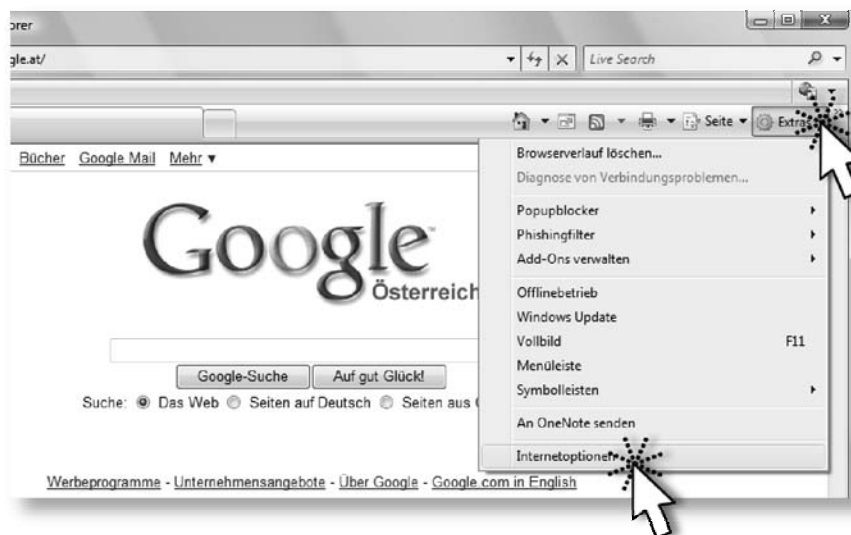


7. Sicherheit im Internet

Temporäre Internet-Dateien (Cache)

Wenn Sie eine HTML-Seite laden, so wird diese nicht nur auf Ihrem Bildschirm angezeigt, sondern sie wird auch in einem bestimmten **Ordner Ihrer Festplatte** mit allen Dateien abgespeichert. So können sie später, wenn Sie die Seite erneut aufrufen, diese **schneller laden**.

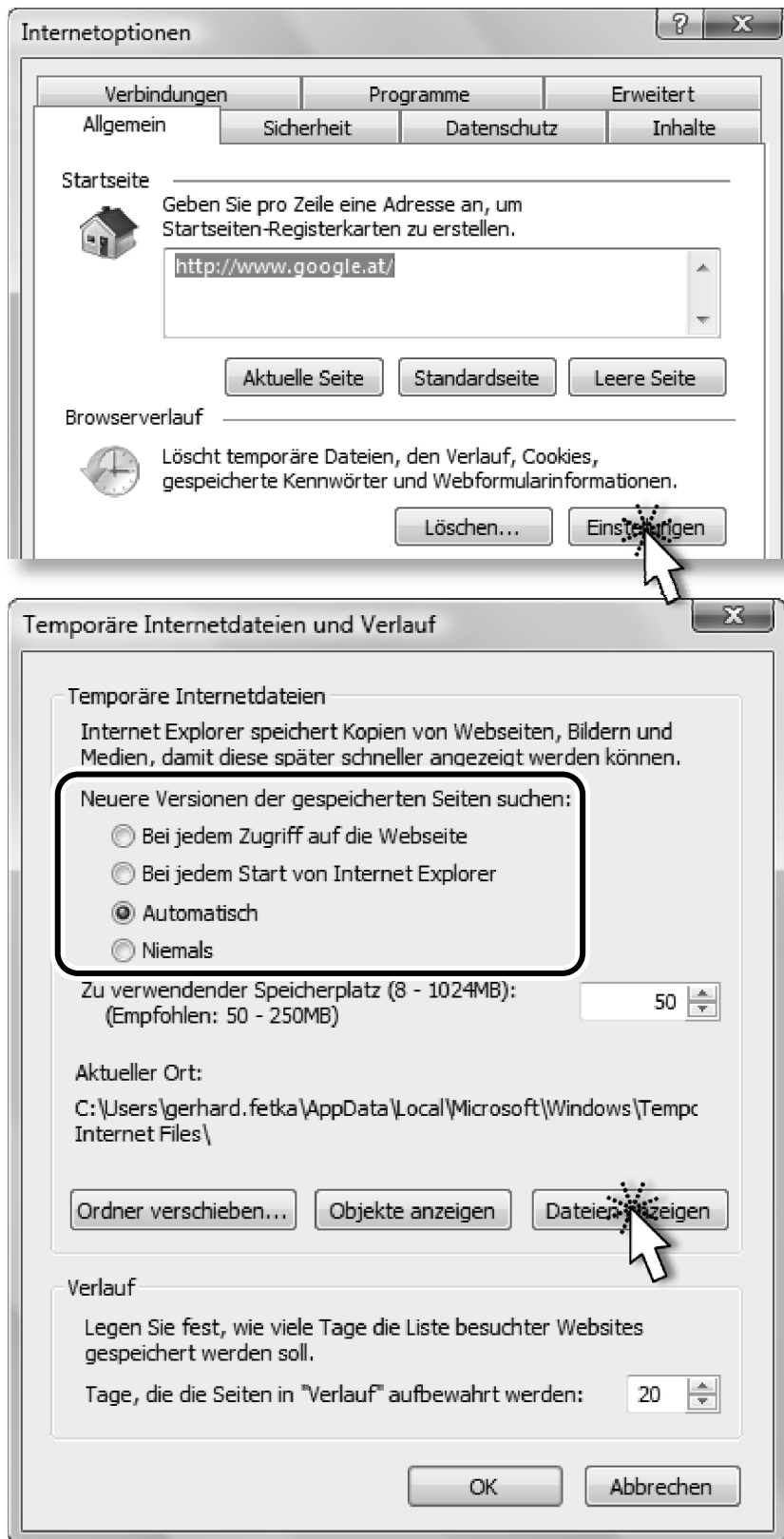
Öffnen Sie die **Einstellungen** der **temporären Internetdateien** in der ersten Registerkarte ALLGEMEIN der INTERNETOPTIONEN.

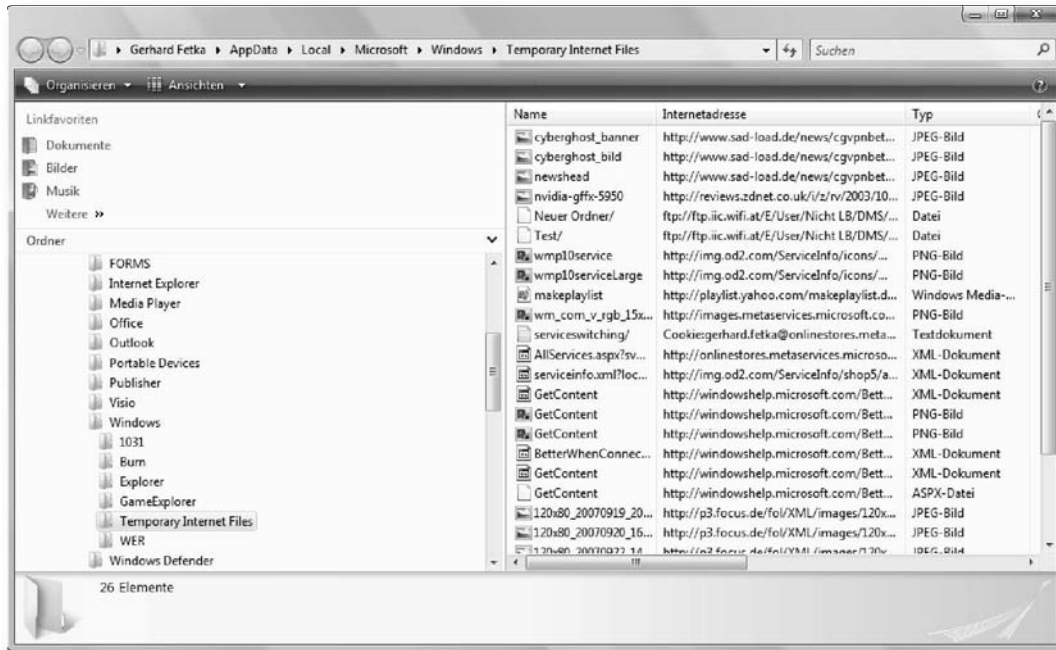


Hier können Sie alle Ihre **temporären Dateien löschen**.



Sie können auf Ihre temporären Internetdateien aber auch zugreifen und diese konfigurieren.





Cookies

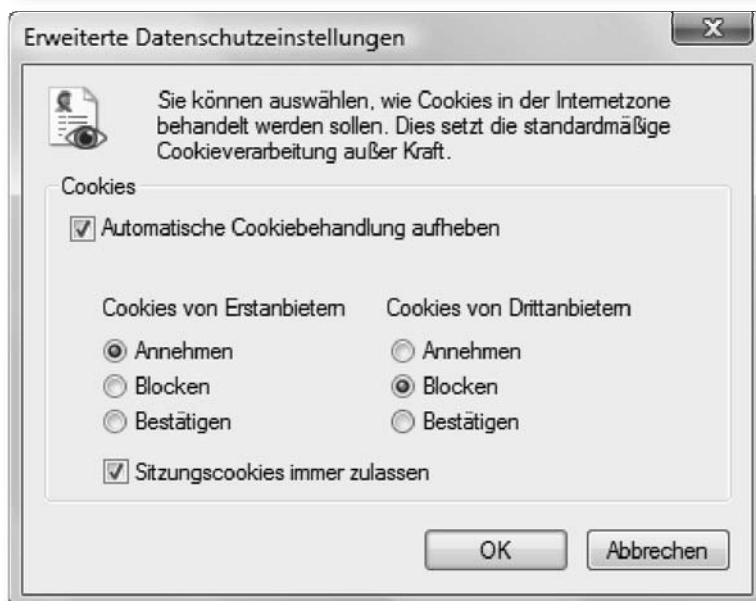
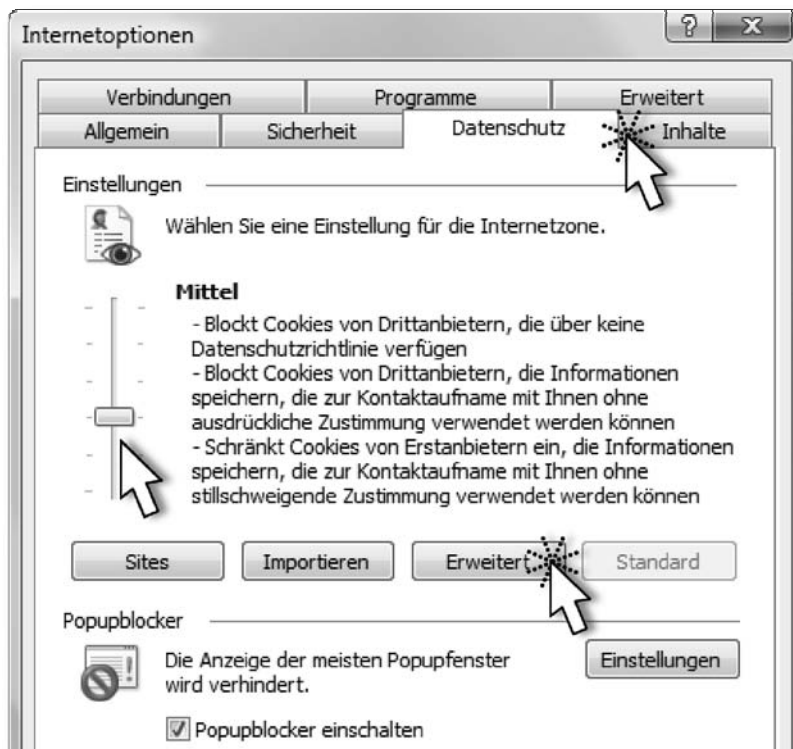
Diese „Kekse“ werden von WWW-Servern meistens als Information über Ihr **Surfverhalten** auf **Ihrer Festplatte** abgelegt.

Die Behandlung dieser verschlüsselten Dateien wird über die **INTERNETOPTIONEN** gesteuert.

Öffnen Sie die **Einstellungen** der **temporären Internetdateien** in der ersten Registerkarte **ALLGEMEIN** der **INTERNETOPTIONEN**.



Wählen Sie die Registerkarte DATENSCHUTZ.



Hier können Sie die Aufnahme dieser „Kuckuckseier“ über einen Schieberegler anpassen.

Viele Server **verweigern** bei Ihrer **Ablehnung** von Cookies die Darstellung gewisser Inhalte. Für **Telebanking-Systeme** und **Webshops** sind Cookies **wichtige Hilfsmittel**, um kurzzeitig Informationen über Ihre Identität und Berechtigung zu speichern.

Firewall

Eine **Firewall** (engl.: *Feuermauer, Brandmauer*) verhindert das aktive Eindringen von Web-Inhalten, wie **Trojanern** (Viren), **ActiveX** und **Java**-Elementen. Auch aktive **Hacker**, also Personen, die sich unbefugt Ihren PC über das Internet zunutze machen wollen, werden so effizient **abgeschirmt**.

Firmen und Büros verwenden meist (teurere) **Hardware-Firewalls**.



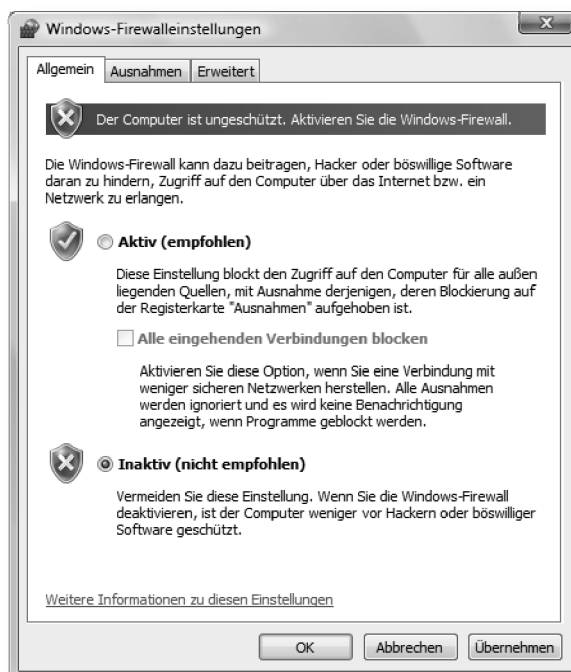
Um eine Firewall für eine Firma gut zu konfigurieren, benötigt man viel **Fachwissen** und **Erfahrung**.

Vorkonfigurierte **Firewalls** sind schon in sogenannten **Internet-Access-Routern** („MODEMS“) eingebaut.



Diese **Netzwerkverteiler** ermöglichen mehreren PCs in einem kleinen Heim- und Firmennetzwerk den gemeinsamen Internet-Zugriff und sind bereits ab **€ 80,-** erhältlich!

Bei Heimanwendern sind Software-Firewalls der unterschiedlichsten Anbieter sehr beliebt. Diese sind aber meistens **nicht notwendig**, da **Windows Vista** bereits eine Firewall **integriert** hat und da die meisten Internet-Router bereits hardwareseitig mit einer Firewall ausgerüstet sind.



Es darf für Ihren PC immer nur **eine einzige Firewall** aktiv sein!
Mehrere Firewalls gemeinsam arbeiten gegeneinander.



Virenschutz

Was ist ein Virus?

Ein Computervirus ist ein schädliches Programm, das sich beliebig vervielfältigen kann und das den Sinn und Zweck verfolgt, den Betriebsablauf Ihres Computers zu stören und sich so schnell wie möglich weiter zu verbreiten.



Meistens werden bei einer Vireninfektion auch Ihre Daten in Mitleidenschaft gezogen!

Viren werden von Menschen geschrieben, deren Motive dafür nicht immer klar sind; meistens sind es Geltungssucht oder Rache.

Sie können sich ein Virus mit Software über dubiose Internet-Seiten mit herunterladen (*downloaden*). Auch so genannte „**Internet-Beschleuniger**“ und Zugänge zu Erotik-Seiten können **Dialer** (teure Einwahl-Nummern) auf Ihrem PC installieren. **Die meisten Viren erhalten Sie allerdings über E-Mails, die Sie bewusst öffnen.**

Es gibt die verschiedensten Arten von Viren. Zurzeit sind einige tausend Virenstämme bekannt.

Die wichtigsten Virenarten aus dem Internet:

- o **Trojanische Pferde (Trojaner)**

... werden von Anwendern selber (als Dateianhänge in E-Mails) geöffnet, in der Meinung, es handle sich um ein unverzichtbares **Gratisprogramm**, um lustige oder pikante **Bildschirmschoner** oder um nützliche **Informationen**.



Ein Trojaner öffnet Hackern eine Hintertür zu Ihrem PC und verbreitet sich über Ihr E-Mail-Adressbuch.

o **Würmer**

... verbreiten sich selbständig und extrem schnell in Netzwerken. Würmer sind für **mittlere** und **große Firmen** eine größere Gefahr als für Heimnetzwerke.

o **Dialer**

... ändern die **Rufnummer** Ihrer Einwahlverbindung (MODEM und ISDN) in eine **teure Mehrwertnummer**. **Breitband-Verbindungen** (DSL, Telekabel, mobil) können von Dialern **nicht verwendet** werden!



o **Hoaxes**

... sind Scherz- und Falschmeldungen, die als E-Mail-Virus-Warnungen getarnt sind. Den **Schaden** richten dann die **Anwender** oft **selber** an, indem sie wichtige, als „Virus“ verunglimpft **Systemdateien** vorsichtshalber löschen.

o **Phishing**

... ist die zurzeit gefährlichste Virenart für Sie! Diese fingierten E-Mails **täuschen** authentische **E-Mails** von **Banken** vor und fordern die Kunden auf, ihre elektronischen Unterschriften (**TAN**) einzugeben. Wenn Sie das tun, dann wird Ihr Konto von **gut organisierten Banden** leergeräumt!



Sie erkennen Phishing-E-Mails (auch) am schlechten Deutsch.

Was können Sie gegen Viren tun?


MS Office-Programme prüfen automatisch vor dem Öffnen eines Dokuments oder einer einer E-Mail **beigefügten Datei**, ob diese bedenkliche Strukturen oder Dateinamen-Erweiterungen enthalten.

Sie benötigen allerdings trotzdem ein gutes **Anti-Viren-Programm**, das sich in regelmäßigen Abständen automatisch über das Internet **aktualisiert**, Ihre E-Mails **überwacht** und Ihren Computer auf Virenbefall **überprüft**.

Antiviren-Software aus dem Web laden

Schritt 1 Starten Sie den Internet Explorer. Sie brauchen dafür eine Verbindung zum Internet.



Schritt 2 Klicken Sie in die **Adresszeile** des Internet Explorers, **tippen** Sie *www.free-av.de* und **bestätigen** Sie diese Adresse mit der **Eingabetaste** .



Hier finden Sie das hervorragende, **kostenlose** Programm von **Avira**.



Anmerkung:

Diese Seite kann zum Zeitpunkt Ihres Besuches anders aussehen als sie hier gezeigt wird!

Klicken Sie auf den Link zum Download der Software.

Schritt 3



Laden Sie jetzt das Programm auf Ihren PC.

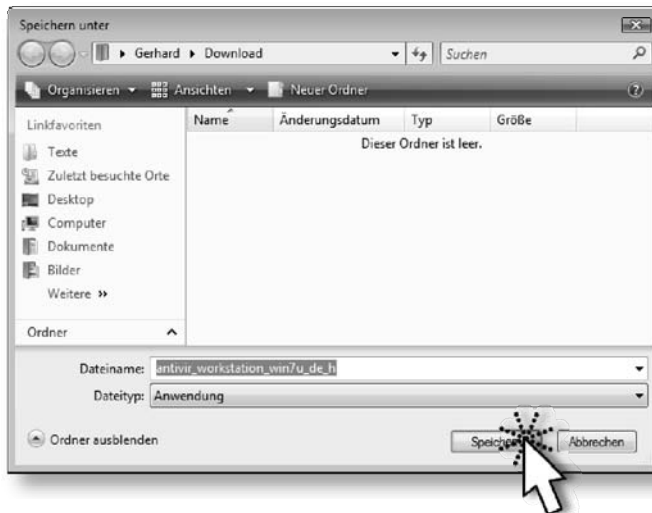
Schritt 4



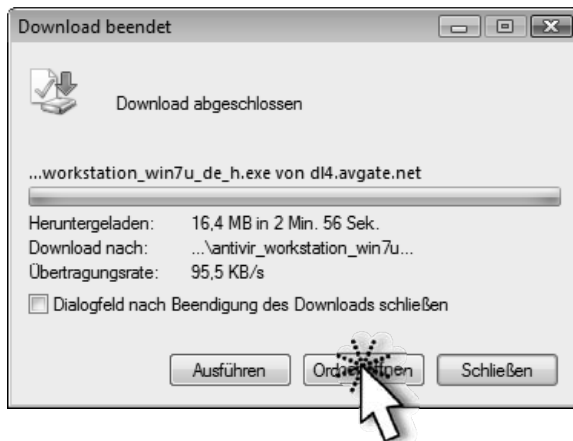
Die Abfrage des Dateidownloads beantworten Sie mit .



Schritt 5 Wählen Sie den Speicherort.



Schritt 6 Jetzt wird es etwas dauern. Wenn das Herunterladen beendet ist, dann öffnen Sie den Speicherort mit **Ordner öffnen**.



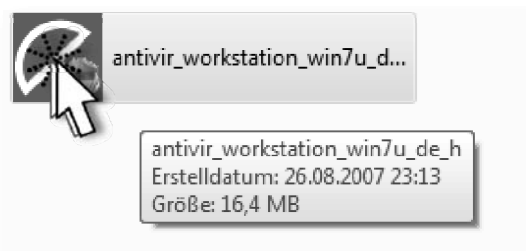
Antiviren-Software installieren



Zum **Installieren** von **Software** auf einem Computer benötigen Sie **Administrator-Rechte!**

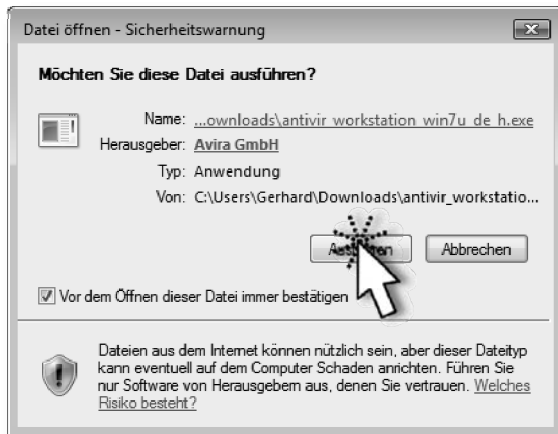
Schritt 7

Starten Sie die **Installation** von **Avira AntiVirus** durch einen **Doppelklick** auf die Datei im geöffneten Ordner **DOWNLOAD**.



Bestätigen Sie die **Sicherheitswarnung** mit **Ausführen**.

Schritt 8



Bestätigen Sie auch die nachfolgende Warnung der **Benutzerkontensteuerung**.

Schritt 9

Gehen Sie nun im **Assistenten** fortgesetzt mit **Weiter >** weiter und **bestätigen** Sie allfällige Vereinbarungen bezüglich **Lizenzvertrag** und rein **privater Nutzung**.

Stellen Sie dann den Installations-Assistenten **fertig**.



Schritt 10

Den Computer auf Viren manuell überprüfen

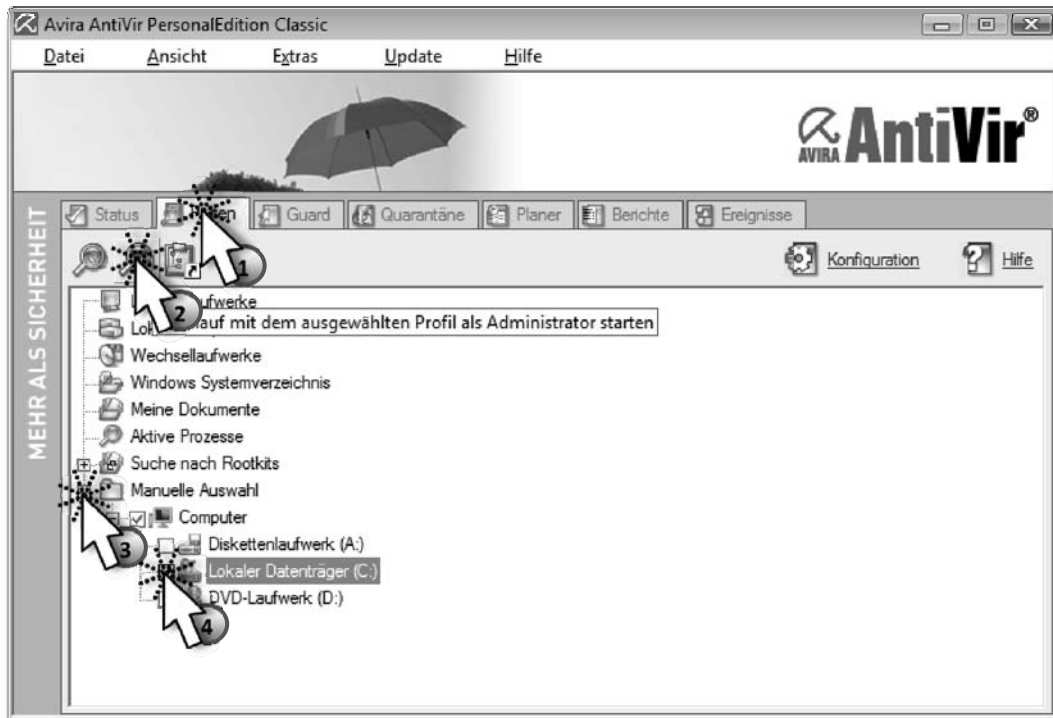
Antiviren-Programme laufen nach ihrer Installation **ständig im Hintergrund** und **überwachen** Ihren PC. Sie finden das Symbol eines Antiviren-Programms **immer im Info-Bereich** Ihrer **Taskleiste**.

Starten Sie von dort Ihr Antiviren-Programm mit einem Doppelklick.

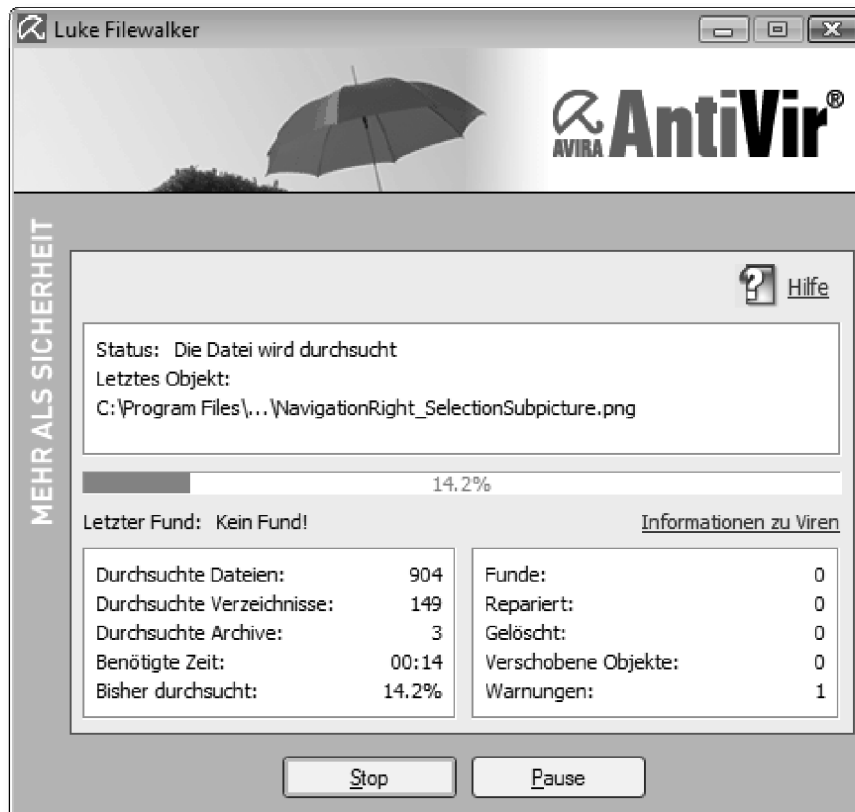
Schritt 1



Schritt 2 Im **Hauptbildschirm** können Sie **Einstellungen** vornehmen und **Prüfungen starten**. Starten Sie jetzt die Prüfung Ihrer **Festplatte C:**.



Die Prüfung wird durchgeführt.



Wenn ein Virus gefunden wird, schlägt das Programm **Alarm**.



Sie haben jetzt die Wahl, ob Sie ...

Schritt 3

- ... das beschädigte Programm durch **Quarantäne** isolieren wollen,
- ... das beschädigte Programm **löschen** wollen,
- ... den **Zugriff** auf das beschädigte Programm **verhindern** wollen,
- ... das beschädigte Programm einfach **ignorieren** wollen oder,
- ... das beschädigte Programm **reparieren** (desinfizieren) wollen.

Eine **Reparatur** ist **selten möglich**. **Löschen** Sie das beschädigte Programm lieber!



Antiviren-Software updaten

Gerade bei einem Antiviren-Programm ist regelmäßiges **Updating** (Instandhalten) ein **unverzichtbarer Bestandteil** Ihrer Vorsorge zur Datensicherheit.

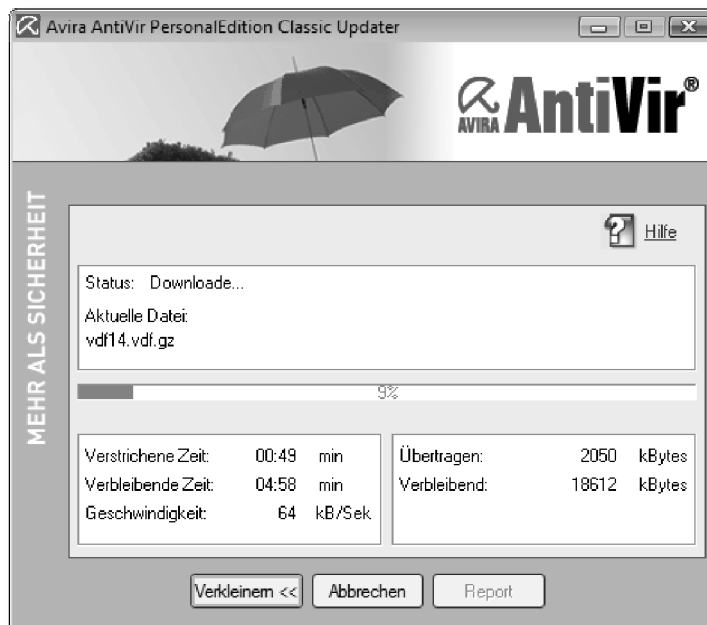
Viele Hersteller von Antiviren-Programme verlangen für automatische Update-Abos **Geld**.

Avira AntiVirus aktualisiert sich **täglich gratis** mit den neuesten **Viren-Kennungen** – dafür darf Sie aber auch ab und zu eine **Werbe-einschaltung** nicht stören.

Nach der Installation fragt Avira, ob das Programm eine Verbindung zum **Internet** für ein **Update** herstellen soll. **Bestätigen** Sie die Dialogbox.



Die neuesten Viren-Kennungen werden vom Avira-Server heruntergeladen.



Sichere Internet-Verbindungen

Manchmal ist es wichtig, dass Ihre Bewegungen und Aktionen auf Internetseiten vor den Blicken Unbefugter verborgen sein müssen. Das betrifft vor allem:

- Telebanking
- Webshopping und Kreditkartenzahlungen
- Web-Formulare für persönliche Daten
- öffentliche Verwaltung und Gesundheitswesen

Vertrauliche Bereiche der sogenannten **New Economy**, also **eCommerce** und **eBusiness**, sowie auch sensible Bereiche der öffentlichen Verwaltung (**eGovernment**) werden über das sichere Internet-Protokoll



https (*Hyper Text Transfer Protocol Secure sockets*)

verschlüsselt (**encrypted**) und über digitale Zertifikate abgewickelt.

Digitale Zertifikate



Ein digitales Zertifikat für Webseiten wird von einer Zertifizierungsstelle für Webseiten ausgestellt. Damit wird die Identität des Inhabers sichergestellt.

Eine der Zertifizierungsfirmen ist **VeriSign**. Hier können Inhaber von Webseiten persönliche Zertifikate kaufen.



Weitere Anbieter:

GlobalSign, Thawte und a.trust (www.a-trust.at).

Digitale Zertifikate sind immer an lebendige Personen gebunden und sollen veröffentlicht werden. Ein Klick auf das **Zertifizierungslogo** der Webseite zeigt Ihnen die **Identität** des Herausgebers:

19/3/2008 19:20
www.verisign.de verwendet VeriSign-Dienste folgendermaßen:

SITENAME:	www.verisign.de
SSL-ZERTIFIKAT-STATUS:	Gültig (15-May-2007 bis 11-Jan-2009)
FIRMA/ORGANISATION:	VERISIGN, INC. Mountain View California, US

	Verschlüsselte Datenübertragung	Diese Website kann Ihre persönlichen Informationen über ein VeriSign SSL-Zertifikat sicher übertragen. Informationen, die mit Adressen ausgetauscht werden, die mit https beginnen, werden vor der Übertragung mittels SSL verschlüsselt.
	Identität verifiziert	VERISIGN, INC. wurde als Eigentümer oder Betreiber der Website unter www.verisign.de verifiziert. Offizielle Unterlagen bestätigen, dass VERISIGN, INC. ein rechtsgültiges Unternehmen ist.

Vergewissern Sie sich immer, dass die Adresse der Website, die Sie besuchen, mit der gewünschten Adresse übereinstimmt, um die bestmögliche Sicherheit bei Website-Besuchen zu gewährleisten. Stellen Sie sicher, dass der URL dieser Seite mit "https://seal.verisign.com" beginnt. >> REPORT SEAL MISUSE

Einkaufen im Internet

Aufgabe:

Lernen Sie das Einkaufen im Internet in einem Webshop kennen.

Lernziele:

- Webshops
- der Bestellvorgang
- web-basierende Formulare



Dieser (echte) Webshop soll jetzt als nur als **Beispiel** dienen. Bitte schließen Sie den Bestellvorgang **nicht** ab!

Schritt für Schritt:

Schritt 1

Besuchen Sie einen Webshop.

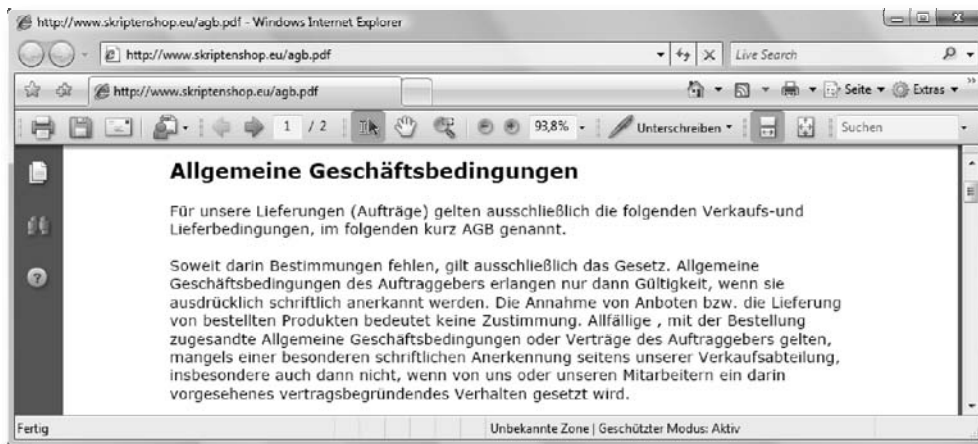


Schritt 2

Lesen Sie die Allgemeinen Geschäftsbedingungen (AGB):



Sie sollten die **allgemeinen Geschäftsbedingungen** eines Webshops vor dem Einkauf immer **gründlich lesen!**



Suchen Sie ein Produkt legen Sie es in den **Einkaufswagen** und schließen Sie den Einkauf ab.

Schritt 3



Bei den meisten Webshops müssen Sie sich als Kunde registrieren.



Nachdem Sie Ihre persönlichen Daten in das Webformular eingetragen haben, überprüfen Sie Ihre Bestellung.



Als Zahlungsmittel sind meistens **Kreditkarte** oder **Nachnahme** üblich.

Bestellen Sie jetzt aber nicht! Sonst wird geliefert ...!



Kreditkarten



Kreditkarten sind ein beliebtes und sicheres Zahlungsmittel.

Sie können **Zahlungen** im **WWW** oft mit nur **vier Angaben** tätigen:

- **Kreditkartenfirma:** *MasterCard*
- **Kartenbesitzer:** *Annamaria Hinterbacher*
- **Kartenummer:** *1234 5678 9123 0005*
- **Verfallsdatum:** *10/2010*

Diese wenigen vertraulichen Daten genügen, um Geld zu bewegen!

Selbstverständlich müssen diese Transaktionen sicher und **verschlüsselt (encrypted)** ablaufen:



Achten Sie bei Kreditkartenzahlungen **immer** auf das verschlüsselte **https**-Protokoll und auch auf mögliche **digitale Zertifikate** des Shopbetreibers!

Sie werden vom Internet Explorer informiert, wenn Sie sichere, verschlüsselte Seiten betreten oder verlassen:

Eine sichere Seite erkennen Sie an diesem **Symbol in der Adresszeile:**



Weitere Angaben zu Ihrer Sicherheit beim Einkauf im WWW:

CVC-Code

Cardholder Verification Code

= die letzten drei Ziffern der Nummer im Unterschriftsstreifen



Zusätzliche Kennwörter oder Codes für E-Commerce



Gefahren bei der Verwendung von Kreditkarten:

- Sie können bei der Bezahlung im WWW **betrogen** werden.
- Beispiel: Ihre über ein Web-Auktionshaus (z.B. *eBay*) ersteigerte und mit Kreditkarte **bezahlte Ware** wird vom Verkäufer **nicht geliefert**.
- Ihre **Kreditkartennummer** mit Verfallsdatum kann **ausgespäht** werden.
- Eine **andere Person kauft** mit diesen Daten in Ihrem Namen ein.
- Ihre Kreditkarte kann **gestohlen** werden.
- Sie haben unvorsichtigerweise auch den **PIN-Code** für die Barbehebung in der Geldbörse notiert. Eine **andere Person** behebt mit dieser Karte **Bargeld** an Geldausgabe-Automaten.

Aber auch dann, wenn Ihre Daten missbräuchlich verwendet wurden, ist der **Schaden leicht zu begrenzen**, wenn Sie gegen die betreffenden Abbuchungen **SOFORT Einspruch** erheben:

*Mit der **Meldung** an die Kreditkartenfirma ist der Karteninhaber **von der Haftung befreit**. Tritt **zwischen** Ereignis und Meldung ein **Schaden** ein, so ist die Haftung der Karteninhabers bei Handelsumsätzen mit **€ 72,67** begrenzt.*

*Bei einer missbräuchlichen Verwendung der **Kreditkarte und PIN** zum Bargeldbezug an Automaten beträgt die Haftung je Abrechnungsperiode **€ 1.200,-**. Grundsätzlich ist ein Missbrauch unter Verwendung der Geheimzahl nur dann möglich, wenn **Täter** neben der Kreditkarte auch **Kenntnis der richtigen PIN** hat. Daher soll die **PIN nicht aufgezeichnet** werden. Bei Verwendung der PIN ist darauf zu achten, dass kein Unbefugter sich diese Information aneignen kann (Ausspähen).*

Kontrollieren Sie immer Ihre monatlichen Kreditkarten-Abrechnungen!



Eine Kreditkarte ist trotz allem eines der sichersten Zahlungsmittel für den Warenverkehr im Internet.