Computer Viren: Eine tägliche Bedrohung

Seit etwa Februar 2004 sind wieder enorm viele Viren in verschiedenen Varianten im Umlauf. Die Verbreitung der Viren geschieht hauptsächlich per E-Mail, wobei es derzeit nicht selten ist, dass ein Benutzer pro Tag bis zu 20 Mails mit Viren erhält.

Sehr oft sind die Absender von Viren-Mails gefälscht, d.h. der angegebene Absender ist nicht der tatsächliche Absender des Mails. Verteilt werden solche Mails - wie auch SPAM - immer mehr von ungesicherten Privat-PCs mit festem Internetanschluss (z.B. Kabel-Anschlüssen). Aktuelle Studien belegen, dass über 50% der SPAM- und Virenmails von solchen ungesicherten Privat-PCs stammen. Verschiedene Internetprovider sind jetzt daran, solche Massenverteiler zu identifizieren und deren Zugang ins Internet kurzerhand zu sperren!

Deshalb - und auch zum Wohl aller anderen Internetbenutzer - wird es immer wichtiger, dass *jeder* PC zuverlässig gegen Viren geschützt ist. Aktuelle Antivirusprogramme gehören auf jeden PC der über einen Internetanschluss verfügt. Doch das Antivirusprogramm muss auch regelmässig aktualisiert - sprich gegen neue Viren geimpft - werden.

Die nachfolgende Dokumentation beschreibt die Kontrolle der Software McAfee VirusScan Enterprise 7.1, wie Sie selbst kontrollieren können, ob die Aktualisierung erfolgreich war und wie man Viren aufspüren kann. Ausserdem bietet sie weitere Informationen zu den Themen Dialer, Adware und Spyware. Bei Bedarf wird dieses Dokument aktualisiert und die jeweils neueste Version unter **www.traberedv.ch/infos.htm** publiziert.

Oberneunforn, 6. April 2004
Traber EDV Service

Inhaltsverzeichnis

1 Einleitung

Im Gegensatz zu früher, als man die meisten Viren per Diskette bekam, kommt die grösste Anzahl der Viren heute per E-Mail.

Die meisten heutigen Viren, welche sich per Mail fortpflanzen, fälschen den Absender!

Die folgende Aussage ist deshalb in mehr als 90% von allen Fällen *falsch*:

"E-Mail von Person A ist mit einem Virus verseucht, also ist der Computer von Person A auch mit einem Virus verseucht."

Wegen der Absenderfälschung tritt häufig auch folgende Situation ein:
Sie erhalten eine Viruswarnung von einem (Ihnen meistens fremden) Mailserver der Sie darauf aufmerksam macht, dass Ihr PC mit einem Virus verseucht sei. Da aber möglicherweise der Absender des ursprünglich verseuchten Mails mit Ihrer Mailadresse gefälscht war, erhält nicht der tatsächliche Absender die Warnmeldung, sondern fälschlicherweise eben Sie. Lassen Sie sich durch solche Warnungen nicht irritieren, sondern lassen Sie Ihren PC auf Viren durchsuchen wie dies weiter hinten in dieser Doku beschrieben ist.

Die vorliegende Dokumentation ist nur für VirusScan Enterprise 7.1 von McAfee gültig. Bei älteren Versionen und anderen Produkten verlaufen die verschiedenen Prozeduren jedoch ähnlich.

Traber EDV Service übernimmt keine Haftung für Schäden, falls trotz den beschriebenen Tests und Massnahmen ein Virus auf den Computer gelangen sollte.

Bei Fragen und Problemen hilft Ihnen Traber EDV Service gerne weiter.

2 Konfiguration des Virenscanners

Ihr Virenscanner wird automatisch vom Server her konfiguriert, welcher ständig für eine optimale Konfiguration und somit für einen optimalen Schutz gegen Virenbefall sorgt. Sie brauchen sich nicht um die Einstellungen ihres Virenscanners zu kümmern. Sollten Sie Fragen haben oder sollten Sie vermuten dass ihr Virenscanner nicht optimal konfiguriert ist, wenden Sie sich bitte an ihren Administrator.

3 Aktualisieren des Virenscanners

Wie schon bei der Konfiguration übernimmt auch hier der Server die Aufgabe, ihren Computer automatisch mit den neuesten Sicherheitsupdates auszurüsten. Ihr Computer wird jeweils beim Start und/oder über Mittag automatisch vom Server mit den neuesten Anti-Virus-Updates versorgt

Dies garantiert ihnen einen möglichst hohen Schutz gegen Viren, da Sie automatisch mit den neuesten "Impfstoffen" versorgt werden. Auch hier gilt: Sollten Sie irgendwelche Fragen haben, wenden Sie sich bitte an ihren Administrator.

4 Überprüfen der aktuellen Version der Virendefinitionen

Sie können wie folgt überprüfen, ob Ihr Virenscanner aktuell ist oder nicht:

Klicken Sie mit der *rechten* Maustaste auf das VirusScan-Symol rechts in ihrer Taskleiste (links neben der Uhr)

Folgendes Menu erscheint:

Klicken Sie mit der linken Maustaste auf "Info zu VirusScan Enterprise...".

Nun sollten Sie folgendes Fenster erhalten:

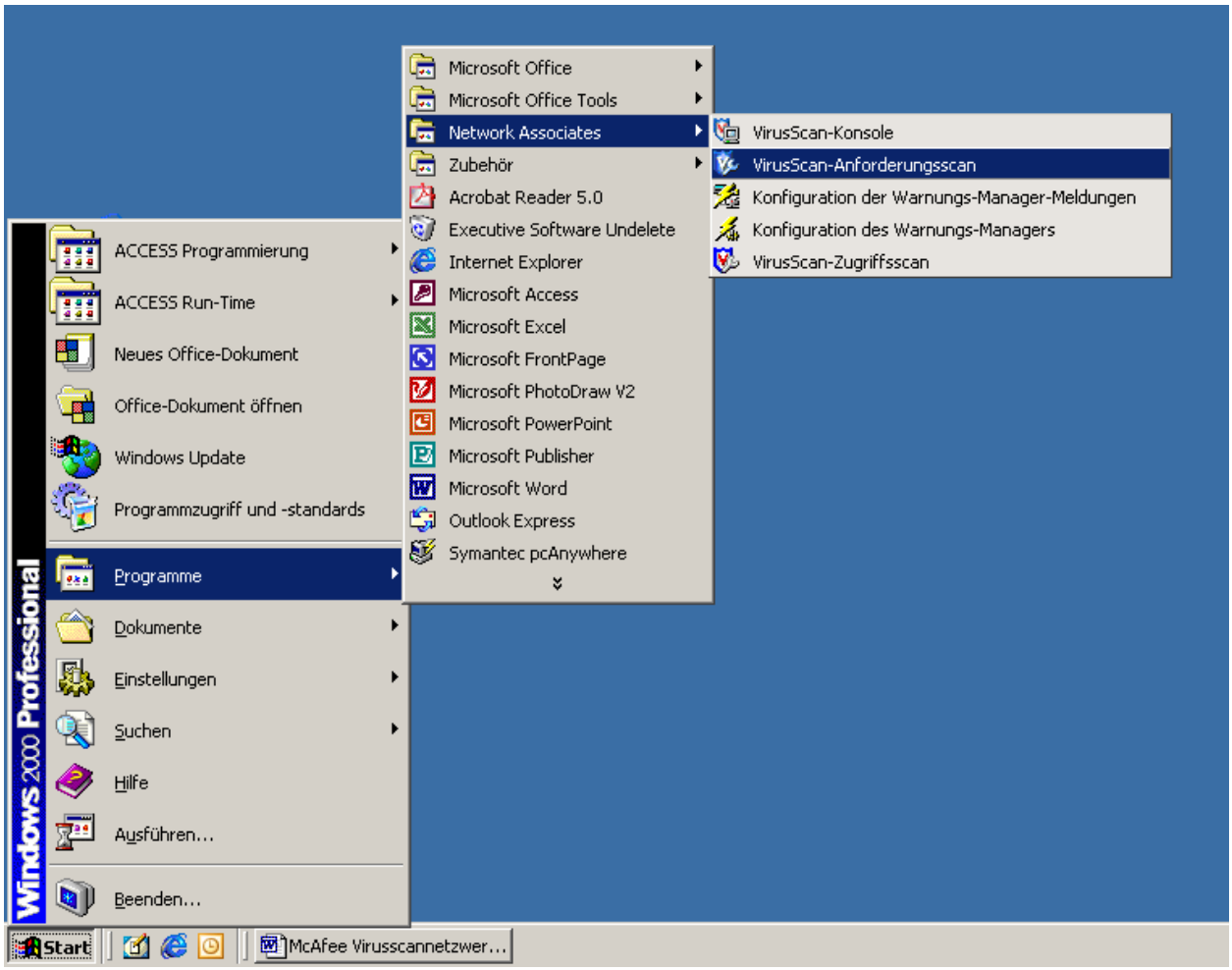
Wichtig: Das "Erstellt am" Datum sollte nicht älter sein als 2 Wochen!

Sollte das "Erstellt am:" Datum älter als 2 Wochen sein, melden Sie dies bitte schnellstmöglich ihrem Administrator.

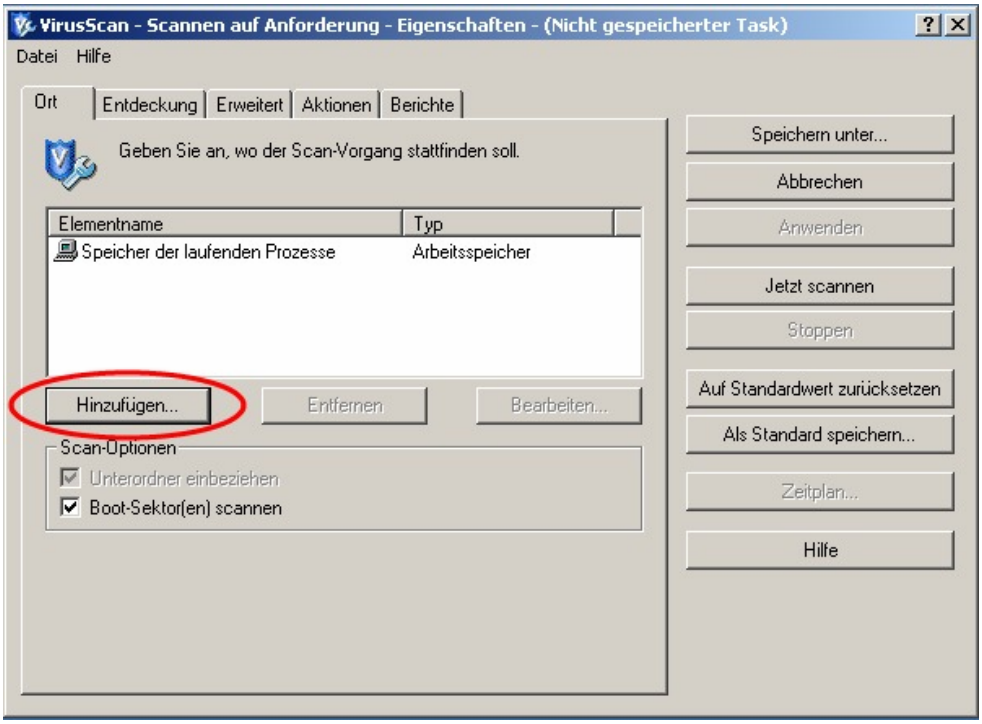
5 Den Computer nach Viren durchsuchen

Ihr Virenscanner kontrolliert ihren PC ununterbrochen nach Viren, sodass Sie sich auch hier kaum um ihren Virenschutz zu kümmern brauchen. Sollten Sie jedoch selbst nach Viren forschen wollen, gehen Sie bitte wie folgt vor:

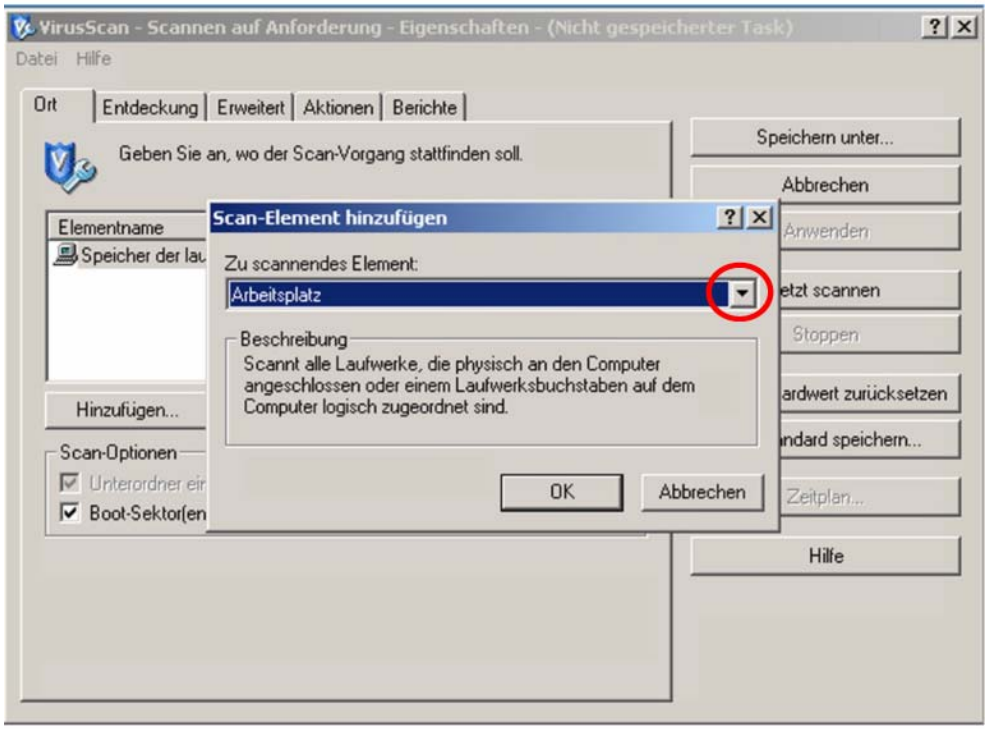
Klicken Sie mit der linken Maustaste auf "Start" (ganz links unten). Danach auf "Programme", und dann auf "Network Associates". Im Menu angekommen, klicken Sie auf "VirusScan-Anforderungsscan".



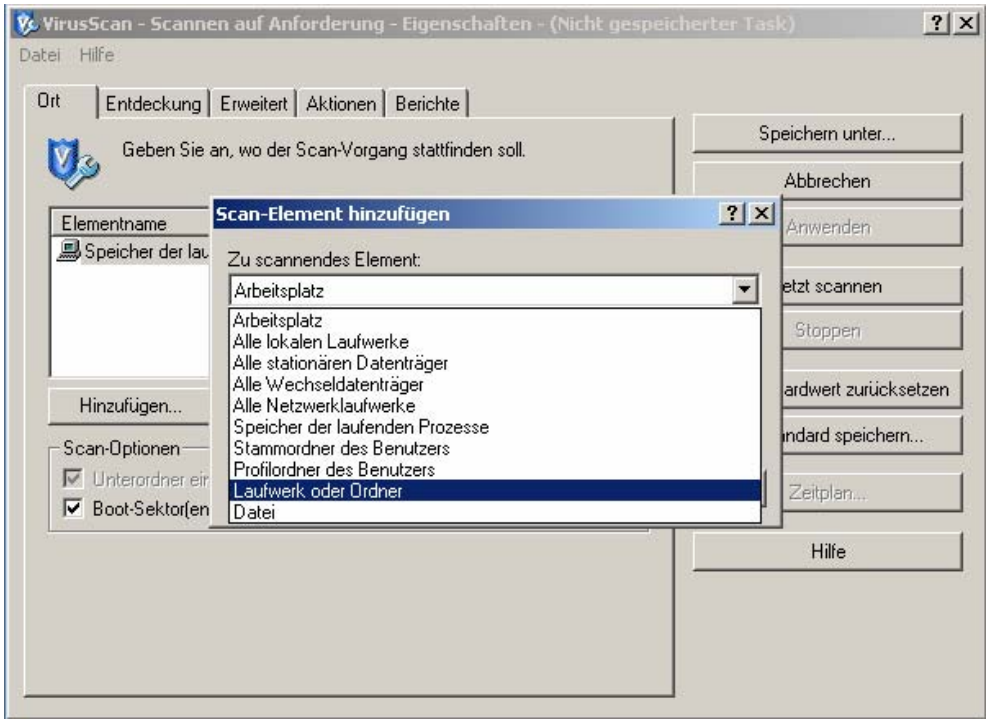
Klicken Sie im darauf folgenden Fenster auf "Hinzufügen".



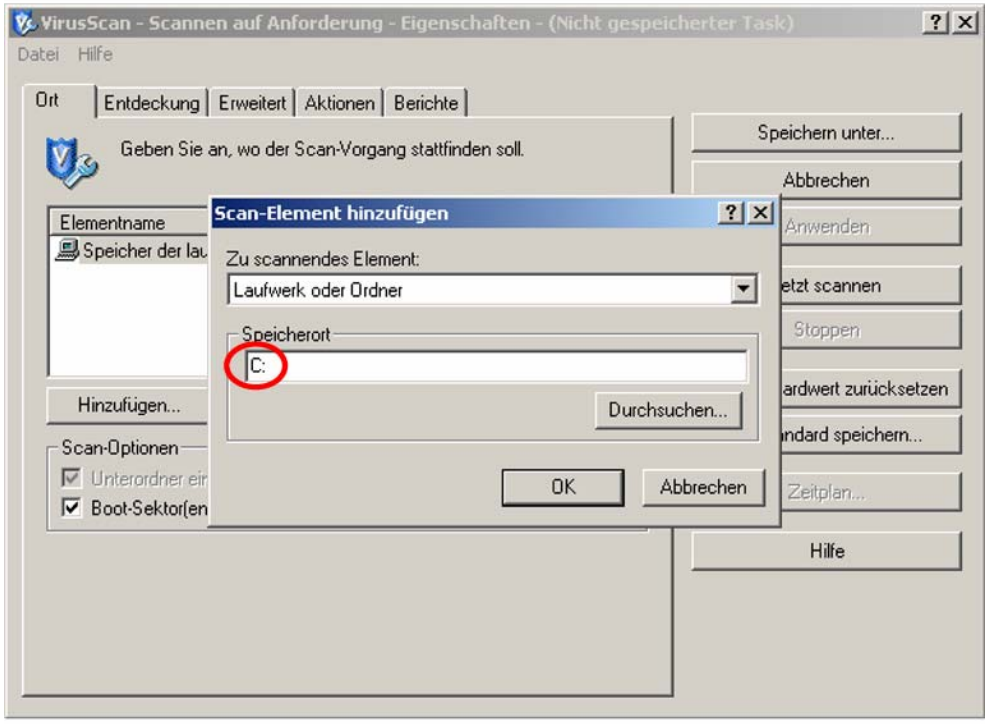
Im nächsten Fenster klicken Sie auf den kleinen Pfeil.



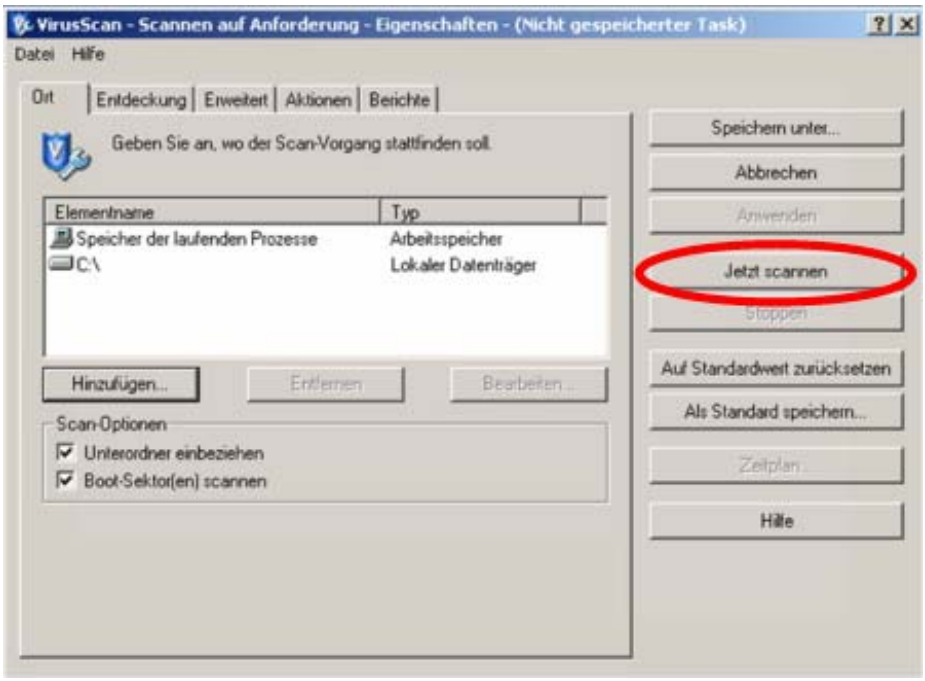
Im darauf folgenden Fenster wählen Sie "Laufwerk oder Ordner"



Danach schreiben Sie in das untere weisse Feld "C:" und bestätigen danach mit einem Klick auf "OK".



Nun sind alle Vorkehrungen getroffen, und Sie können mit einem Klick auf "Jetzt scannen" die Virensuche in ihrem PC starten.

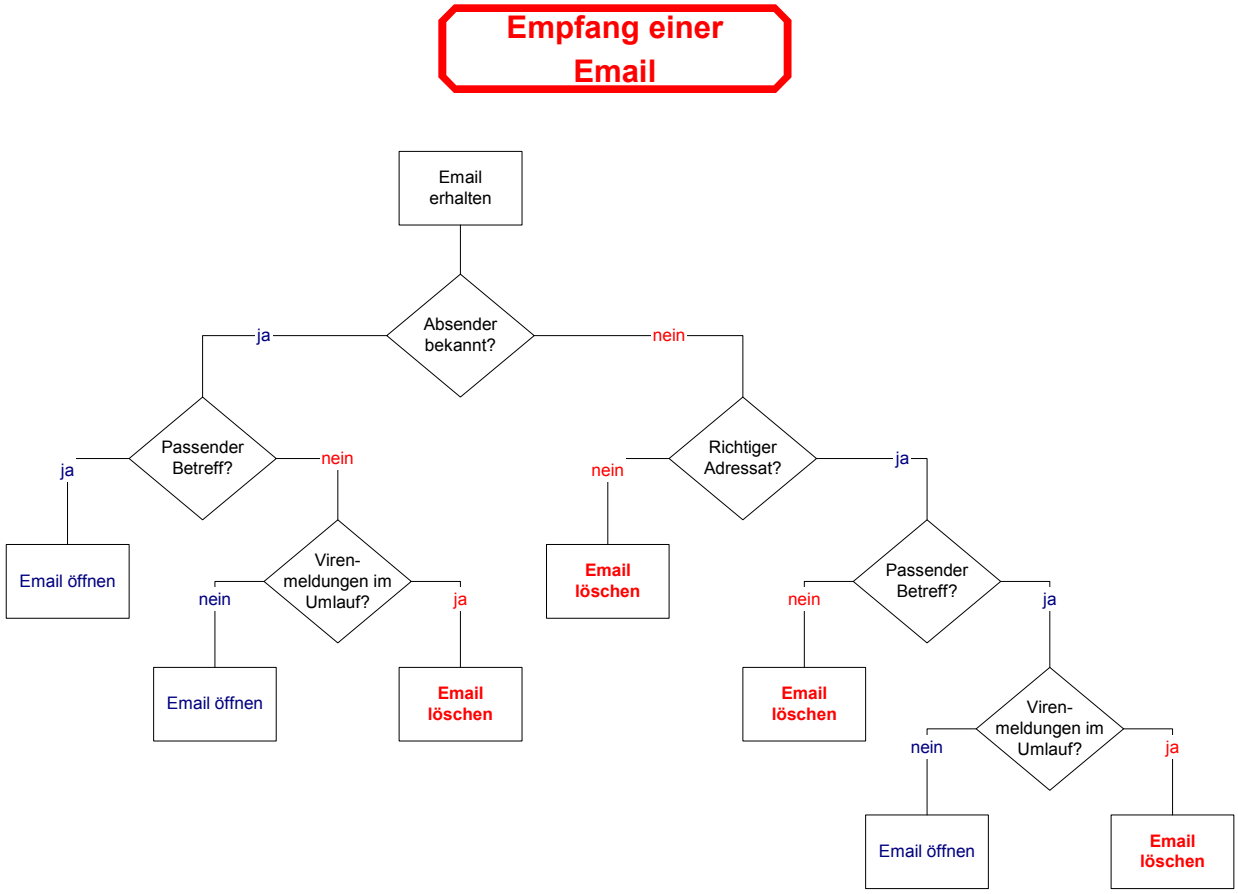


Sobald ihr Virenscanner seine Arbeit vollendet hat, erhalten Sie einen ausführlichen Bericht über den Vorgang. Sollte ihr PC einen Virus gefunden haben, werden Sie über die getroffenen Massnahmen informiert.

6 Viren gar nicht erst eine Chance geben!

Noch besser als den Computer nach Viren zu durchsuchen ist, den Viren erst gar keine Chance zu geben überhaupt aktiv zu werden.

Man sollte sich beim Erhalt einer Email an gewisse Regeln halten.
Wir empfehlen folgendes Vorgehen:



Traber EDV Service lehnt jede Haftung für Schäden ab, die durch das oben stehende Vorgehen entstehen können.

7 Hinweise und Verhaltensregeln zu SPAM

SPAM bedeutet soviel wie unerwünschtes EMail. Der Name SPAM kommt ursprünglich aus einem Sketch von Monthy Python.
Gegen SPAM gibt es einige mehr oder weniger wirksame Methoden:

- Einschalten des Spam-Filters bei seinem EMail-Provider (sofern von diesem angeboten)
- Einsatz eines eigenen lokalen Spam-Filters auf dem PC oder dem Server. Einige EMail-Programme bringen schon von Haus aus einen mit (z.B: Outlook 2003).
- Ändern der Email-Adresse
- Einhalten folgender Verhaltensregeln:
  - **Nie auf ein Spam-EMail antworten!**
  - **Nie auf einen Link klicken wo man sich aus der Mailing-Liste austragen könne.** (so oder ähnlicher Wortlaut)
  - **Die EMail-Adresse nicht wahllos auf Homepages im Internet angeben. Massenemails mit BCC verschicken.** (dabei üblich, im "An"-Feld die eigene Email-Adresse eintragen)

8 Hinweise zu Dialern

Unter einem Dialer versteht man ein Programm, welches die Einwahlnummer für das Internet ändert. Die neue Einwahlnummer beginnt dann mit 0900, 0905, 0906 oder ähnlich und kann bis zu CHF 4.- in der Minute und/oder CHF 99.- pro Anruf kosten. Eine sehr hohe Telefonrechnung ist garantiert!

Weiter können Dialer die Systemstabilität und Geschwindigkeit Ihres PC negativ beeinflussen.

Einen Dialer fängt man sich bei Surfen auf "dubiosen" Seiten im Internet ein. Hat er sich erst einmal auf dem System eingenistet, braucht es fundierte Kenntnisse um diesen von dort wieder zu entfernen.

Es ist ratsam, generell die 0900-Nummern sperren zu lassen. Der beste Schutz vor den Dialern bietet jedoch der Wechsel z.B. auf ADSL (bei gleichzeitigem Ausziehen der Wählleitung).

Wichtig: Ein Dialer ist kein Virus, Ihr Virenscanner schützt Sie leider nur begrenzt davor.

9 Kreditkarten

Benutzen Sie Ihre Kreditkarte im Internet höchstens bei Anbietern, die Ihnen bekannt sind. Mit Vorteil kaufen Sie nur bei seriösen, bekannten inländischen Unternehmen per Kreditkarte im Internet ein (z.B. Bertelsmann, ExLibris usw.).

Antworten Sie **NIE** auf Mails in denen Sie aufgefordert werden, Ihre Kreditkarteninformationen per Mail zu bestätigen oder zu erneuern. Seriöse Unternehmen fragen Sie telefonisch für die notwendigen Informationen an oder bieten allenfalls in einem Mail einen Link an welcher zu einer gesicherten Seite (SSL) führt (z.B. EBay). Gerade EBay ist ein schönes Beispiel: vor ca. 8 Wochen gingen viele böswillige Mails herum, in denen der Absender als 'EBay' gefälscht wurde und die Kunden zum Versand der Kreditkarteninfos *per Mail* aufgefordert wurden...

10 File Sharing: EMule, Morpheus & Co

Gleich vorneweg genommen: Entgegen aller Gerüchte ist das Herunterladen von Musik und Videos/DVD mit Hilfe von File-Sharing Tools **illegal**. Mehrere EU-Länder haben in den letzten Monaten ihre Gesetze verschärft; die Schweiz will ca. 2006 nachziehen. Angeblich soll nur das Verbreiten von solchen Inhalten verboten sein, das reine Herunterladen jedoch nicht. Die Stolperfalle an der Sache ist nur: jedes File-Sharing Tool wie EMule, Morpheus und andere bieten die schon heruntergeladenen Dateien den anderen Benutzern an, denn nur auf dieser Basis funktioniert das File-Sharing. Damit ist der Tatbestand des Anbietens jedoch gegeben und man macht sich strafbar.

Hinzu kommt, dass einige dieser Tools den Hackern Tür und Tor öffnen um ihre schädlichen Inhalte an den Antivirus-Programmen vorbeizuschmuggeln. Einige dieser Programme sind schon so weit entwickelt, dass sie sogar über Firewalls hinweg funktionieren und damit sogar ein Firmennetzwerk theoretisch "im Internet publizieren können". Auf einem Netzwerk-PC hat ein File-Sharing Tool also definitiv nichts verloren; fehlbare Mitarbeiter können sogar bei Bedarf für Schadenersatz verantwortlich gemacht werden!

Hände weg von File-Sharing Tools !

11 AdWare und Spyware

Adware werden Programme genannt, die "nach Lust und Laune" auf Ihrem PC Werbefenster einblenden, sobald er mit dem Internet verbunden ist. Teilweise werden auch Suchergebnisse von Suchmaschinen wie Google und Yahoo verfälscht, um den Benutzer auf Werbeinhalte zu locken. Ein typisches Beispiel für Adware ist der "Hotbar", der die Knöpfe des Internet-Explorers ergänzt und verschönert.

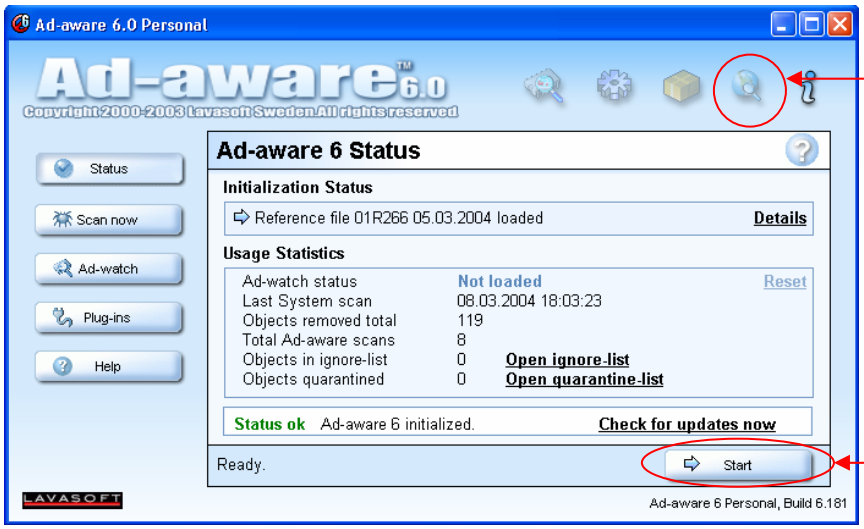
Spyware sind Programme, die Daten über den PC und den Benutzer sammeln und ins Internet senden (Mail-Adressen, Kreditkarteninfos usw.). Aufgrund dieser Infos nimmt dann auch "plötzlich" und "unerklärlich" die Anzahl der SPAM-Mails zu (vergleiche Kap. 8). Typische Beispiele für Spyware sind Gator Date Manager und Breitling World Time (GMT).

Auch die neuesten Antivirus-Programme sind (wie bei den Dialern) nicht in der Lage, solche Software vollständig zu erkennen. Aufgabe der Antivirus-Software ist, schädigende Programme zu blockieren (wobei man sich fragen muss, inwieweit Spyware nicht auch schädigend ist...).

Gegen Adware und Spyware gibt es ein kostenloses Tool (in englisch), mit dem man seinen Rechner auf Adware und Spyware untersuchen kann. Das Tool kann unter folgender Adresse heruntergeladen werden:

http://traberedv.dyndns.org/Download/Utilities/ und dann Ad Awarexxxx.exe anklicken

Beachten Sie, dass auch dieses Tool immer wieder mit den neuesten Informationen aktualisiert werden muss! Die kostenpflichtige Version ist in der Lage, Adware und Spyware zu erkennen, *bevor* sie überhaupt auf dem Rechner installiert wird.



Internet-Update starten

PC überprüfen

12 Firewalls

Unter einer Firewall versteht man eine Einrichtung, die den PC oder das Netzwerk gegen Angriffe von aussen schützt. Die Firewall kann ein Gerät sein (z.B. ein ADSL-Modem mit Firewall) oder auch eine Software (z.B. Norton Internet Security Suite oder ZoneAlarm).

Der Blaster-Wurm hat im Herbst 2003 neue Maßstäbe gesetzt, indem er sich innert 30-90 Sekunden nach Verbindungsaufnahme ins Internet auf NT-basierenden Systemen (Windows NT, Windows 2000 und Windows XP) einnisten kann, obwohl auf den Systemen eine aktuelle Antivirus-Software installiert ist.

Auf jeden alleinstehenden PC (mit Windows NT oder 2000) gehört deshalb eine Firewall, sofern diese nicht schon im Verbindungsgerät (z.B. ADSL-Modem) eingebaut ist. Rechner mit Windows 95/98 benötigen derzeit keine Firewall weil es noch (?) keine Viren gibt, die diese Systeme angreifen. Windows XP hat eine Firewall integriert, allerdings muss diese auch aktiviert sein (was bei PC's aus den Billig-Läden bzw. ab der Stange oft nicht der Fall ist).

Eine kostenlose Software-Firewall können Sie herunterladen unter:

www.zonelabs.de/download/znalm.html

Eine Software-Firewall sollte jedoch **nur** dann installiert werden, wenn keine Hardware-Firewall vorhanden ist. Das Prinzip "doppelt genäht hält besser" trifft bei Firewalls *nicht* zu. Im Zweifelsfall fragen Sie lieber zuerst einen Fachmann, bevor Sie beliebig Software installieren.

Netzwerkbenutzer aufgepasst: Wenn Sie an Ihrem Arbeitsplatz einen Computer verwenden der am internen Netzwerk angeschlossen ist, dürfen Sie auf **keinen** Fall Software-Firewalls auf Ihren PC installieren. Diese können den Betrieb des internen Netzwerks stören! Das Firmennetzwerk ist bestimmt schon mit einer Firewall am richtigen Ort ausgerüstet, sonst hätte Ihr PC ja schon längst den Blaster-Wurm "eingefangen" und würde sich alle 60 Sekunden selbst herunterfahren... Kontaktieren Sie bei Bedarf Ihren Systemadministrator.