Das Franzis Praxisbuch
288 Seiten praktisches Internet-Know-how

Thomas Schirmer / Andreas Hein

Internet-Praxisbuch

Anschließen · Absichern · Lossurfen

- DSL und WLAN anschließen und konfigurieren
- So beherrschen Sie Facebook, Twitter & Co.
- Die optimalen Einstellungen für Internet Explorer, Mail und Chat

FRANZIS

Inhaltsverzeichnis

10 Online-Gefahren: So schützen Sie sich effektiv

Wie Sie in den vorhergehenden Kapiteln erfahren haben, bietet das Internet eine Unmenge interessanter Möglichkeiten. Sie können sich informieren und weiterbilden, aktuelle Nachrichten aus aller Welt abrufen, im Web günstig einkaufen und Reisen buchen oder planen, Ihre Geldgeschäfte unabhängig von Öffnungszeiten der Banken erledigen, per E-Mail, Chat oder Video-Internet-Telefonie mit Menschen rund um den Globus zum Nulltarif kommunizieren und vieles mehr. Alle diese Nutzungsmöglichkeiten lassen das Internet immer mehr zu einem unverzichtbaren Medium werden. Allerding gibt es leider auch eine Schattenseite. So zieht das Internet mit den zunehmenden Nutzerzahlen leider auch immer mehr Betrüger und Gauner an, die sich durch verschiedene Arten von Schadprogrammen und Betrügereien bereichern wollen.

Allerdings sind Sie derartigen Angriffen nicht schutzlos ausgeliefert. Ganz im Gegenteil können Sie durch Verwendung von Schutzprogrammen und einem sicherheitsbewussten Verhalten die Risiken auf ein Minimum reduzieren, sodass Sie weitgehend unbeschwert im Internet surfen können.

10.1 Gefahren im Internet

Das Internet ist zu einem echten Massenmedium geworden und wird von immer mehr Menschen auch für Zwecke wie Einkaufen oder das Online-Banking genutzt. Mit dieser Kommerzialisierung wird das Internet aber auch für Ganoven und Betrüger aller Art attraktiv, die sich hier bereichern wollen.

Die modernen Internet-Kriminellen zielen und arbeiten mit immer komplexeren und verfeinerten Methoden.

Während noch vor einigen Jahren Computerviren zumeist von jugendlichen »Amateuren« stammten, die mit diesen Schadprogrammen oftmals lediglich ihre Fähigkeiten auf diesen Gebiet unter Beweis stellen wollten, stammen die modernen

Schadprogramme von Profi-Entwicklern und es hat sich eine hochgradig arbeitsteilige Szene im Bereich der Computer-Kriminalität entwickelt.

Wurden früher daher spektakuläre Computerviren und Computerwürmer entwickelt, die sich innerhalb kürzester Zeit auf Millionen PCs ausbreiteten und sichtbare Beeinträchtigungen oder Schäden hervorriefen, arbeiten die modernen Schadprogramme gut getarnt und weitgehend unbemerkt.

Spyware, Backdoors, Trojaner und Co.

Heute dominieren Schädlinge wie Spyware, Backdoors und Trojaner die Szene der Schadprogramme. Bei Spyware handelt es sich um Spionageprogramme, die beispielsweise die Aktivitäten der Anwender beim Surfen protokollieren oder sogar sämtliche Eingaben aufzeichnen und auf diese Weise dann z. B. auch geheime Zugangsdaten wie Benutzernamen und Kennwörter ausspionieren können. Mit diesen gesammelten Daten kann dann ein erheblicher Missbrauch betrieben werden, etwa beim Online-Banking, aber auch bei anderen Internet-Diensten (z. B. eBay-Konten). Die Täter können damit die Identität der ahnungslosen Opfer annehmen und auf deren Kosten z. B. Waren bestellen etc.

Backdoors werden solche Werkzeuge genannt, die den PC so manipulieren, dass von außen, also über das Internet hierauf zugegriffen werden kann, ohne dass dies der Nutzer direkt merkt. Über eine solche Backdoor können dann wiederum andere Schadprogramme auf den Rechner gelangen bzw. der Rechner kann ferngesteuert werden. Als Trojaner bezeichnet man Schadprogramme, die heimlich auf den Rechner gelangen und sich dabei in anderen Programmen bzw. Dateien verstecken.

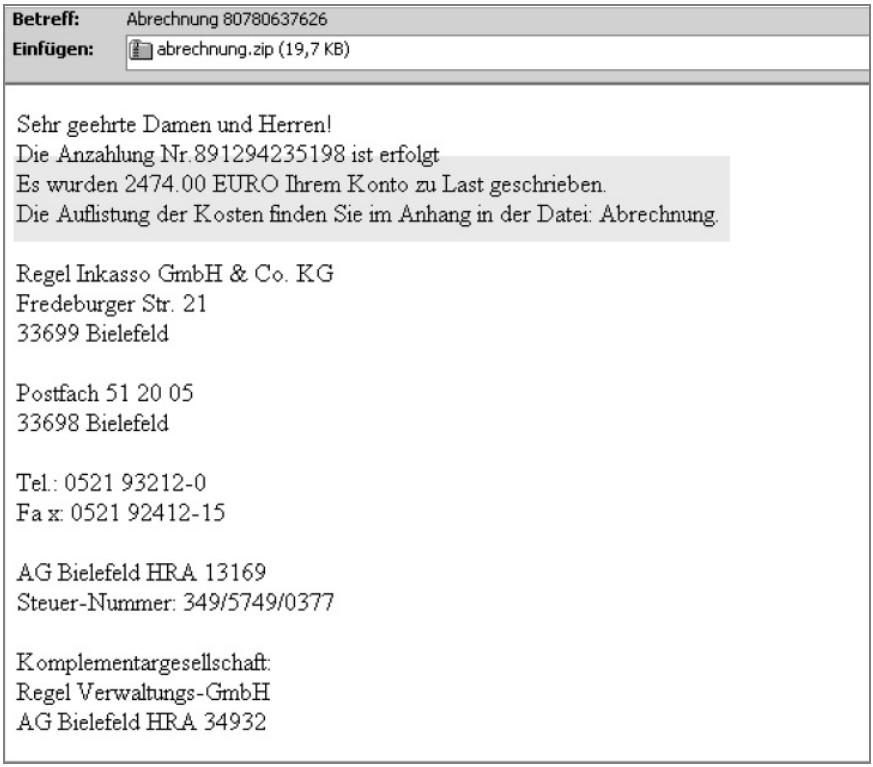
Neben den Daten auf den Rechnern stellen auch schon die PCs und Internetverbindungen der Opfer selbst einen erheblichen Wert für die Ganoven dar. So können Sie etwa eine Schadsoftware auf einen Rechner schmuggeln, über die Sie dann weitgehend die Rechneraktivitäten manipulieren können. Hierüber lassen sich derartig manipulierte PCs etwa zum Versand von Spam-Mails missbrauchen. Nach Schätzungen von Experten gibt es mittlerweile Millionen derartig infizierter PCs, die dann zentral von den Angreifern gesteuert und damit dann auch für andere kriminelle Zwecke missbraucht werden können. Organisiert sind diese ferngesteuerten Rechner in sogenannten Bot-Netzen. Die größten dieser Bot-Netze sollen sogar mehr als eine Million PCs enthalten.

Denkbar sind damit etwa gezielte Angriffe auf Webserver oder andere Rechner im Internet. Dazu werden die Rechner so eingesetzt, dass sie gleichzeitig sehr viele Anfragen an das potenzielle Opfer richten, um diesen Server durch Überlastung lahmzulegen. Auf diese Weise können etwa Betreiber von Internet-Shops erpresst werden, denn die Ausfälle der Webserver verursachen erhebliche Umsatzeinbußen und sorgen bei den verärgerten Kunden, die die überlasteten Shops nicht mehr erreichen können, für Unzufriedenheit.

So gelangen die Schädlinge auf Ihren PC

Bis vor Kurzem brachten die Kriminellen die Schadprogramme vor allem über E-Mails in Umlauf. Die unerwünschte Software versteckte sich dabei in den Dateianhängen, die hier mitgeschickt werden. Erst wenn diese Anhänge geöffnet werden, können sich die Schädlinge auf dem PC des Opfers einrichten.

Damit die Empfänger diese Anhänge tatsächlich auch öffnen, wenden die Ganoven immer raffiniertere Techniken an. So werden oftmals Drohszenarien aufgebaut und in der E-Mail steht etwa von einer hohen Telefon- oder Providerrechnung, einer Strafanzeige wegen illegaler Downloads oder ähnliches. Für weitere Details zu dem Vorrang sollen die Empfänger dann den Dateianhang öffnen. Derart unter Druck gesetzt, vergessen viele Menschen dann ihre Vorsicht, öffnen den Anhang und infizieren damit den Rechner.



Betreff: Abrechnung 80780637626
Einfügen: abrechnung.zip (19,7 KB)

Sehr geehrte Damen und Herren!
Die Anzahlung Nr.891294235198 ist erfolgt
Es wurden 2474.00 EURO Ihrem Konto zu Last geschrieben.
Die Auflistung der Kosten finden Sie im Anhang in der Datei: Abrechnung.

Regel Inkasso GmbH & Co. KG
Fredeburger Str. 21
33699 Bielefeld

Postfach 51 20 05
33698 Bielefeld

Tel.: 0521 93212-0
Fa x: 0521 92412-15

AG Bielefeld HRA 13169
Steuer-Nummer: 349/5749/0377

Komplementargesellschaft:
Regel Verwaltungs-GmbH
AG Bielefeld HRA 34932

Bild 10.1: Mit E-Mails wie diesen versuchen die Betrüger die Empfänger zum Öffnen von verseuchten Dateianhängen zu bewegen.

Um mögliche Virenschutzprogramme zu täuschen, verstecken die Ganoven die Schädlinge oftmals wie im obigen Beispiel in Zip-Dateien, die mitunter nicht bzw. nur unzureichend kontrolliert werden.

Einfallstor Browser und Zubehör

Seit einiger Zeit werden die Schadprogramme allerdings auch immer öfter direkt über manipulierte Webseiten in Umlauf gebracht. Schlimmstenfalls reicht es dann schon aus, eine derart manipulierte Seite aufzurufen, und schon wird die Schadsoftware übertragen und aktiviert.

Dabei können auch ganz seriöse und bekannte Internet-Auftritte von den Betrügern manipuliert worden sein, ohne dass die Betreiber der Website davon etwas mitbekommen. Es wurden auch Angriffe registriert, bei denen die Gefahr durch die auf den Webseiten eingeblendeten Werbebanner ausging.

Bei diesen Angriffen werden Sicherheitslücken im Browser, zunehmend aber auch in Zusatzprogrammen, wie etwa den beschriebenen Multimedia-Playern, ausgenutzt. Selbst Programme wie *Word*, *Excel* oder PDF-Reader werden immer öfter missbraucht, indem entsprechend manipulierte Dokumente mit Schadsoftware infiziert werden und beim Öffnen dieser Dokumente die Infektion erfolgt.

Spionage, Manipulation, Missbrauch

Die neuen Schadprogramme können ganz unterschiedliche Ziele verfolgen. So gibt es beispielsweise hochspezialisierte Banking-Trojaner, die es auf die Zugangsdaten der Nutzer von Online-Bankkonten abgesehen haben. Dazu werden die Internetverbindungen überwacht und beim Aufruf der Website einer Online-Bank werden die hier vorgenommenen Eingaben überwacht und an die Betrüger übermittelt.

Andere Schädlinge stehlen auf ähnliche Art und Weise Zugangsdaten zu anderen Online-Diensten. Mit diesen Daten können die Betrüger dann ebenfalls Unheil anrichten, etwa wenn sie über das eBay-Konto eines ahnungslosen Nutzers Waren erwerben oder Diebesgut anbieten.

Eine andere Art der Bedrohung besteht darin, dass Ihr PC nach dem Befall einer Schadsoftware quasi ferngesteuert werden kann. Diese Armeen ferngesteuerter PCs nennen die Fachleute auch Bot-Netze und die einzelnen Rechner werden mitunter als Zombie-Rechner bezeichnet.

An Bedeutung verloren haben dagegen die Dialer. Hierbei handelt es sich um Schadprogramme, die bei Wählverbindungen per Modem und ISDN die eigentlich am PC eingerichtete und gewünschte Verbindung durch einen deutlich teureren Dienst ersetzen. Da jedoch immer weniger Internetnutzer diese Verbindungsart nutzen, spielt auch diese Bedrohung nur noch eine geringe Rolle. Bei modernen Breitbandverbindungen (DSL, Kabel) gibt es diese Art von Betrügereien dagegen nicht.

Nicht nur per E-Mail

Diese Schadprogramme können jedoch nicht nur per E-Mail auf Ihren Rechner gelangen, immer öfter finden diese Angriffe auch über ganz normale Webseiten statt. Schwachstellen im Browser oder in anderen Programmen, mit denen Dateien aus dem Internet direkt geöffnet bzw. wiedergegeben werden, werden dabei ausgenutzt. Es kann dann schon ausreichen, eine entsprechend manipulierte Webseite aufzurufen, und schon wird der Schädling übertragen.

Nicht alle Schädlinge werden über das Internet übertragen, auch andere Datenträger, etwa CDs, USB-Sticks oder Flash-Speicherkarten können mitunter unerwünschte Software enthalten. Auch bei Nutzung dieser Speichermedien sollten Sie daher vorsichtig bleiben.

10.2 So können Sie sich schützen

Den Bedrohungen aus dem Internet sind Sie allerdings nicht gänzlich schutzlos ausgesetzt. Ganz im Gegenteil gibt es verschiedene Schutzmaßnahmen, mit denen Sie Ihren PC weitestgehend vor diesen Gefahren sichern können. Neben verschiedenen technischen Einrichtungen trägt zudem ein vorsichtiges Verhalten viel zu einer besseren Sicherheit bei. Die wichtigsten Sicherheitsmaßnahmen wollen wir Ihnen daher an dieser Stelle kurz beschreiben.

Antiviren-Software

Zu den wichtigsten Schutzvorkehrungen gehört ein Antiviren-Programm, das auf jedem Rechner vorhanden sein sollte. Diese Programme kontrollieren üblicherweise während der PC-Nutzung im Hintergrund jeden Zugriff auf Dateien aller Art und geben bei Verdacht entsprechende Warnhinweise bzw. blockieren den Vorgang.

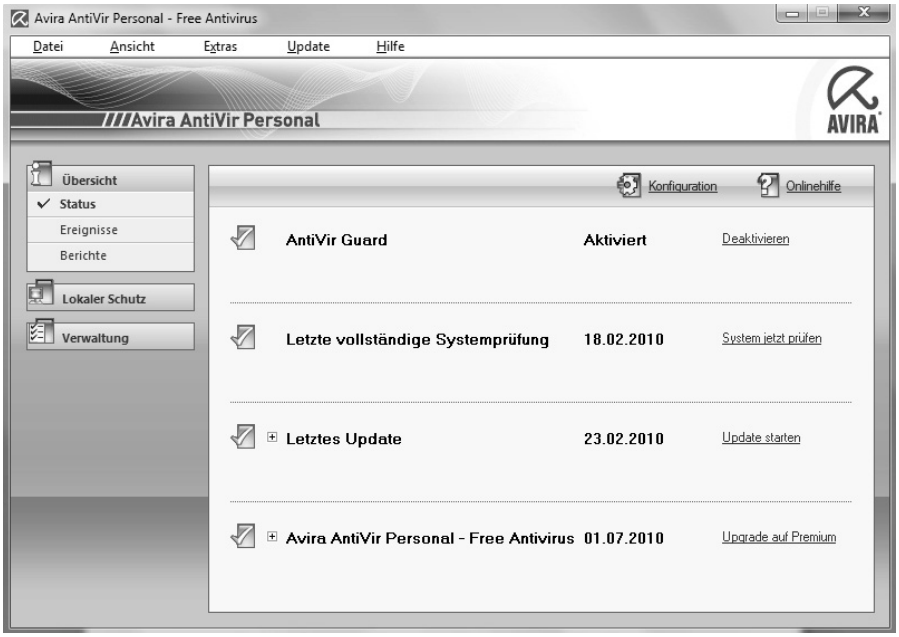


Bild 10.2: Nur ein Virenschutz mit aktuellen Updates kann Sicherheit bieten.

Mittlerweile schützen die meisten der Antiviren-Programme auch gegen die neueren Schadprogramme wie Spyware oder Backdoors. Auch beim Surfen im Web schützen immer mehr dieser Programme, allerdings gibt es leider auch einige Anwendungen, die gerade diesen wichtigen Schutz nicht bieten.

Generell ist es bei Antiviren-Programmen allerdings so, dass sie eine Schadsoftware anhand eines charakteristischen Merkmals erkennen müssen, um diese eindeutig zu identifizieren und davor zu schützen. Dazu wiederum muss diese Schadsoftware ja bereits bekannt sein bzw. verwendet werden. Erst mit einiger Verzögerung können die Hersteller von Antiviren-Programmen ihre Produkte daher entsprechend aktualisieren. Mittlerweile erfolgen diese Updates meist sogar mehrmals täglich, um mit der immens gewachsenen Zahl von Schadprogrammvarianten mithalten zu können.

Nur ein aktuelles Antiviren-Programm bietet Schutz
Einen guten Schutz kann ein Antiviren-Programm nur dann bieten, wenn es permanent aktualisiert wird. Programme, die über längere Zeit nicht mehr auf den neuesten Stand gebracht wurden, wiegen den Anwender dagegen lediglich in einer trügerischen Sicherheit, da viele Schadprogramme unerkannt bleiben.

Ein Antiviren-Programm müssen Sie sich als Windows-Anwender in jedem Fall separat anschaffen, denn zum Lieferumfang von Windows gehört eine solche Software nicht. Zu den bekannten Anbietern gehören Software-Unternehmen wie Avira (*www.avira.de*), Kaspersky (*www.kaspersky.de*), AVG (*www.avg.de*) oder Symantec (*www.symantec.de*).

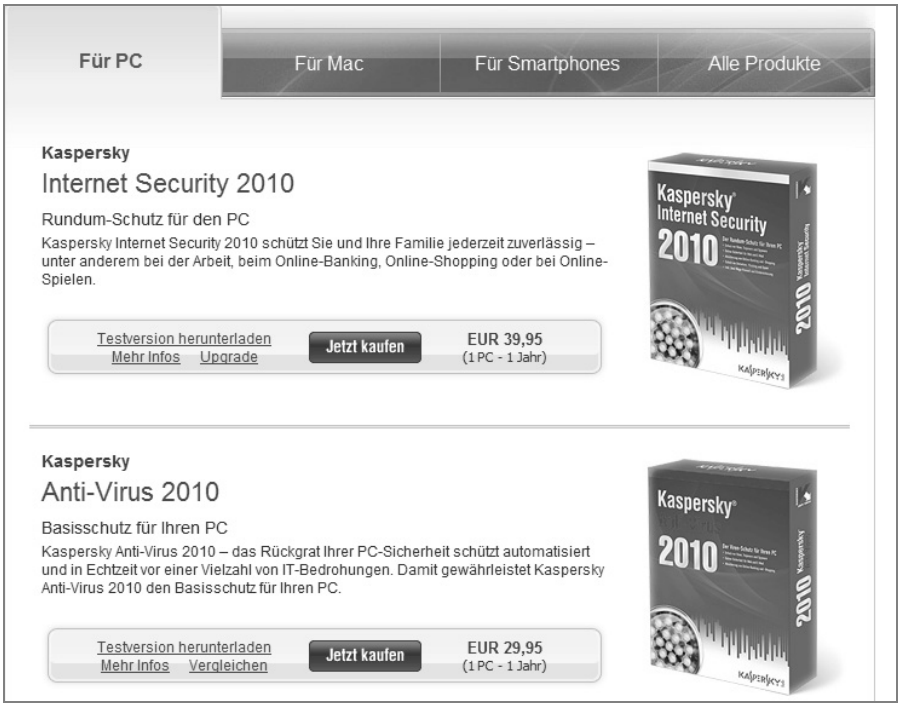


Bild 10.3: Der Funktionsumfang der Schutz-Software kann unterschiedlich groß sein.

Die Programme kosten je nach Funktionsumfang zumeist zwischen 25 und 50 EUR pro Jahr. Nach Ablauf dieser Zeit muss dann eine neue Programmversion oder ein Update erworben werden. Mitunter gibt es dieses Update zu einem etwas günstigeren Preis. Nur noch wenige Anbieter wie etwa Avira bieten auch Gratisversionen für Privatanwender an, allerdings fehlen bei diesen Versionen häufig wichtige Komponenten. Im Zweifelsfall sollten Sie die Ausgaben für ein Antiviren-Programm als wichtige Investition in die Sicherheit Ihres PCs hinnehmen, denn der Ärger und die Beeinträchtigungen oder sogar finanziellen Schäden durch einen erfolgreichen Angriff eines Schadprogramms sind deutlich schlimmer als diese Ausgaben.

Immerhin gibt es seit Vista mit dem Windows Defender bereits eine Software, die zumindest vor vielen Spyware-Programmen und ähnlichen Schadprogrammen schützt. Eine Antiviren-Lösung ersetzt der Windows Defender allerdings nicht.

Zusätzlicher Schutz durch die Firewall
Neben einen Antiviren-Programm kann auch eine (Personal) Firewall für mehr Sicherheit sorgen. Diese »Brandschutzmauer« stellt eine Barriere zwischen Ihrem PC und dem Internet dar und blockiert vor allem den direkten Zugriff von außen auf Ihren Rechner. In neueren Windows-Versionen (Windows 7, Vista, XP mit Service Pack 2) ist eine solche Firewall bereits enthalten und standardmäßig auch aktiviert. Eine zusätzliche Firewall auf dem Rechner wird daher zumeist nicht mehr benötigt.

Software aktualisieren

Neben der Nutzung eines Antiviren-Programms sollten Sie in jedem Fall dafür sorgen, dass die von Ihnen genutzten Programme immer auf dem neuesten Stand sind, denn immer wieder werden in allen möglichen Software-Produkten Schwachstellen entdeckt, durch die Schadsoftware auf Ihren PC gelangen kann.

Für das Windows-Betriebssystem inklusive der dazugehörigen Anwendungen wie dem Internet Explorer bietet Ihnen das automatische Windows-Update eine wichtige Hilfe. Ist diese Option aktiviert, werden alle wichtigen Aktualisierungen selbsttätig heruntergeladen und auch gleich installiert, sodass Sie sich hierüber keine weiteren Gedanken machen müssen.

Auch viele andere Programme, etwa Browser wie Firefox oder Opera, blenden mittlerweile automatisch eine Meldung ein, wenn aktuelle Sicherheitsupdates oder neue Programmversionen verfügbar sind. Allerdings müssen Sie hier zunächst noch dem Download und der Installation des Updates zustimmen.

Da aber auch z. B. Multimedia-Player oder andere Werkzeuge wie der Adobe Reader zum Anzeigen von PDF-Dateien, Schwachstellen besitzen können und daher aktualisiert werden müssen, gibt es zusätzliche Hilfsprogramme, mit denen Sie feststellen können, welche Programme auf Ihrem PC überhaupt installiert sind und ob diese auf dem jeweils aktuellen Stand sind. Zu diesen Programmen gehört etwa der Secunia Personal Software Inspector (www.secunia.com).

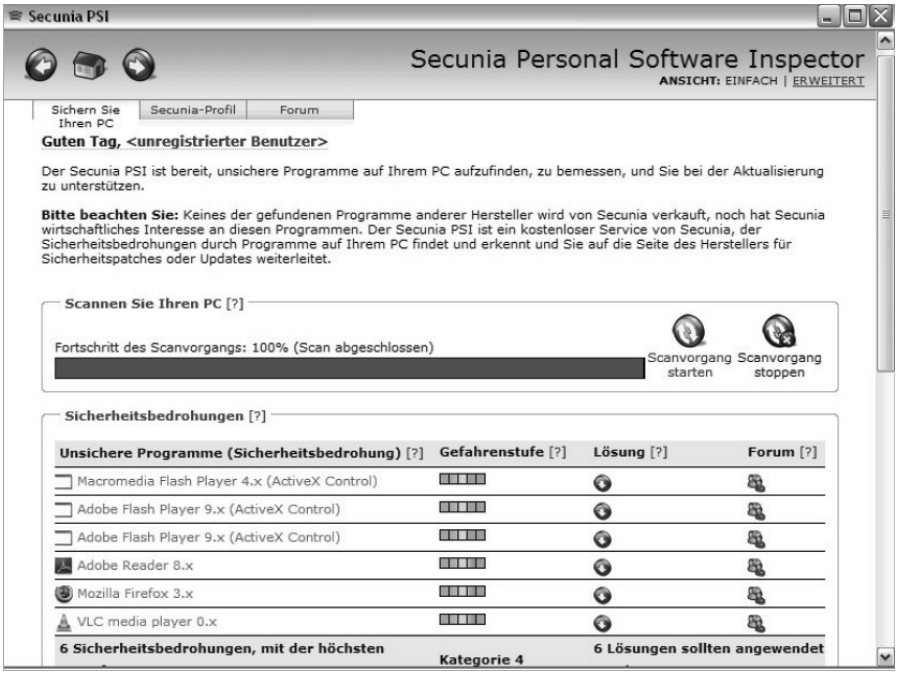


Bild 10.4: Mit dem kostenfrei erhältlichen *Personal Software Inspector* erhalten Sie einen Überblick über die Aktualität der vorhandenen Programme auf Ihrem PC.

Gerade angesichts der aktuellen Bedrohungen sollten Sie dafür sorgen, dass möglichst alle Anwendungen auf Ihrem PC aktuell sind und damit den bestmöglichen Schutz vor Angriffen bieten.

Nur notwendige Software installieren
Eine wichtige Schutzmaßnahme besteht auch darin, dass Sie auf Ihrem PC möglichst nur die Programme installiert haben, die Sie auch tatsächlich benötigen. Weniger ist auch in dieser Hinsicht mehr, wobei dieses »mehr« sich hier vor allem auf die Sicherheit bezieht. Denn mit jedem zusätzlichen Programm steigt ja auch das Risiko, dass hier entsprechende Schwachstellen vorhanden sind. Vor allem bei Programmen, die direkt Daten aus dem Internetöffnen bzw. wiedergeben, sollten Sie daher wirklich nur die unbedingt notwendigen Anwendungen installieren.

Vorsichtig sein

Der dritte wesentliche Baustein in jedem Schutzkonzept ist ein vorsichtiges Verhalten, denn blind verlassen dürfen Sie sich auf diese technischen Schutzkomponenten nicht. Wie schon erwähnt, können auch die aktuellsten Sicherheitsanwendungen keinen hundertprozentigen Schutz bieten und Sie sollten sich daher möglichst so umsichtig verhalten, dass erst gar keine Schadprogramme auf Ihren PC gelangen.

Dazu gehört primär ein vorsichtiger Umgang mit E-Mails. Seien Sie in jedem Fall skeptisch bei unverlangt zugesandten Dateianhängen und öffnen Sie derartige Anhänge im Zweifelsfall nicht. Ist Ihnen der Absender bekannt, fragen Sie gegebenenfalls nach, was es mit der E-Mail auf sich hat.

Ebenso sollten Sie nicht auf Links in verdächtigen E-Mails klicken, auch wenn das Ziel noch so verlockend scheint. Häufig werden Sie auf diese Weise auf Webseiten gelockt, die Schadprogramme in Umlauf bringen. Und wenn Ihr PC dann noch die entsprechenden Schwachstellen aufweist, ist die Infektion schnell passiert. Löschen Sie derartige unerwünschte E-Mails möglichst schnell.

Sicherheit für den Browser

Wie weiter oben bereits erwähnt, lauern Schadprogramme nicht mehr nur in E-Mail-Anhängen, sondern werden zunehmend auch über manipulierte Webseiten in Umlauf gebracht. Eine besondere Rolle dabei spielen bestimmte Webseiten-Elemente, durch die diese Übertragung erst möglich wird. Vor allem JavaScript erweist sich dabei als besonders heikel. Zwar lässt sich jeder Browser so einstellen, dass JavaScript nicht mehr ausgeführt wird, wodurch dann das Risiko weitgehend gebannt ist, allerdings führt dies dann dazu, dass sehr viele völlig harmlose Webangebote nicht mehr oder nur stark eingeschränkt nutzbar sind.

Einen guten Kompromiss bietet das Zusatzprogramm *NoScript*, das es jedoch nur für den *Firefox-Browser* gibt. Hier werden zunächst zwar auch die JavaScript-Elemente blockiert, jedoch kann man diese beim ersten Besuch einer Seite gezielt freigeben und der Browser merkt sich diese Einstellungen für künftige Aufrufe. Auf diese Weise lässt sich schnell und mit wenig Aufwand eine Liste mit den Webseiten erstellen, die solche Skripte ausführen dürfen, während man bei unbekannten Seiten besser geschützt bleibt.

Bild 10.5: Mit dem Firefox-Browser und der Erweiterung *NoScript* können Sie sich recht gut vor gefährlichen Webseiten schützen, ohne dass das Surfen zu unbequem wird.

10.3 Sicherheit auf einen Blick: Das Windows Wartungscenter

Die neueren Windows-Versionen sind bereits mit zahlreichen Komponenten ausgestattet, die zur Sicherheit bei der Internetnutzung beitragen. Dazu gehören etwa:

- Automatisches Windows Update
- Windows Firewall
- Windows Defender
- Benutzerkontensteuerung

Das automatische Windows Update sorgt dafür, dass alle wichtigen Updates, vor allem alle sicherheitsrelevanten Aktualisierungen für Windows automatisch übertragen und auch gleich installiert werden. Standardmäßig ist diese Funktion aktiviert, sodass Sie in aller Regel keine Änderungen vornehmen müssen.

Ähnliches gilt auch für die Windows-Firewall, um die Sie sich daher normalerweise auch nicht weiter kümmern müssen. In allen neueren Windows-Versionen (Vista, Windows 7) bietet die hier enthaltene Firewall einen ausreichenden Schutz und zusätzliche Programme dieser Art werden daher nicht mehr benötigt.

Der Windows Defender ist ein Schutzprogramm, das zusammen mit Windows ausgeliefert wird. Es arbeitet ähnlich wie ein konventionelles Antiviren-Programm, kann ein solches jedoch nicht vollständig ersetzen, da es nur bestimmte Arten von Schadprogrammen erkennen und beseitigen kann. Als Ergänzung zu einer anderen Antiviren-Lösung ist es jedoch sinnvoll.

Die Benutzerkontensteuerung schließlich sorgt dafür, dass sich Schadprogramme nicht unbemerkt vom Nutzer installieren können oder dass wichtige Einstellungen nicht heimlich von einer Software geändert werden können. Bei bestimmten Aktionen fragt Windows daher nach, ob sie tatsächlich ausgeführt werden sollen, oder ob der Vorgang abgebrochen werden soll. Auch dieses Element ist standardmäßig aktiviert und sollte nicht abgeschaltet werden, wenn auch die Rückfragen in einigen Situationen etwas nervig sein können.

Über das Wartungscenter in Windows 7 (bzw. das Sicherheitscenter in den Vorgängerversionen) können Sie sich auf einen Blick darüber informieren, ob diese Einstellungen tatsächlich so sind, wie sie eigentlich sein sollten.

Zum Aufruf des Wartungscenters klicken Sie auf das Symbol mit dem Fähnchen in der Windows-Taskleiste und dann den Link Wartungscenter öffnen.

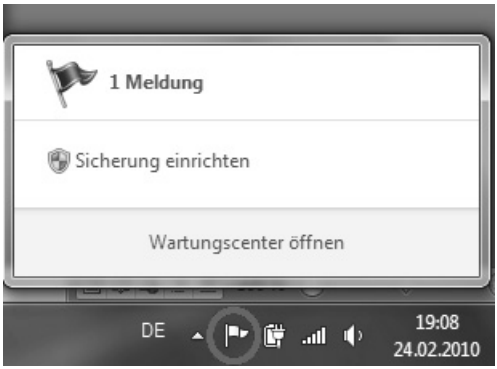


Bild 10.6: Über das Fähnchen-Symbol erreichen Sie das Wartungscenter.

Klicken Sie hier auf den Eintrag *Sicherheit* und in der aufklappenden Liste sehen Sie, welche sicherheitsrelevanten Einstellungen auf Ihrem Rechner aktiv sind. Werden mangelhafte Einstellungen festgestellt, etwa ein fehlendes oder nicht mehr aktuelles Antiviren-Programm oder ein abgeschaltetes Windows Update, meldet das Wartungscenter Ihnen dies explizit und macht Sie auf den Handlungsbedarf aufmerksam. Dabei werden auch konkrete Hinweise gegeben, wie Sie den Mangel abstellen können.

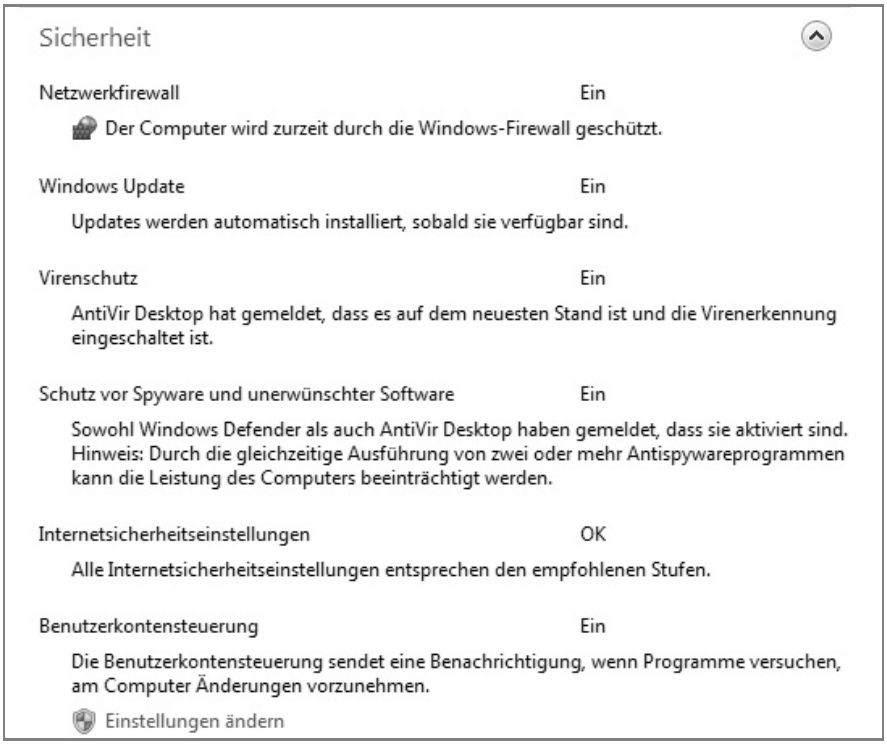


Bild 10.7: Im Idealfall sind alle wichtigen Sicherheitsvorkehrungen getroffen.

Keine hundertprozentige Sicherheit
Auch wenn Sie alle notwendigen Sicherheitsvorkehrungen auf Ihrem Rechner getroffen haben, können Sie sich niemals hundertprozentig sicher fühlen. Eine absolute Sicherheit gibt es weder im echten Leben noch in den elektronischen Welten. Sie sollten daher stets wachsam bleiben und vor allem unnötige Risiken vermeiden, indem Sie etwa unerwünschte E-Mail-Anhänge niemals einfach so öffnen, nur weil Sie sich auf Ihr Antiviren-Programm verlassen. Auch beim Surfen im Web oder der Verwendung sonstiger Datenträger sollten Sie vorsichtig bleiben, um Schadprogrammen möglichst keine Chance zu geben.

Die verschiedenen Sicherheitskomponenten können Sie auch einzeln direkt aus der Systemsteuerung heraus aufrufen, sich über deren Status informieren und gegebenenfalls Änderungen der Einstellungen vornehmen. Neben den in Windows eingebauten Vorkehrungen wie der Windows Firewall, dem Windows-Update oder dem Windows Defender trägt sich üblicherweise auch jede Antiviren-Software in die Systemsteuerung ein und kann dann hierüber erreicht werden.

Windows Defender

Für den Windows Defender können Sie beispielsweise festlegen, wie oft und zu welchen Zeitpunkten er automatisch eine Überprüfung des Rechners vornehmen soll. Dazu klicken Sie z. B. in der Systemsteuerung (Symbolansicht) den Eintrag *Windows Defender* an.

Anschließend klicken Sie im Programmfenster auf den Eintrag *Extras* und dann auf den Link *Optionen*. Hier haben Sie dann die Möglichkeit ein bestimmtes Intervall für die Überprüfungen vorzugeben (z. B. täglich oder jeweils an einem bestimmten Wochentag), die Uhrzeit für die Durchführung sowie die Art (Schnellüberprüfung oder die aufwendigere aber genauere vollständige Überprüfung) festzulegen. Am sinnvollsten ist es, diese Tests in solche Zeiten zu verlegen, in denen Sie den Rechner nicht gerade für wichtige Aufgaben benötigen, denn die Überprüfungen beanspruchen etliche Ressourcen. Voreingestellt ist hier daher die Option, dass die Überprüfungen nur dann durchgeführt werden, wenn der Rechner sich im Leerlauf befindet.

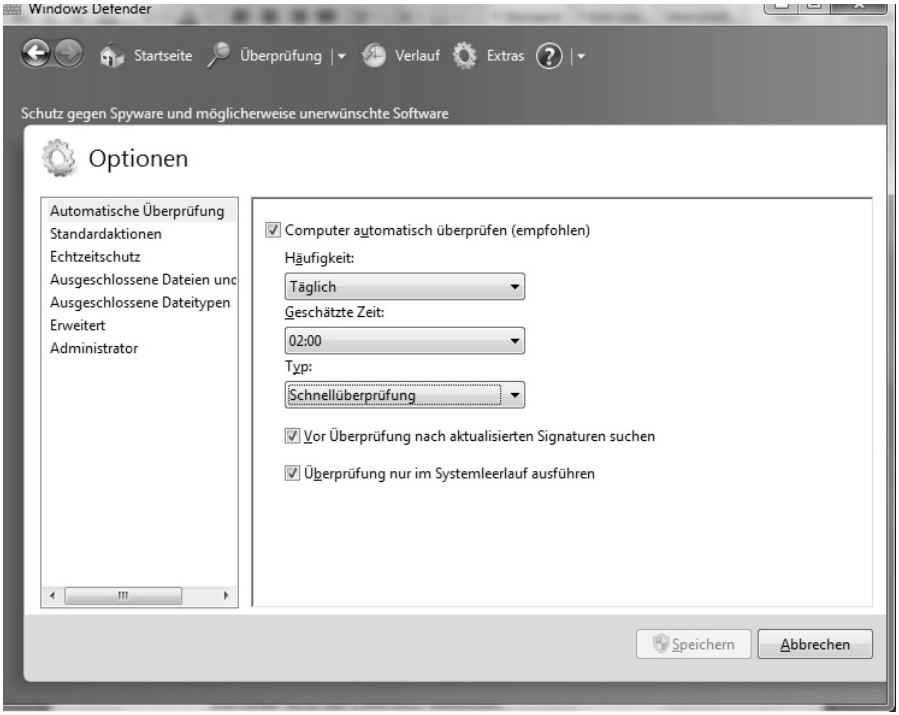


Bild 10.8: Legen Sie fest, wann Windows Defender die Überprüfungen durchführen soll.

Klicken Sie im Programmfenster des Windows Defenders auf die Schaltfläche *Überprüfung* startet ein solcher Test unmittelbar, wobei standardmäßig die Schnellüberprüfung durchgeführt wird. Wollen Sie die vollständige Überprüfung direkt starten, klicken Sie auf die kleine Schaltfläche neben dem Eintrag und wählen Sie diese Option dann aus.

Auch das Antiviren-Programm konfigurieren
Üblicherweise sind die Antiviren-Programme so eingestellt, dass sie gleich nach der Installation alle Dateizugriffe überwachen und bei verdächtigen Dateien sofort Alarm schlagen, um eine Infektion zu verhindern. Ähnlich wie den Windows Defender sollten Sie das Antiviren-Programm jedoch auch so konfigurieren, dass regelmäßig eine gründliche Überprüfung aller Dateien auf dem Rechner erfolgt. Starten Sie dazu das Schutzprogramm auf Ihrem PC und treffen Sie diese Einstellungen.

10.4 Vorsicht Falle: Betrügereien im Web

Neben den Angriffen durch Schadsoftware aller Art lauern im Internet noch einige andere Gefahrenquellen. Weit verbreitet sind etwa die sogenannten Abo-Fallen, bei denen bestimmte Dienste wie etwa Kochrezepte, persönliche Horoskope, Gesundheitsberatung, Gratis-SMS, Software-Downloads, Bewerbungs- oder Hausaufgabenhilfen angeboten werden.

Die Nutzer werden animiert, diese Dienste auszuprobieren, wozu zunächst jedoch eine anscheinend unverbindliche Registrierung verbunden ist. Wer hier dann seine persönlichen Daten eingibt, schließt dann häufig zugleich ein kostenpflichtiges Abonnement ab, für das meist Gebühren von rund 5 bis 15 Euro im Monat in Rechnung gestellt werden. Zudem wird gleich eine Mindestvertragslaufzeit von 12 oder gar 24 vereinbart, sodass eine erkleckliche Summe zustande kommt.

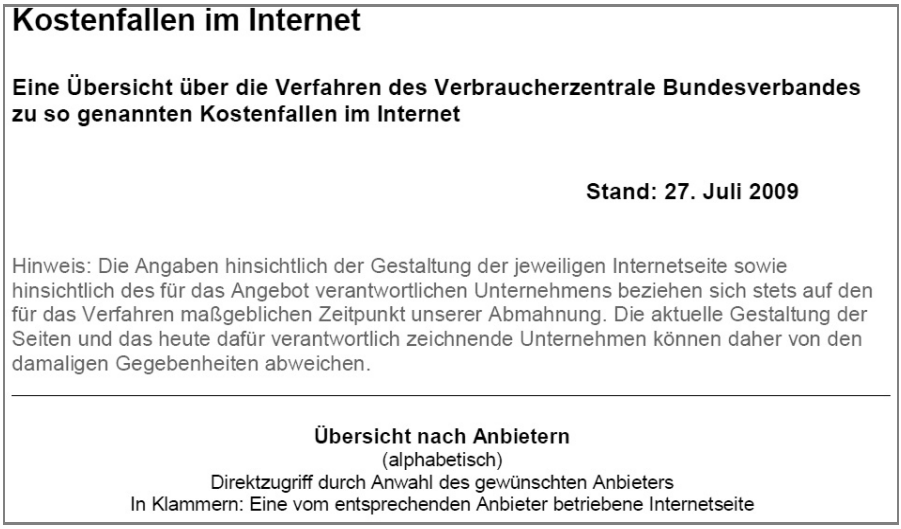
Bild 10.9: Die vorgeschriebenen Hinweise auf den Abschluss eines kostenpflichtiges Abonnements sind auf den Abofallen-Seiten nur schwer zu entdecken.

Die gesetzlich vorgeschriebenen Hinweise, dass mit der Registrierung zugleich ein kostenpflichtiges Abonnement abgeschlossen wird, sind auf den Webseiten nur sehr schwer zu finden, sodass gerade unerfahrene Internetnutzer immer wieder auf derartige Angebote hereinfallen, zumal es ähnliche Inhalte im Internet auf sehr vielen Seiten tatsächlich völlig gratis gibt.

Nach einiger Zeit bekommen die Nutzer dann die Rechnungen per Post oder per E-Mail und bei Nichtbezahlung bauen diese Anbieter dann eine Drohkulisse auf und kündigen Klagen oder eine Benachrichtigung der Schufa etc. an. Viele Kunden lassen sich von diesen Ankündigungen einschüchtern und zahlen den meist ja noch verkraftbaren Betrag, um dann ihre Ruhe zu haben.

Allerdings haben Sie als Opfer einer solchen Kostenfalle durchaus gute Chancen, auch ohne Zahlung des Abo-Preises davon zu kommen. Denn in den meisten Fällen verstoßen die Anbieter mit diesen Diensten gleich gegen mehrere gesetzliche Vorgaben und werden daher den Gang vor ein Gericht scheuen. Zudem gehen seit einiger Zeit auch Verbraucherschützer aktiv gegen diese dubiosen Anbieter vor und strengen ihrerseits Klagen an.

Eine umfangreiche Liste mit solchen zweifelhaften Angeboten finden Sie auch auf den Webseiten des Bundesverbands der Verbraucherschutzzentralen (*www.vzbv.de/mediapics/kostenfallen_im_internet.pdf*).



Kostenfallen im Internet

Eine Übersicht über die Verfahren des Verbraucherzentrale Bundesverbandes zu so genannten Kostenfallen im Internet

Stand: 27. Juli 2009

Hinweis: Die Angaben hinsichtlich der Gestaltung der jeweiligen Internetseite sowie hinsichtlich des für das Angebot verantwortlichen Unternehmens beziehen sich stets auf den für das Verfahren maßgeblichen Zeitpunkt unserer Abmahnung. Die aktuelle Gestaltung der Seiten und das heute dafür verantwortlich zeichnende Unternehmen können daher von den damaligen Gegebenheiten abweichen.

Übersicht nach Anbietern
(alphabetisch)
Direktzugriff durch Anwahl des gewünschten Anbieters
In Klammern: Eine vom entsprechenden Anbieter betriebene Internetseite

Bild 10.10: Die Verbraucherzentralen führen eine Liste mit bekannten Abo-Fallen.

Um derartige Ärgernisse jedoch von vornherein zu vermeiden, sollten Sie vor der Teilnahme an Aktionen bzw. der Registrierung bei Internet-Diensten aller Art stets die genauen Vertragsbedingungen und AGBs durchlesen, die auf den Seiten angegeben sein müssen. Im Zweifelsfall sollten Sie dann eher auf die Angebote verzichten und ihr Glück auf anderen Webseiten suchen.

Komplizen gesucht

Skeptisch bleiben sollten Sie in jedem Fall auch bei unerwarteten Job-Angeboten, die Ihnen per E-Mail zugestellt werden. Hier beschreiben die vermeintlichen Arbeitgeber häufig sehr professionell eine scheinbar überaus attraktive und dazu lukrative Tätigkeit, mit der Sie mit vergleichsweise wenig Anstrengungen gutes Geld verdienen können.

Letztlich geht es bei diesen Angeboten immer darum, dass Sie Ihr Girokonto zur Verfügung stellen sollen, auf das Geldbeträge eingezahlt werden, die sie dann nach Abzug einer recht verlockenden Provision weiterüberweisen sollen. Meist soll dieser Transfer über Dienste wie Western Union ins Ausland erfolgen.

In keinem Fall sollten Sie auf ein derartiges Angebot reagieren, denn wenn Sie tatsächlich in dieser Art tätig werden, bekommen Sie sehr bald Schwierigkeiten mit Polizei und Staatsanwaltschaft, denn Sie machen sich hierbei des Vergehens der Geldwäsche schuldig. Hinter diesen Angeboten stehen professionelle Phishing-Ganoven, die ergaunerte Bankzugangsdaten verwenden, um Geld von den Konten ihrer Opfer abzuheben. Um dabei keine Spuren zu hinterlassen und weniger Verdacht zu erregen, bedienen die Betrüger sich auf diese Weise teilweise ahnungsloser Mittäter, die ihr Konto zur Verfügung stellen.

Jobangebot:

Wir bieten Ihnen einfache Arbeit an, die keine spezielle Fertigkeiten und keine Geldanlagen verlangt. Sie können diese Arbeit mit Ihrer Hauptarbeit vereinbaren. **Mit uns können Sie leicht 5000-6000 Euro pro Monat verdienen, dabei brauchen Sie für diese Arbeit 2-3 Stunden pro Tag 1-2 Mal pro Woche.**

Kurze Beschreibung der Tätigkeit:
Ihre Aufgabe ist, Geldüberweisungen auf Ihr Konto zu erhalten, das Geld in bar abzuheben und abzüglich Ihrer Provision unserem Agent per System der Bargeldüberweisungen Western Union oder Money Gram zu überweisen. **Gewöhnlich überweisen wir auf Ihr Konto 4000-6000 Euro. Ihre Provision wird 20 % (20 Prozenten) von jeder Geldüberweisung ausmachen. Ihre Provision (20 Prozenten) bekommen Sie, sofort nach dem Geldeingang auf Ihr Konto. Auf diese Weise wenn Sie 6000 Euro auf Ihr Konto erhalten, verdienen Sie 1200 Euro.** Sie können Ihre Provision gleich abheben oder auf dem Konto lassen. Die restliche Summe 4800 Euro sollen Sie am Tag des Geldeingangs in bar abheben und unserem Agent per Western Union oder Money Gram überweisen (Gebühr für Überweisung bezahlen wir). Zeitaufwand für diese ganze Arbeit beträgt nicht mehr als 3 Stunden. **Wenn Sie 2 Überweisungen pro Woche erhalten werden, können Sie nicht weniger als 6000 Euro von jedem Konto pro Monat verdienen.**

Diese Tätigkeit abweichend von den meisten Angeboten, die Sie per e-Mail bekommen, verletzt nicht Gesetze von BRD. Es gibt überhaupt kein Risiko für Sie. Sie werden keinen Verdacht bei der Bank und bei der Steuerbehörde erregen, wenn Sie 1-2 Geldüberweisungen pro Woche auf jedes von Ihren Konten bekommen werden.

Bild 10.11: Angebote wie diese sollten Sie ignorieren und die E-Mails am besten gleich entsorgen.

Falscher Virenalarm

Noch eine weitere ziemlich üble Betrugsmasche ist seit einiger Zeit vergleichsweise populär geworden. Hierbei wird beim Besuch von Webseiten auf einmal ein gefälschter Virenalarm eingeblendet und der Surfer aufgefordert, eine spezielle Software zum Entfernen dieses Schadprogramms herunterzuladen bzw. die Schädlinge direkt zu entfernen. Bei einer Variante dieser Betrügereien enthält dann allerdings erst die heruntergeladene vermeintliche Sicherheitssoftware die Schadkom-

ponente, die dann etwa Daten ausspioniert oder andere Schäden anrichtet. Fachleute bezeichnen diese gefälschten Viren-Meldungen auch als Scareware.

Bei der zweiten Variante müssen Sie die angebotene Schutzsoftware zum Entfernen des vermeintlichen Schädlings käuflich erwerben. Hier zahlen Sie dann für eine absolut wirkungslose Software, die eine nur erfundene Bedrohung auf Ihrem Notebook beseitigt. In jedem Fall sollten Sie daher nur auf solche Warnhinweise reagieren, die tatsächlich vom Antiviren-Programm auf Ihrem PC stammen.

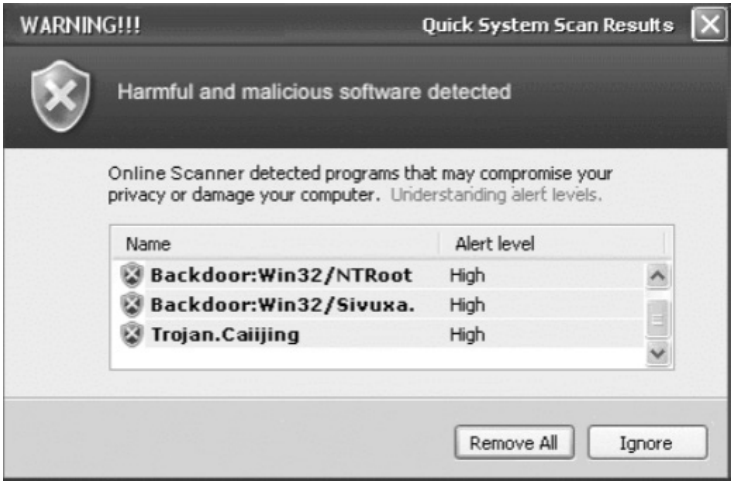


Bild 10.12: Gefälschte Viren-Hinweise sollen entweder zum Kauf nutzloser Schutzsoftware animieren oder erst den Download einer echten Schadsoftware bezwecken.

S Stichwortverzeichnis

Thomas Schirmer / Andreas Hein

Internet-Praxisbuch

Anschließen · Absichern · Losurfen

Keine Angst vor dem Internet! In diesem Internet-Praxisbuch nehmen wir Sie an die Hand, wir zeigen Ihnen, wie Sie eine Verbindung ins Internet aufbauen und wie Sie sich mit dem Internet Explorer sicher darin bewegen. Sie werden im Internet bequem einkaufen und Ihren nächsten Urlaub buchen. Sie werden Bankgeschäfte erledigen und sich so manchen Gang zu Ämtern und Behörden sparen. Gerade dabei darf die Sicherheit natürlich nicht zu kurz kommen – wir zeigen Ihnen, worauf es ankommt!

- **Die ersten Onlineschritte**
  Die Autoren stellen das wichtigste Internetprogramm vor, den Browser. Wenn Sie ihn beherrschen, beherrschen Sie das Internet. Neben der reinen Browserbedienung widmen wir uns auch den Suchmaschinen, wie zum Beispiel Google.
- **E-Mail-Einführung**
  POP, IMAP oder doch gleich Exchange? Welches Mailsystem passt am besten zu Ihnen, und wo erhalten Sie überhaupt eine eigene E-Mail-Adresse? Hier steht's.
- **Einkaufen im Internet**
  Keine Frage, das Onlineshoppen ist erwachsen geworden. Es ist nicht nur bequem, sondern bietet auch handfeste Vorteile: ein gesetzlich verbrieftes Rückgaberecht zum Beispiel. Probieren Sie es aus!
- **Freunde und Hobbys im Internet**
  Facebook, Twitter, StayFriends & Co. haben es gezeigt: Das Internet ist durchaus sozial und hat nichts mehr mit verstaubten Hinterzimmern zu tun. Werden Sie ein Teil der Web-2.0-Community.
- **Sicheres Internetbanking**
  Überweisungen am Bankschalter sind mittlerweile teurer als Onlineüberweisungen – ganz abgesehen vom Komfortvorteil der Onlinevariante. Wir zeigen ganz klar den Nutzen und das Risiko, Sie haben dann die Wahl!
- **Das Internet als Reisebüro**
  Die meisten Suchanfragen im Internet beziehen sich auf Reiseangebote. Wir zeigen, wie Sie das günstigste Angebot zu Ihrem Traumurlaub finden – von der Flugbuchung bis zu realistischen Fotos vom geplanten Urlaubsort.
- **Onlinegefahren**
  Wir wollen es nicht verschweigen: Das Internet hat seine Unschuld verloren und bietet Platz für Kriminelle. Man muss wissen, was man im Internet tut – hier erfahren Sie es!

Aus dem Inhalt:

9 783645 600484

10,– EUR [D]
ISBN 978-3-645-60048-4