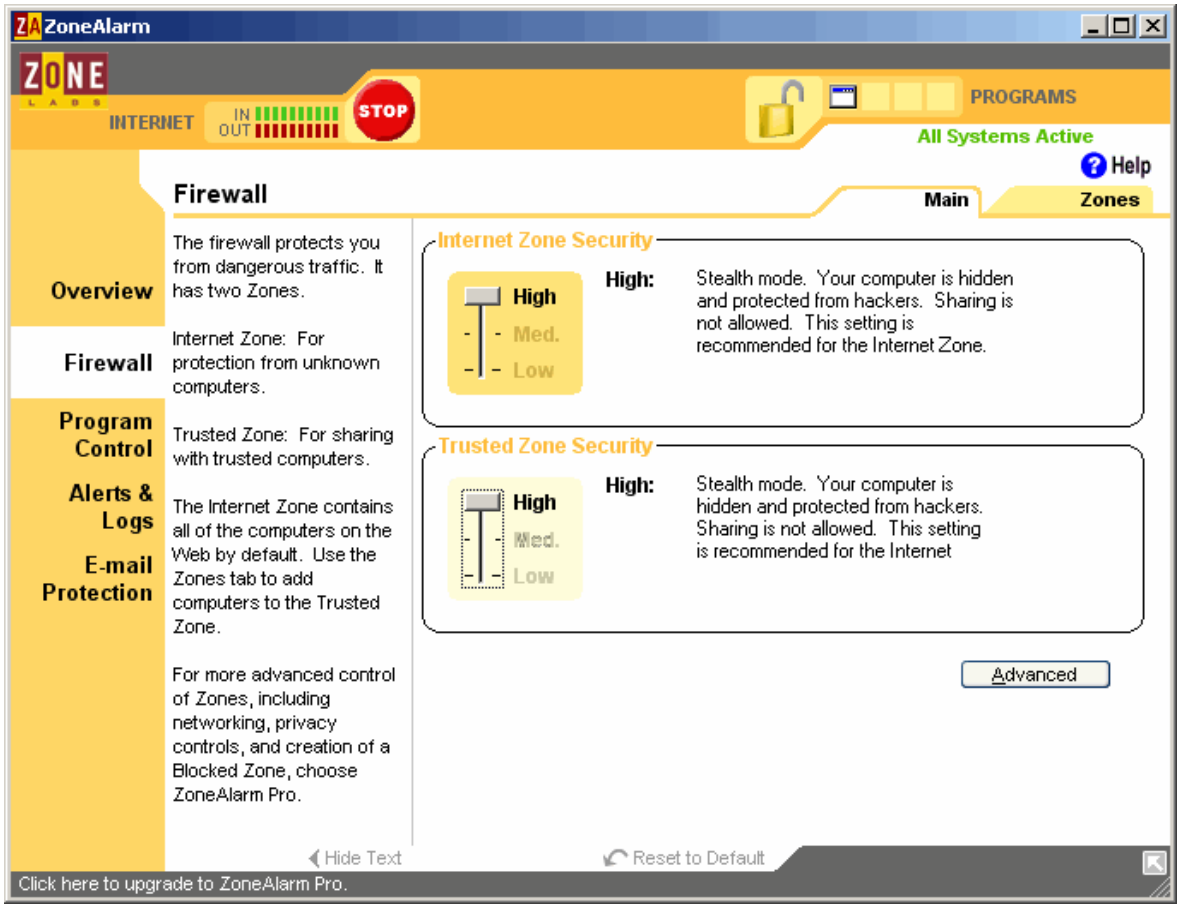

Abbildung 22 – Einstellung der Firewall

„Alerts & Logs“ sollten angeschaltet sein (siehe Abbildung 21), damit man z.B. bei jedem möglichen Angriff von ZoneAlarm eine Benachrichtigung erhält. Ebenso sollte auch die Funktion „Basic Mail Safe“ beim Menüpunkt „E-Mail Protection“ aktiviert sein (siehe Abbildung 22), damit Dateien, welche potentiell Viren enthalten könnten, wie z.B. (in der uns zur Verfügung gestellten Basic Version) VB-Scripts, generell zunächst in Quarantäne gesetzt werden.

Abbildung 21 – Meldungen

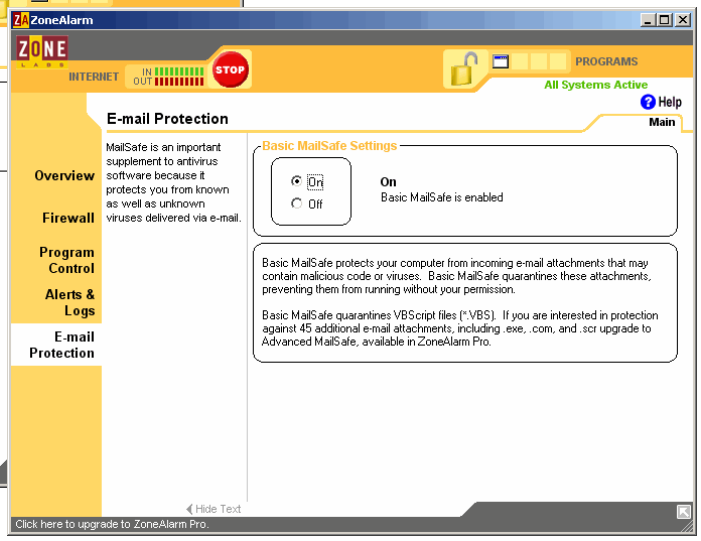

Abbildung 22 – E-Mail-Empfang absichern

10. Anpingen des Rechners anhand seiner IP-Nummer, einmal mit aktivierter Firewall des Nachbarrechners und einmal mit deaktivierter Firewall des Nachbarrechners

Nachdem alle Gruppen ZoneAlarm auf den Computern installiert haben, überprüfen wir, ob der Computer der Gruppe 3 (IP: 212.201.25.123) auch die Firewall aktiv hat (siehe Abbildung XXX). Anhand der „Zeitüberschreitung der Anforderung“ erkennen wir, dass der Ping vom anderen Computer, also mithilfe einer aktiven Firewall geblockt wurde.

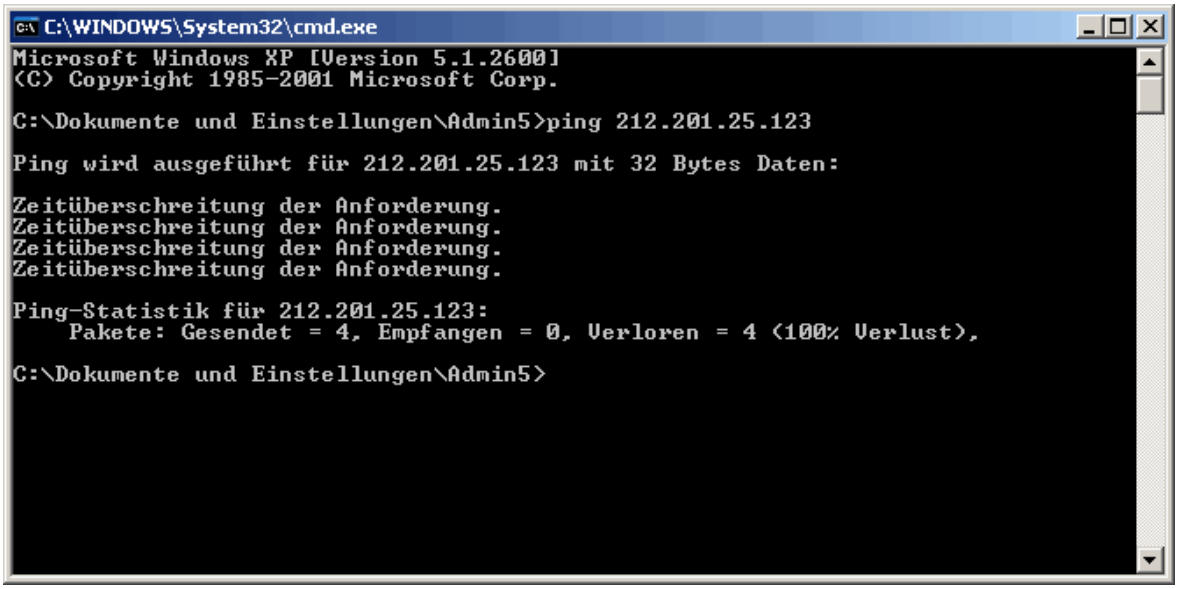

Abbildung 23 – Ping eines Rechners mit eingeschalteter Firewall

Der Computer der Gruppe 4 (IP: 212.201.25.124) dagegen hat seine Firewall nicht aktiviert. Unser Computer bekommt vom anderen Computer eine Antwort auf seinen Ping. Dadurch erkennt man zum einen, dass keine Firewall aktiv/installiert ist und zum anderen, dass es diesen Computer überhaupt im Netzwerk gibt.

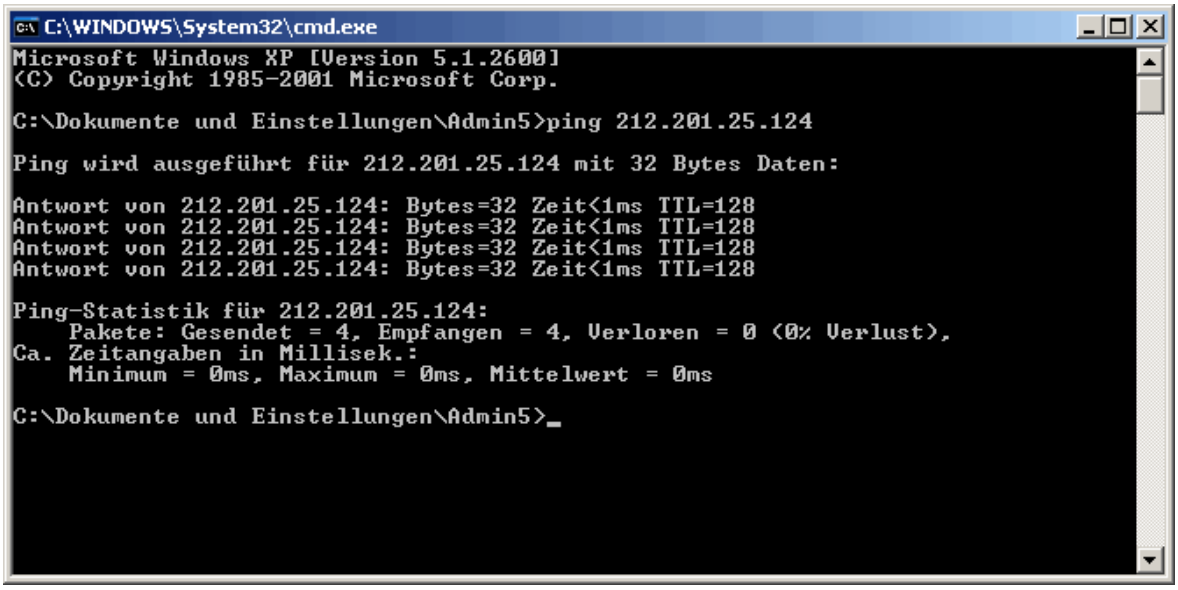

Abbildung 24 – Ping eines Rechners ohne oder mit ausgeschalteter Firewall

Gruppe 3 versucht nun ebenfalls einen Ping an unseren Computer zu senden, ZoneAlarm blockt dies aber ab und erstattet eine Meldung. Hätten wir unsere Firewall nicht aktiviert, so hätten wir von dem Ping nichts mitbekommen.

Abbildung 25 – Firewall blockiert einen Ping

11. Nun ist das kleine Virenquiz auszufüllen, welches im Ordner „Viren Know How“ auf dem Server zu finden ist

Frage 01: A	Frage 06: B	Frage 11: C	Frage 16: A
Frage 02: B	Frage 07: A	Frage 12: C	Frage 17: B
Frage 03: A	Frage 08: B	Frage 13: A	Frage 18: A
Frage 04: B	Frage 09: B	Frage 14: B	Frage 19: B
Frage 05: A	Frage 10: B	Frage 15: C	Frage 20: A

(Das Virenquiz beinhaltet einen Programmierfehler bei Frage 3, trotz richtiger Antwort kommt eine Falschmeldung)

12. Installieren weiterer Virenscanner (bitDefender, Sophos) und gleichzeitiges Scannen mit mehreren Virenscannern. Was passiert?

Das Installieren weiterer Virenscanner macht eigentlich kaum Sinn. Es kann zwar passieren, dass der eine Virenscanner einen Virus nicht findet, ein anderer jedoch schon. Allerdings wird durch mehrere aktive Scanner jedes System drastisch ausgebremst, sodass ein Arbeiten daran nach kurzer Zeit unmöglich wird. Gleichzeitiges Scannen mit Virenscannern führt dazu, dass der eine Virenscanner eine verseuchte Datei zum Scannen öffnet, der andere gleichzeitig aktive Scanner diese Datei als Virus erkennt, den Nutzer davor warnt und den Zugriff von Programmen darauf sperrt.

Persönlicher Virenreport (Person A)

Person A
Today's Date: **20.05.2005**
Which virus attacked your system(s)? **I Love You!**
1 of PC's infected by the virus?
1 of PC's owned by you (or your company)?
How did you discover the virus?

- **e.g. scanner**/memory resident scanner/ checksummer/ software monitoring device/ hardware monitoring device/ experiencing the resulting damage/ other

If you used an anti-virus package, why did you use it?

- **Used frequently & the virus unexpected**/ used because the system behaved suspicious

Did you use another scanner to get confirmation?

- **No**/Yes

Where did the virus come from?

- Original software disk/via modem / **got from a friend**/ restored it from infected backup/no idea/ other

Has the system ever had a virus in the past?

- Never/**Yes, but with a different virus**/ Yes, with the same virus

Did the virus cause damage to data?

- **No**, only some files or bootsectors infected/yes, but there was a recent backup so finally there was no damage/ Yes, loss of some data

How many financial damage was caused by the virus in total ($)? **0 $**
How did you get rid of the virus?

- Everything restored from backup/ re-installation of software/ **virus remover used**/ No successlooking for solution.

Did you remove the virus on your own?

- **Yes**/ no

If no, help from:

- inside the company/ third party for free/ expert.

Did the virus attack change your policy with regard to viruses?

- No, we still don't defend ourself against viruses at all/ No, the current measures suit our needs/ Yes, but we are still searching for an anti-virus package/ **Yes, we have found a solution against viruses.**

How do you currently defend against viruses?

- Not at all/ **scanner**/ memory resident scanner/ checksummer/ **monitoring software**/ hardware immunizer/ **other(Firewall)**.

Persönlicher Virenreport (Person B)

Name/Title/Company/Address/ZIP/District Code/City/Country/Phone Number:
Person B

Today's Date:
14.04.2005

Which virus attacked your system(s)?
SubSeven (Trojan/Backdoor)

# of PC's infected by the virus?
One

# of PC's owned by you (or your company)?
Two

How did you discover the virus?
Realtime Software Scanner

If you used an anti-virus package, why did you use it?
Used frequently & the virus unexpected

Did you use another scanner to get confirmation?
No

Where did the virus come from?
Removable Media

Has the system ever had a virus in the past?
Yes, but with a different virus

Did the virus cause damage to data?
No

How many financial damage was caused by the virus in total ($)?
0 $

How did you get rid of the virus?
Virus remover used

Did you remove the virus on your own?
Yes

Did the virus attack change your policy with regard to viruses?
No, the current measures suit our needs

How do you currently defend against viruses?
Software Scanner, Software Firewall, Hardware-Firewall

If you use a program against viruses, how often do you use it?
Realtime protection, manual Scan once a month

If you use a scanner, how often do you update it?
As soon as available (automaticly)

Did you report the virus attack to the authorities?
No