

Spyware, Adware und sonstige Gemeinheiten: Eine tägliche Bedrohung

Die nachfolgende Dokumentation beschreibt die Problematik mit unerwünschten Programmen. Weitere Informationen zum Thema Antivirus sowie die neuste Version dieses Dokuments finden Sie unter <http://www.traberedv.ch>.

Oberneunforn, 26. Februar 2005
Traber EDV Service

Inhaltsverzeichnis

1	Zusammenfassung für Lesefaule	1
2	Einleitung.....	2
3	Was ist Spyware?.....	2
4	Dialer	3
5	File Sharing: Kazaa, EMule, Morpheus & Co.....	4
6	Spyware und Adware	5
7	Wie fängt man sich Spyware oder Adware ein?.....	6
8	Benutzung von Ad-Aware SE.....	7
9	Firewalls	9
10	Kreditkarten	10

1 Zusammenfassung für Lesefaule

- Mails von unbekanntem Absendern mit merkwürdigen Betreffs löschen statt öffnen
- Keine Gratis-Software vom Internet herunterladen
- Keine File-Sharing-Tools wie Kazaa, EMule, Morpheus verwenden
- Auf Mails die zur Eingabe von Kreditkartennummern auffordern nie reagieren
- Kaufen Sie Ihren PC bei einem ausgewiesenen Fachhändler statt beim Discounter
- Den PC alle 2-4 Wochen auf Spyware und Adware prüfen
- Die Funktion des Antivirus-Programms regelmässig überprüfen

2 Einleitung

Schnell mal eine Software vom Internet heruntergeladen, hier ein Versprechen für Gratis-Spiele, MMS-Bilder, aus Versehen auf eine dubiose Homepage geraten und schon ist es passiert. Der Computer ist mit Adware, Spyware usw. verseucht. Der Computer wird immer langsamer, es tauchen ungewollte Fenster auf mit Werbeversprechungen, was man so alles "vergrössern" könnte. Dies sind nur einige Beispiele der vielen Möglichkeiten wie man so genannte unerwünschte Software antrifft. Wir möchten Ihnen mit diesem Dokument eine kleine Hilfe im Kampf gegen diese Programme geben. Aber wie in so vielen Bereichen des Lebens; Vorbeugen ist besser als später Therapieren. "Komische" Emails löschen, vernünftig surfen und den Inhalt jeder Homepage kritisch betrachten sowie die eigene Schutz-Software auf dem neusten Stand halten ist alles letztlich das A+O der eigenen Informatik-Sicherheit.

Traber EDV Service übernimmt keine Haftung für Schäden, falls trotz den beschriebenen Tests und Massnahmen Viren, Spyware, Adware usw. auf den Computer gelangen sollte.

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

3 Was ist Spyware?

Spyware sind Programme die sich auf dem Rechner einnisten und die Dateien nach Informationen wie Namen, Mailadressen, Kreditkartennummern etc. durchsuchen. Diese Daten werden dann auf verschiedene Server im Internet gesendet und dort weiterverarbeitet. Spyware wird auch von den neuesten Antivirus-Programmen NICHT oder nur ungenügend erkannt. Die harmloseste Auswirkung von Spyware ist, dass man dann plötzlich SPAM (Mail-Werbung) bekommst die man gar nicht will. Die schlimmste Auswirkung wäre, dass auf der Kreditkarte einige Monate nach dem Spyware-Befall ein paar Tausender belastet werden die man dann berappen muss. Das Ganze wird neuerdings auch "Phishing" genannt, die Medien haben schon verschiedentlich darüber berichtet. Es existiert bereits eine "Mafia", welche die mit Hilfe von Spyware gesammelten Kreditkarteninformationen gegen hartes Geld im Internet verkauft. Diejenigen, die solche Informationen kaufen und dann verwenden sind auch diejenigen, die dann rechtlich geradestehen müssen. Für die "Mafia" ein lukratives Geschäft, denn sie haben die Informationen legal verkauft; nur die Käufer handeln illegal...

Weitere Informationen zu diesem wichtigen Thema finden Sie im Kapitel 6 !

4 Dialer

Unter einem Dialer versteht man ein Programm, welches die Einwahlnummer für das Internet ändert oder zusätzlich zur "normalen" Einwahl nebenbei eigene Anrufe tätigt. 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.

Ein Dialer kann sich während dem Surfen auf "dubiosen" Seiten im Internet auf dem PC einnisten.

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). Swisscom hat zwar im Mai 2004 die offensichtlich unseriösen Anbieter ausgesperrt; trotzdem lässt sich nicht vorhersagen, welche trickreichen Ideen noch auf den "Markt" kommen.

Wichtig: Ein Dialer ist kein Virus weil er in bestimmten Fällen ja erwünscht sein kann, Ihr Virens scanner schützt Sie deshalb leider nur begrenzt davor.

5 File Sharing: Kazaa, 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 2004 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 Kazaa, EMule, Morpheus und andere bieten die schon heruntergeladenen Dateien sofort den anderen Benutzern wieder an, denn nur auf dieser Basis funktioniert das File-Sharing. Damit ist der Tatbestand des Anbietens gegeben und man macht sich strafbar.

Der Kassensturz hat Ende 2004 in einer Sendung behauptet, das Herunterladen mit einem File-Sharing Tool sei legal und dabei einen Juristen zitiert der die Sache angeblich untersucht hat. Es liegt auf der Hand dass ein Jurist nicht wissen kann auf welcher technischen Basis der Dateiaustausch funktioniert und somit kann er auch nicht wissen, dass während dem Herunterladen mit einem File-Sharing Tool der Tatbestand des Anbietens schon nach wenigen Minuten erfüllt ist - was in der Schweiz ebenfalls strafbar ist! Im Zusammenhang mit Kinofilmen und Kinderpornographie wurden in der Schweiz seit Mitte 2004 bereits Hausdurchsuchungen und Beschlagnahmungen (mehrere hundert!) vorgenommen; ein Gerichtsverfahren gegen einen minderjährigen Verbreiter von Kinofilmen ist derzeit (Anfang 2005) im Gang. Weitere Verfahren werden zweifellos folgen...!

Beim surfen im Internet - also auch beim Herunterladen von Inhalten ist man keineswegs anonym! Mit Hilfe des zuständigen Providers lässt sich der Empfänger jeder Information bzw. jeder Bewegung von irgendwelchen Daten relativ einfach feststellen. Wer also stundenlang File-Sharing Tools benutzt kann problemlos bei Bedarf mit seinem Namen und Wohnadresse identifiziert werden.

Zu beachten ist auch, dass die meisten der Tauschbörsenprogramme Spyware sind! Kazaa zum Beispiel legt Wert auf ihrer Homepage, dass Kazaa keine Spyware sei. Das stimmt eigentlich auch, aber: Kazaa funktioniert nur, wenn das zugehörige Drittprogramm P2P (automatisch und ohne Hinweis) mitinstalliert wird. Geht man dem Hersteller von P2P nach stellt man fest, dass P2P vom Hersteller offiziell als Spyware deklariert wird. P2P greift übrigens derart in die Windows-Komponenten ein, dass nach Deinstallation oder schon nur nach einer Änderung der Internetverbindung keine Kommunikation mehr möglich ist. Da ist dann bereits ein Fachmann gefragt, um die Sache wieder in Ordnung zu bringen.

Hinzu kommt, dass einige dieser Tools den Hackern Tür und Tor öffnen um ihre schädlichen Inhalte an den Antivirus-Programmen vorbeizuschmuggeln. Die meisten dieser Programme sind heute 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 bei Bedarf für Schadenersatz verantwortlich gemacht werden!

Hände weg von File-Sharing Tools !

6 Spyware und Adware

Adware (ad = amerikanische Abkürzung für Advertising = Werbung) 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, Yahoo und anderen verfälscht, um den Benutzer mit den falschen Links auf Werbeinhalte oder sogar Seiten mit aktiver Ad- oder Spyware zu locken. Ein typisches Beispiel für Adware ist der "Hotbar", der vordergründig die Knöpfe des Internet-Explorers ergänzt und verschönert, letztendlich aber nur für dauernde Ad's (Werbung) sorgt.

Spyware (spy = spähen, ausspähen) 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 auch Kap. 3). Typische Beispiele für Spyware sind Gator Date Manager und Gator 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 mehrere kostenlose Tools, mit denen man seinen Rechner auf Adware und Spyware untersuchen kann. Aber **Achtung**: Nicht jedes kostenlose Tool wirkt tatsächlich gegen die Probleme; viele der im Internet angebotenen (kostenlosen) **Tools sind selbst Spyware!**

Traber EDV Service hat 2 kostenlose Tools auf ihre Seriosität untersucht und zur momentan bedenkenlosen Benutzung freigegeben. Es handelt sich um "Ad-Aware SE" (kommt aus Schweden und ist deshalb in englisch) und "Spybot Search&Destroy" (stammt aus Deutschland und ist in deutsch, stellt aber höhere Ansprüche bzw. Wissen bezüglich Bedienung). Wegen der einfacheren Bedienung empfehlen wir Ad-Aware (wird nachstehend noch genauer beschrieben).

Beide Tools können unter folgender Adresse heruntergeladen werden:

<http://traberedv.dyndns.org/Download/Utilities/>

und dann "Ad Aware SE 105.exe" anklicken (für Ad-Aware)

oder "Spybotsd13.exe" anklicken (für Spybot)

Beachten Sie, dass beide Tools immer wieder mit den neuesten Informationen aktualisiert werden müssen! **Wichtig**: Wer schon "Ad-Aware 6.0" einsetzt muss unbedingt auf SE aktualisieren. Für die Version 6.0 gibt es keine Updates mehr – und damit wird diese Version nutzlos! Auch bei Spybot ist bereits eine neuere Version in Arbeit aber noch nicht verfügbar.

Natürlich gibt es noch weitere "fast saubere" Tools. Einige davon schiessen aber weit über Ihr Ziel hinaus. Programme wie "Hijackthis" oder "Antispy XP" sind so eingestellt, dass sie ohne besondere Massnahme durch den Benutzer Dinge aus dem PC löschen die den Betrieb des PC's sogar in Frage stellen. Hijackthis kann zum Beispiel Netzwerkeinstellungen löschen so dass nach dem nächsten Start des PC keine Kommunikation mehr möglich ist, Antispy XP bringt es sogar fertig, Lizenzierungsinformationen zu löschen so dass ein PC mit Windows XP 30 Tage später nicht mehr gestartet werden kann! Wundersamerweise werden solche Tools noch von Computerzeitschriften gelobt; sie sind aber definitiv nur für den Fachmann geeignet und für einen Durchschnittsbenutzer gar nicht empfehlenswert.

7 Wie fängt man sich Spyware oder Adware ein?

Es gibt hauptsächlich 3 Verbreitungsarten:

1) aktives Herunterladen von Gratis-Programmen durch den Benutzer

Die zunehmende "Geiz ist Geil" Einstellung wird von Ad- und Spyware Herstellern schamlos ausgenutzt – nach unserem Dafürhalten nicht ohne Legimität. Es wird ja etwas geboten und die Gegenleistung für das kostenlose Konsumieren von Leistungen ist die Preisgabe von persönlichen Informationen (vergleiche auch Kap. 3). Wer keine Ad- oder Spyware auf seinem PC haben möchte ist angehalten, auch nicht wahllos Gratisleistungen aus dem Internet zu konsumieren bzw. herunterzuladen.

2) unbemerktes Installieren von Programmen während dem surfen auf dubiosen Seiten

Auch das hat letztlich mit dem Konsumieren von Gratisleistungen zu tun. Wer Windows XP hat und den Service Pack 2 installiert – und sein System bzw. vor Allem den Internet-Explorer auch richtig konfiguriert wird jeweils gewarnt bevor ein unerwünschtes Programm installiert wird.

3) per EMail (Mails mit Dateianhängen welche die Spyware enthalten)

Schalten Sie in Ihrem Mail-Programm allfällige Vorschaufenster aus. Schädigende Mails können erst aktiv werden, wenn sie geöffnet werden. Vorschaufenster bewirken ein Öffnen eines Mails, deshalb sollten sie mindestens in folgenden Ordnern abgeschaltet werden: Posteingang, Spam, Junk-E-Mail, Quarantäne, Infected, Isoliert und ähnliche (Namensgebungen und Existenz der Ordner sind abhängig von den verwendeten Mailprogrammen und deren Versionen. Der "Lesebereich" welcher mit Outlook 2003 eingeführt wurde sollte bei diesen Ordnern ebenfalls abgeschaltet bleiben.

An dieser Stelle gehört auch noch etwas Werbung für die Fachhändler im Informatikbereich - insbesondere für Traber EDV Service - hin.

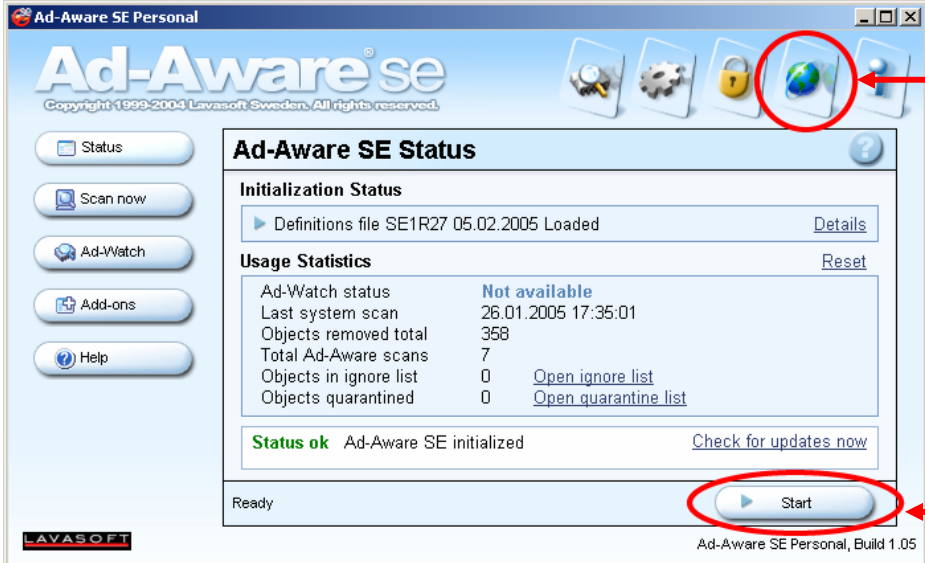
Sie dürfen von PC's und Kommunikationseinrichtungen wie z.B. Wireless-LAN welche im Warenhaus oder beim Discounter gekauft wurden nicht erwarten, dass alle aktuellen Sicherheitsupdates auch tatsächlich installiert sind und das Gesamtsystem richtig konfiguriert ist. Vom Fachhändler dürfen Sie das erwarten. Allerdings kostet der PC dann beim Fachhändler etwas mehr (10-15%) als im Warenhaus, denn schon nur die korrekte Konfiguration eines vorinstallierten Markenprodukts kann 1-2 Arbeits-Stunden in Anspruch nehmen.

Unter den "Fachhändlern" selbst gibt es leider aber auch viele schwarze Schafe. Dabei handelt es sich oft um Einzelpersonen, die nebenbei eine "Informatikfirma" betreiben als Zusatzverdienst. Nicht selten handelt es sich dabei um Studenten, Gastwirte, Chauffeure, Verkäufer, Lageristen oder sonstige Berufsleute die ihre Dienste meistens zu sehr günstigen Konditionen anbieten. In keinem Fall darf man davon ausgehen, dass genügend Know-How und Erfahrung vorhanden ist, um einen PC sicher zu machen. Scheuen Sie sich nicht, solche Kleinfirmen nach Referenzen zu fragen. Als Massstab gilt hier: wer auch für Netzwerke von Firmen (KMU) zuständig ist hat vermutlich auch Know-How im Bereich der Sicherheit. Alles Andere ist meistens nicht seriös und kann mit Hilfe einer Rückfrage bei allenfalls angegebenen KMU-Referenzen nachgeprüft werden.

Wer nur auf den günstigeren Preis beim Kauf eines Computers achtet muss damit rechnen, dass er/sie für den Fachmann / die Fachfrau welche(r) den PC später wieder zum Laufen kriegt **wesentlich** mehr ausgeben muss als er/sie beim Kauf des Systems gegenüber dem Fachhändler gespart hat.

8 Benutzung von Ad-Aware SE

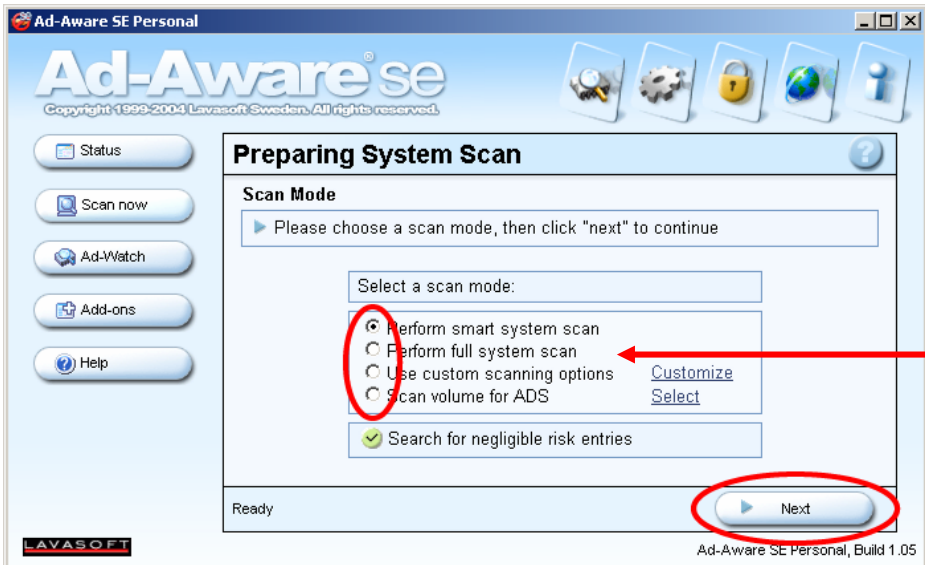
Nach dem Start des Programms sollten Sie zuerst einen Update der aktuellen Informationen machen. Falls der letzte Update schon zu lange zurückliegt werden Sie automatisch dazu aufgefordert.



Internet-Update starten

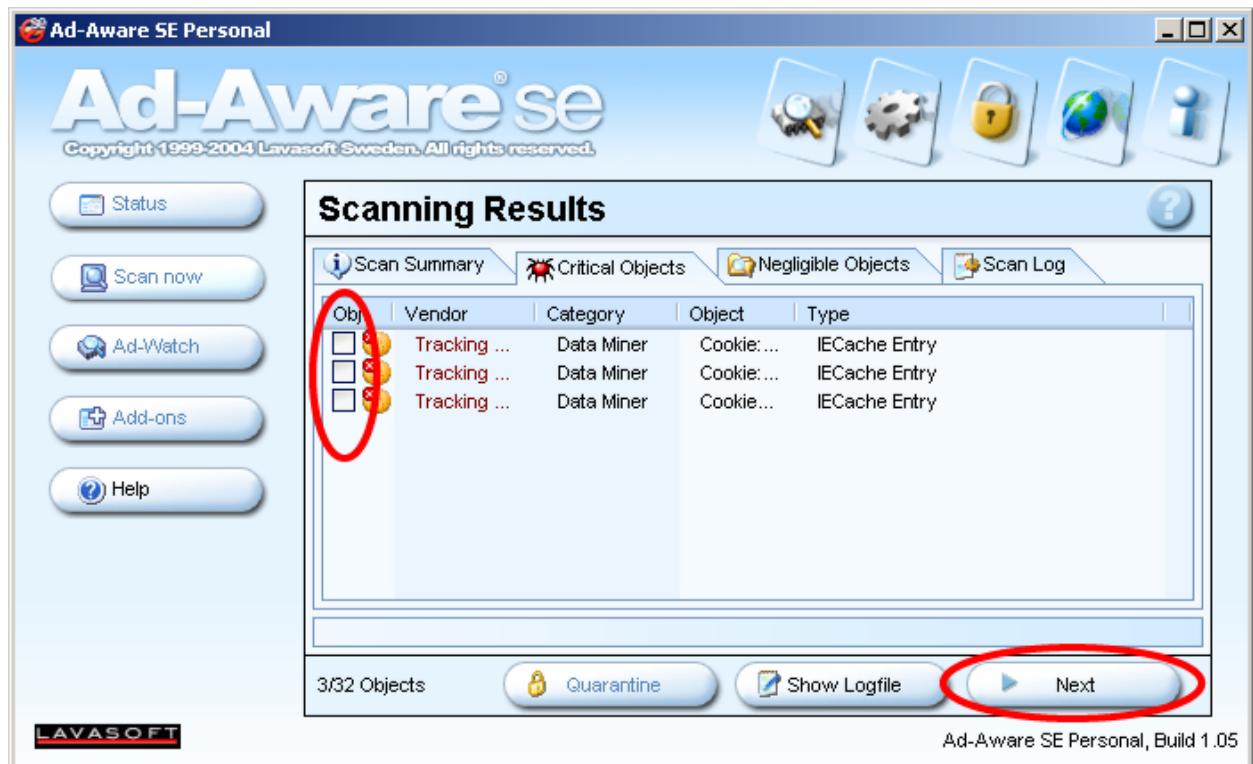
PC-Prüfung starten

Nach dem Update kann mit "Start" die Prüfung des PC gestartet werden. Normalerweise wird ein Smart Scan ausgeführt. Viele Spyware-Hersteller wissen das inzwischen und legen ihre Programme in einem Bereich ab, wo der Smart-Scan nicht überprüft. Sie sollten deshalb immer den "Perform full system scan" ausführen, was allerdings je nach PC 30-90 Minuten dauern kann.

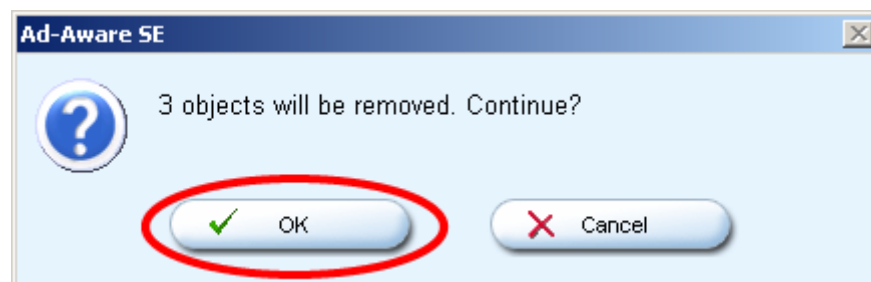


Optionen:
Smart Scan -> "kleine"
Überprüfung
Full Scan -> komplette
Überprüfung

Nach Abschluss des Scans wird das Ergebnis angezeigt. Sie müssen nur auf die "Critical Objects" achten. Wenn hier etwas aufgeführt wird sollten Sie alle Objekte mit dem Kästchen ganz links markieren. Wenn Sie dann auf "Next" klicken werden sie gelöscht. **Hinweis:** wenn Sie mit der *rechten* Maustaste auf ein Kästchen klicken erscheint ein Menu wo Sie "Select all Objects" anwählen können, um alle Einträge auf einen Schlag zu markieren.



Wählen Sie die Objekte zum Löschen aus und klicken Sie auf "Next".



Beantworten Sie die Frage mit "OK", damit werden die zuvor ausgewählten Objekte gelöscht.

9 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 integrierter 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 allein stehenden 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:

<http://www.zonelabs.de/>

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.

Benutzer mit Windows XP aufgepasst: In Windows XP ist eine Firewall integriert! In Warenhäusern und bei Discountern werden immer noch gerne sogenannte Komplettlösungen wie "Norton Internet Security Suite" verkauft. Die Installation eines Antivirus-Programms genügt aber, sofern die im XP integrierte Firewall aktiviert ist. Die Komplettlösung ist natürlich doppelt so teuer wie das reine Antivirus-Programm – und das mag ein Grund sein warum die PC's aus den Warenhäusern schon ab Werk nicht optimal konfiguriert sind. Hier wird der unwissende Kunde einmal mehr über den Tisch gezogen, um ihm zu einem billigen PC teure (unnötige) Zusatzprogramme zu verkaufen. Aus unserer Erfahrung macht die Norton Firewall mehr Probleme als sie löst. Oben genanntes Gratis-Programm "ZoneAlarm" funktioniert wesentlich besser - und wie erwähnt sind unter Windows XP keine weiteren Software-Firewalls notwendig da diese schon in XP integriert ist!

10 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 schriftlich oder im Notfall telefonisch (dann aber Rückruf verlangen) für die notwendigen Informationen an oder bieten allenfalls in einem Mail einen Link an welcher zu einer gesicherten Seite führt.

Gesicherte Sites erkennen Sie am SSL (daran zu erkennen, dass im URL anstelle von <http://> <https://> steht). Inzwischen geraten Sie sogar nach Erhalt eines gefälschten Mails mit entsprechendem Link auf eine SSL-Seite. Allerdings ist diese "gesicherte" Seite nicht echt, was folgendes Beispiel veranschaulicht:

EBay ist ein schönes Beispiel für die Demonstration der unermüdlichen Versuche von Datensammlern (Phisher), mit gefälschten Mails echte Daten zu sammeln. Immer wieder gehen viele böswillige Mails herum, in denen der Absender als 'EBay' gefälscht wird und die Empfänger aufgefordert werden, entweder per Mail ihre Kreditkarteninfos zurückzusenden oder dann in einem im Mail enthaltenen Link die Informationen einzugeben. Klickt man auf den Link erscheint eine Web-Seite die tatsächlich aussieht wie die Seite von EBay. Sie ist auch mit SSL verschlüsselt (das oben genannte Sicherheitskriterium <https://> ist also erfüllt) – und trotzdem handelt es sich um eine Fälschung mit kriminellen Absichten! Untersucht man nämlich den URL genauer (die Adresse im Internet-Explorer) steht da nicht etwa <https://www.ebay....> wie man es erwarten würde sondern z.B. <https://www3.ebay....> oder sonst irgend etwas.

Unser Rat an Sie deshalb: Reagieren Sie grundsätzlich nicht auf alle E-Mails die Sie auf irgendeine Art zur Eingabe von Kreditkarteninfos im Internet bewegen wollen. Nach den vielen Vorfällen in den letzten 18 Monaten schickt Ihnen kein seriöses Unternehmen mehr solche Mails!

Etwas Anderes ist es natürlich, wenn Sie selbst im Internet am Einkaufen sind und zum Abschluss der Bestellung noch die Zahlungsdaten eingeben müssen. Achten Sie in diesem Fall aber immer darauf, dass der Anfang der aktuellen Internetseite mit <https://> beginnt und darauf der reale Name des Anbieters bzw. die ursprünglich aufgerufene Adresse folgt (mit oder ohne www).