eload24

Windows 7: Programme und Daten absichern

Mirko Müller

Klicken, Lesen, Weitermachen. So einfach geht das.

Rubrik	**Betriebssysteme**
Thema	**Windows**
Umfang	**43 Seiten**
eBook	**01032**
Autor	**Mirko Müller**

Sicherheit ist bei Windows 7 ein großes Thema. Schließlich geht es um Ihre Programme und Daten. Damit kein Unbefugter an die Daten herankommt, ist Windows 7 mit einer Fülle von Sicherheitsfunktionen ausgestattet, an denen sich Hacker und Eindringline die Zähne ausbeißen.

Windows 7: Programme und Daten absichern

Mirko Müller

eload24 AG
Sonnenhof 3
CH-8808 Pfäffikon SZ

info@eload24.com
www.eload24.com

Inhalt

Windows 7: Programme und Daten absichern 3
Die Sicherheitsfeatures im Überblick 3
Das Wartungscenter von Windows 7 5
Sicherheit hinter der Firewall 7
Automatische Updates sorgen für Sicherheit 15
Keine Chance für Spyware, Malware und andere Schädlinge 19
Internetsicherheit inklusive Schutz vor Phishing, Datenklau und gefährlichen Downloads 24
Die Benutzerkontensteuerung 28
Sicher arbeiten als Standardbenutzer 33
Was noch fehlt: der Schutz vor Viren 40

Windows 7: Programme und Daten absichern

Sicherheit ist bei Windows 7 ein großes Thema. Schließlich geht es um Ihre Programme und Daten. Damit kein Unbefugter an die Daten herankommt, ist Windows 7 mit einer Fülle von Sicherheitsfunktionen ausgestattet, an denen sich Hacker und Eindringline die Zähne ausbeißen. Dieses eBook zeigt Ihnen, über welche Sicherheitsfunktionen bei Windows 7 zur Standardausstattung gehören und wie Sie sie richtig konfigurieren. Aber auch, welche Sicherheitsfeatures fehlen und unbedingt nachgerüstet werden sollten. Nach der Lektüre des eBooks und der Umsetzung der Tipps ist Ihr PC mit Windows 7 eine gehörige Portion sicherer.

Die Sicherheitsfeatures im Überblick

Dass Windows 7 das Thema Sicherheit ernst nimmt, sieht man sofort an der Fülle von neuen oder im Vergleich zu vorherigen Windows-Versionen kräftig überarbeiteten Sicherheitsmechanismen. Die sieben wichtigsten Sicherheitstools von Windows 7 sind:

- Das Wartungscenter: Das Wartungscenter von Windows 7 ist die zentrale Anlaufstelle für alle Fragen und Einstellungen rund um das Thema Sicherheit und Systemwartung.
- Automatische Updates: Dank automatischer Updates bleibt Windows stets auf dem Laufenden und erhält automatisch und ohne Ihr Zutun immer die neuesten Updates und Aktualisierungen.
- Windows-Firewall: Kein Computer sollte ohne Firewall ins Internet. Bei Windows

7 ist bereits von Hause aus eine solche „Feuerschutzwand" integriert.

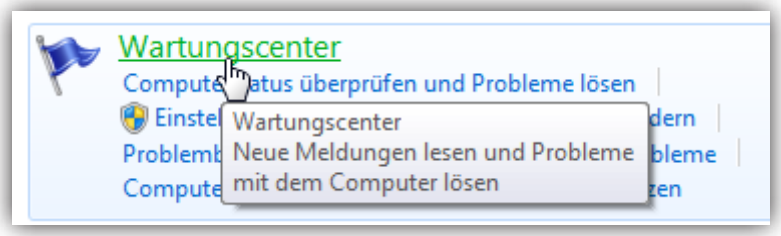
- Benutzerkonten: Jeder Windows-Benutzer bekommt ein sogenanntes Standardbenutzerkonto. Das ist mit weniger Rechten ausgestattet und schützt den PC so vor versehentlichen oder mutwilligen Eingriffen.
- Benutzerkontensteuerung: Windows 7 achtet genau darauf, wer was auf dem Rechner macht. Sollte ein Programm versuchen, heimlich Systemänderungen vorzunehmen oder Hackertools zu installieren, greift die Benutzerkontensteuerung ein und blendet eine Warnung ein. Unabsichtliche oder böswillige Veränderungen am System werden so verhindert.
- Windows Defender: Der Defender (zu deutsch: Verteidiger) schützt Sie vor Eindringlingen wie Trojanern oder Spyware.
- Internetsicherheit: Der Internet Explorer arbeitet standardmäßig im geschützten Modus. Daten anderer Benutzer oder wichtige Systemeinstellungen bleiben so vor manipulierten Webseiten geschützt. Der SmartScreen-Filter bewahrt Sie vor schädlichen Downloads oder dem Ausspionieren von Kennwörtern oder PIN- und TAN-Nummern.

Alle Sicherheitsmechanismen arbeiten Hand in Hand. Wobei gilt: Je mehr der von Windows angebotenen Sicherheitstools Sie benutzen, umso sicherer ist das gesamte System. Auf den nachfolgenden Seiten erfahren Sie, wie die einzelnen Mechanismen funktionieren und wie Sie sie optimal einstellen. Mit dem Ziel, den Computer so sicher wie möglich zu machen.

Das Wartungscenter von Windows 7

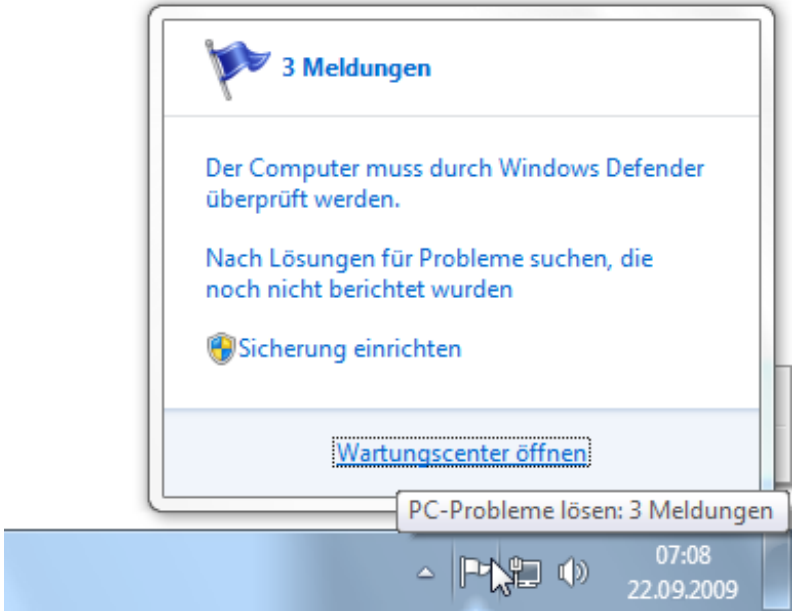
Zentrale Anlaufstelle für alle Sicherheitsfragen ist das Wartungscenter. Hier laufen alle Fäden zum Absichern des eigenen PCs zusammen. Sie erreichen das Wartungscenter folgendermaßen:

1. Klicken Sie das Start-Symbol, und rufen Sie den Befehl Systemsteuerung auf.

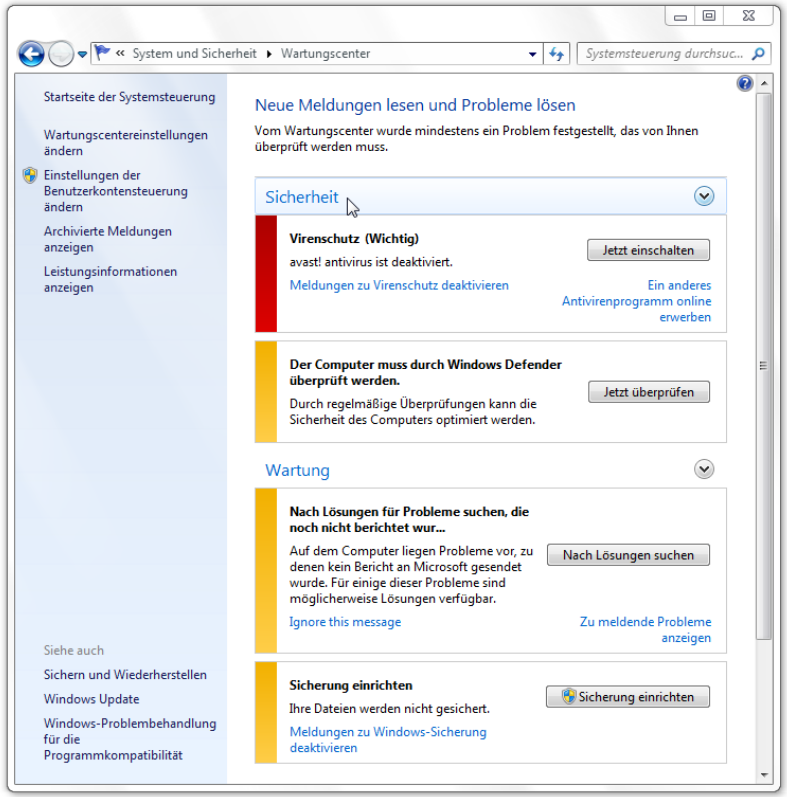


2. Klicken Sie auf Sicherheit und anschließend auf Wartungscenter.

Sollte Windows feststellen, dass mit Ihrem PC eventuell ein Sicherheitsproblem besteht, erscheint in der rechten unteren Ecke der Tastleiste – links neben der Uhr – ein kleines Fähnchen. In diesem Fall können Sie auch hierüber das Wartungscenter erreichen. Ein Klick darauf zeigt eine Übersicht aller aktuellen Probleme und Empfehlungen; mit Wartungscenter öffnen gelangen Sie direkt ins Sicherheitscenter.



Wenn auf Ihrem PC das Fähnchen in der Taskleiste erscheint, hat das zumeist eine Ursache: Windows stört sich daran, dass auf Ihrem PC keine Antivirensoftware installiert ist. Da Windows von Hause aus ohne Antivirenlösung ausgeliefert wird, erscheint das Fähnchen praktisch bei jedem neuen PC. Die Installation einer Antivirensoftware ist für jeden PC ratsam. Mehr hierzu erfahren Sie weiter unten im Abschnitt Was noch fehlt: Der Schutz vor Viren.



Im Windows-Wartungscenter erfahren Sie, welche Schutzmechanismen aktiviert sind – und wo es eventuell Probleme gibt.

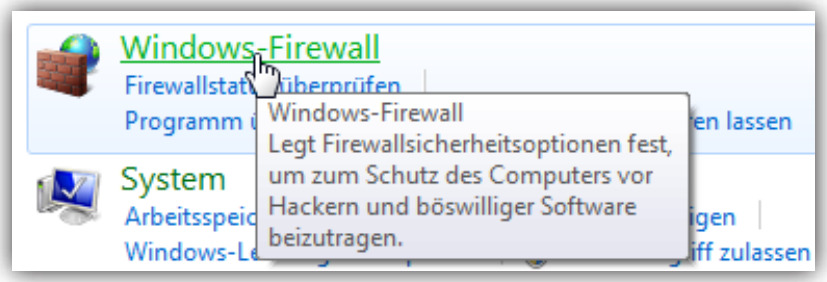
Sicherheit hinter der Firewall

Ohne Firewall mit einem PC zu arbeiten ist wie Autofahren ohne Sicherheitsgurt: Die Fahrt kann durchaus gut gehen – im Falle eines Falles endet die Reise aber mit bösen Verletzungen. Mit „Reise" ist beim PC das Surfen durch das Internet gemeint. Wer hier ohne Firewall unterwegs ist, fängt sich schneller als gedacht einen Virus, Trojaner oder ähnlich gemeine digitale Schädlinge ein.

Die Firewall arbeitet wie ein Türwächter. Bevor ein Datenpaket – zum Beispiel eine Webseite – Ihren PC „betreten" darf, wird es gründlich untersucht. Geprüft wird vor allem, ob sich nicht heimlich ein Stück schädliche Software in den PC mogeln möchte, beispielsweise Würmer. Nur wenn die Firewall grünes Licht gibt, wird das Datenpaket durchgelassen. Das passiert im Hintergrund so schnell, dass Sie von den regelmäßigen Prüfvorgängen nichts mitbekommen.

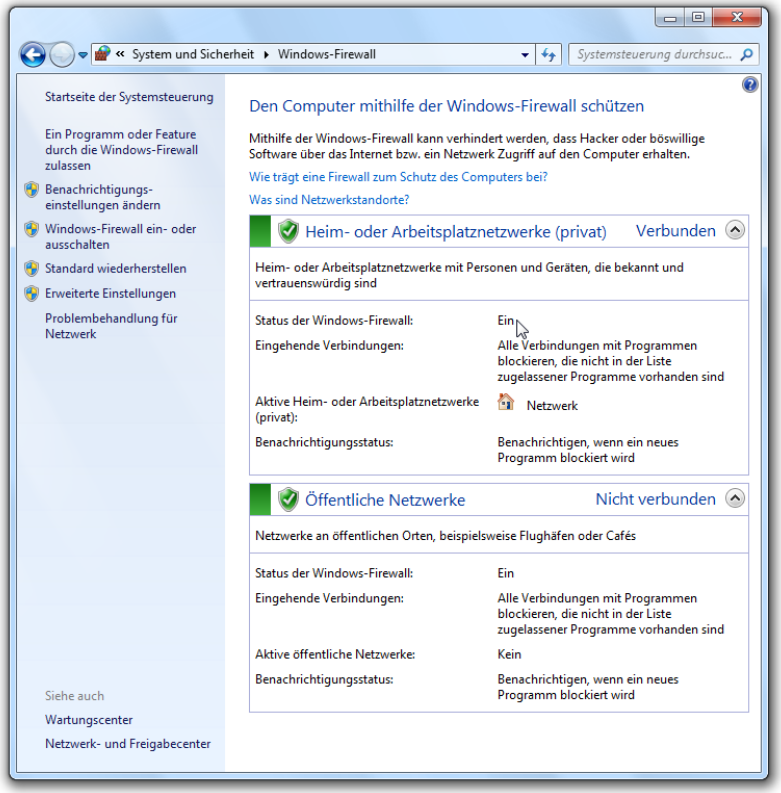
Jeder PC sollte über eine Firewall verfügen – die auch eingeschaltet ist. Bei Windows ist von Hause aus eine eigene Firewall mit an Bord. Ob sie aktiv ist, können Sie leicht in der Systemsteuerung überprüfen:

1. Öffnen Sie die Systemsteuerung mit dem Befehl Start | Systemsteuerung.



2. Klicken Sie auf System und Sicherheit sowie auf Windows-Firewall.
3. Im folgenden Fenster erfahren Sie sowohl für Heim- und Arbeitsplatznetzwer-

ke (das eigene Netzwerk zuhause) als auch für öffentliche Netzwerke (bei Verbindungen über öffentliche WLAN-Hotspots), ob die Firewall richtig konfiguriert ist. Wenn in der Zeile Status der Windows-Firewall die Meldung Ein steht, ist alles in Ordnung. Die Firewall von Windows ist aktiviert und überwacht den ein- und ausgehenden Datenverkehr.

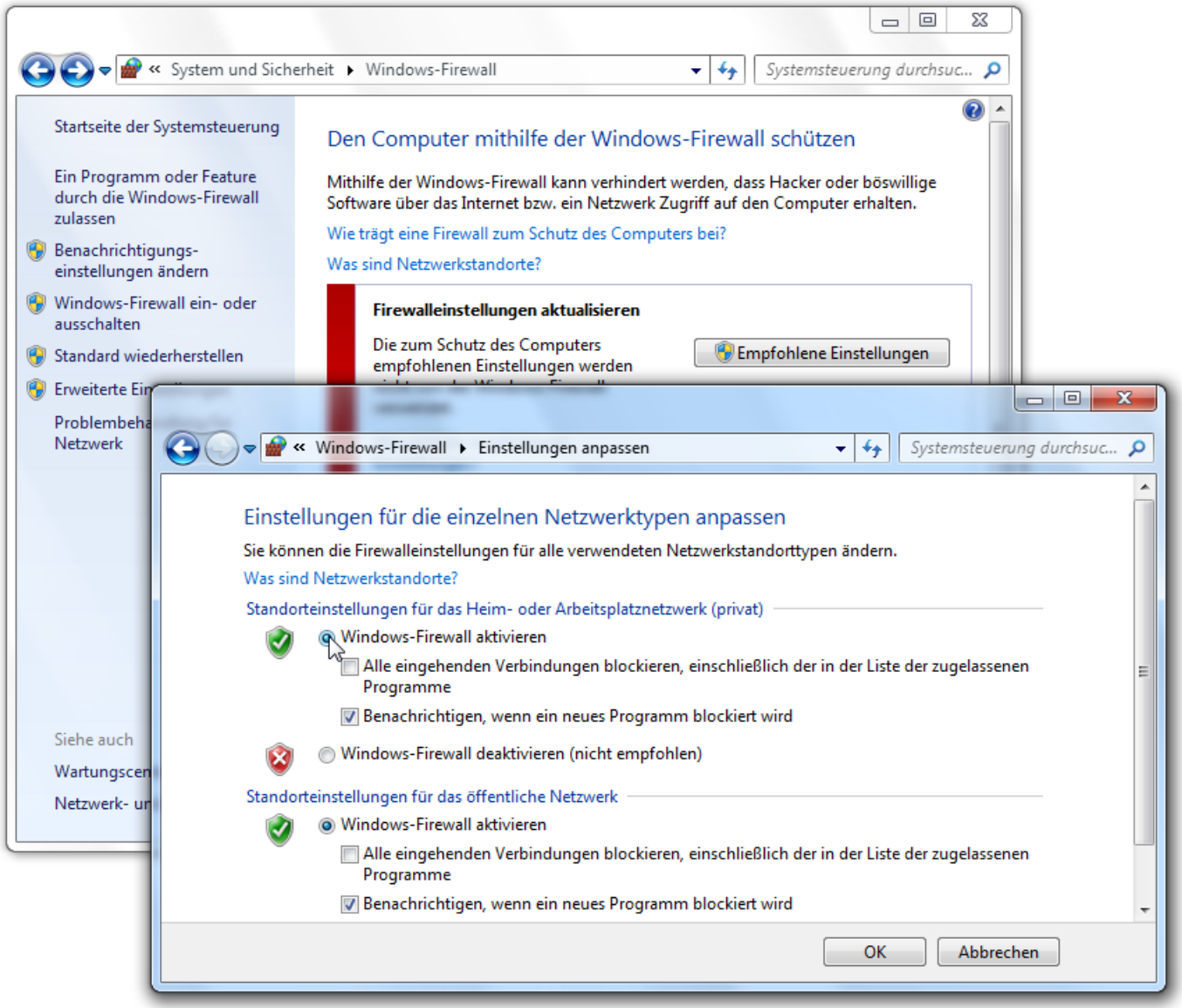


So sind Sie optimal geschützt: Die Firewall ist aktiv und überwacht den gesamten Datenverkehr.

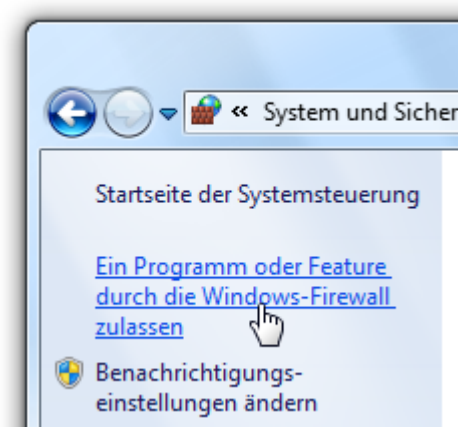
4. Sollte die Firewall ausgeschaltet sein, ist der Rechner gegen Angriffe aus dem Internet ungeschützt. In diesem Fall sollten Sie den Firewall-Schutz wieder aktivieren, indem Sie auf Windows-Firewall ein- oder ausschalten klicken und bei beiden Standorten die Option Windows-Firewall aktivieren einschalten.

Gezielt Programme durch die Firewall lassen

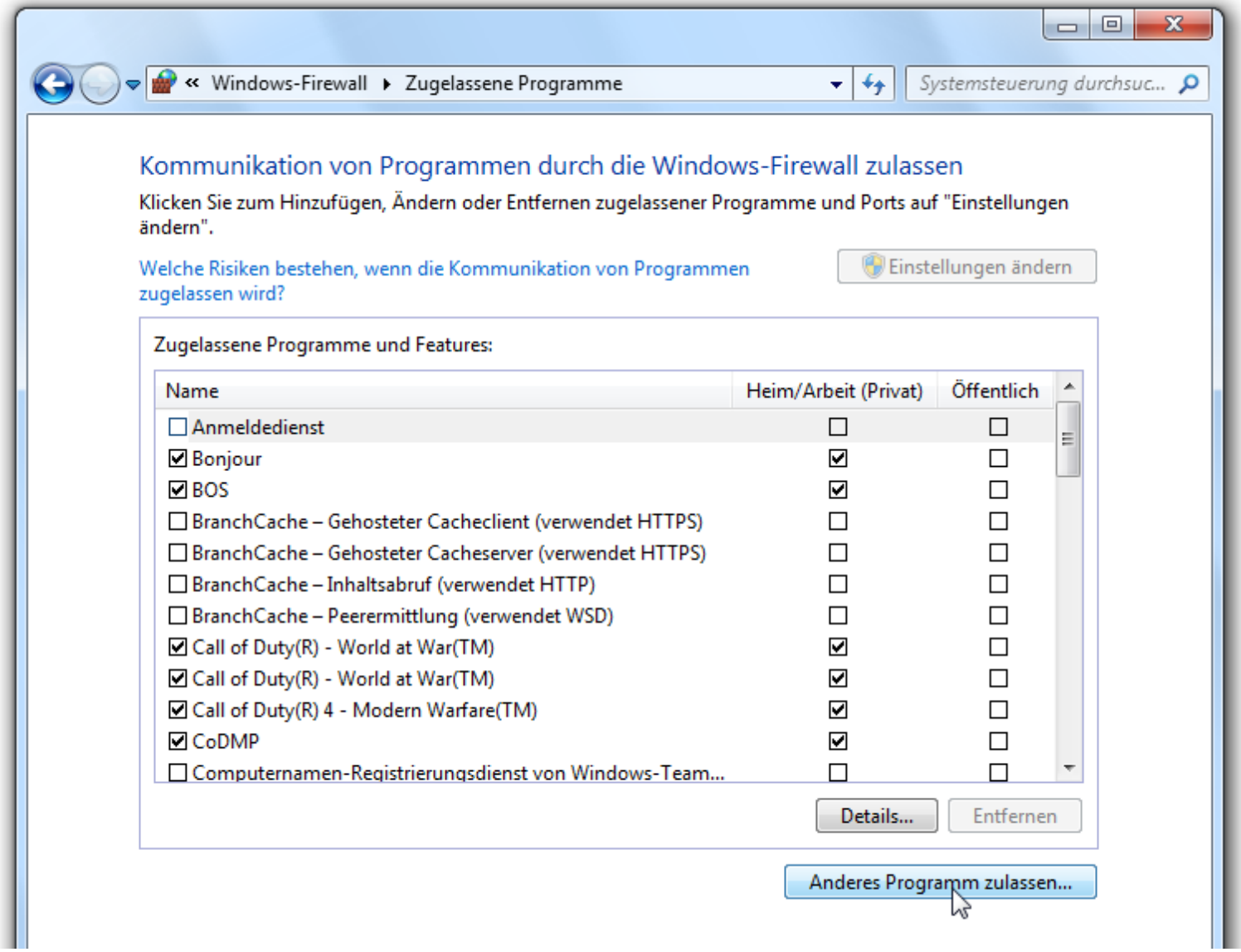
Normalerweise reichen die Standardeinstellungen für einen wirksamen Schutz vollkommen aus. Alle anderen Einstellungen können Sie zunächst unverändert lassen. Nur wenn



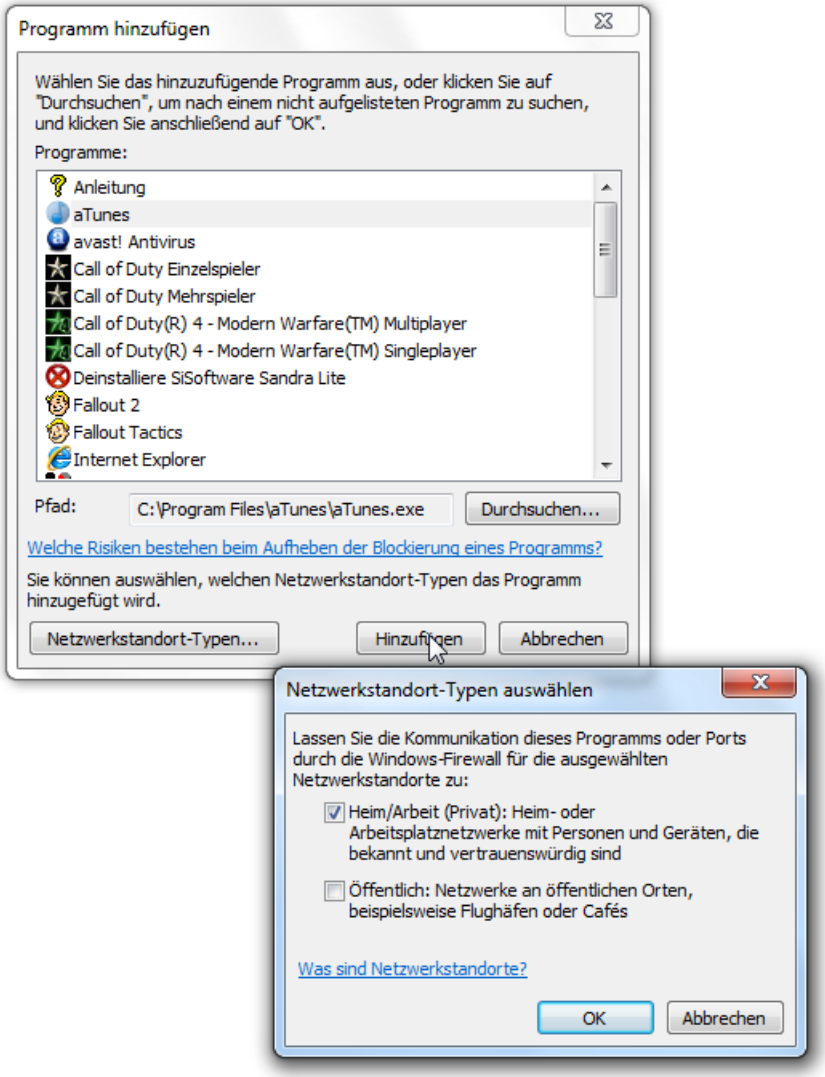
es mit einem neu installierten Programm Probleme gibt und sich damit keine Internetverbindung aufbauen lässt, müssen Sie eingreifen. Dann können Sie das Programm zur Ausnahmenliste hinzufügen und bestimmten Anwendungen den Zugriff aufs Internet gewähren. Programme auf der Ausnahmeliste erhalten eine Sondergenehmigung, um an der Firewall vorbei zu kommen. Setzen Sie diesen Notlösung aber nur sparsam und nur für Programme ein, denen Sie vertrauen:



1. Um bestimmte Programme durch die Firewall zu lassen, klicken Sie in der linken Spalte der Systemsteuerungskomponente Windows-Firewall auf Ein Programm oder Feature durch die Windows-Firewall zulassen.
2. Auf der nächsten Seite sind alle derzeit gültigen Firewall-Regeln aufgeführt. Sie erkennen, welche Programme und Funktionen als sicher eingestuft werden und die Firewall passieren dürfen. Um manuell ein weiteres Programm zu ergänzen, klicken Sie auf Einstellungen ändern und dann auf Anderes Programm zulassen.



3. Im nächsten Fenster sind all derzeit installieren Programme aufgeführt. Wählen Sie das gewünschte Programm aus, und klicken Sie auf Hinzufügen. Über die Schaltfläche Netzwerkstandort-Typen können Sie zusätzlich festlegen, für welche Netzwerkvariante (Heimnetzwerk und/oder öffentliches Netzwerk) die Regel gelten soll.
4. Das Programm erscheint daraufhin in der Liste der zugelassenen Anwendungen. Über die Schaltfläche Details blenden Sie weitere Informationen ein; mit Entfernen entziehen Sie dem Programm die Erlaubnis, durch die Firewall zu kommunizieren.

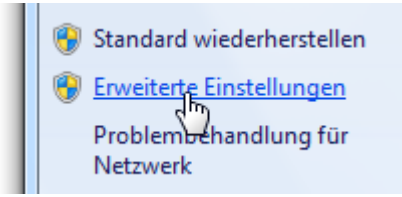


Die Sondergenehmigung können Sie auch dann erteilen, wenn die Firewall eine Software beim unerlaubten Zugriff erwischt. Wenn Sie beispielsweise ein neues FTP-Programm installieren, das die Firewall noch

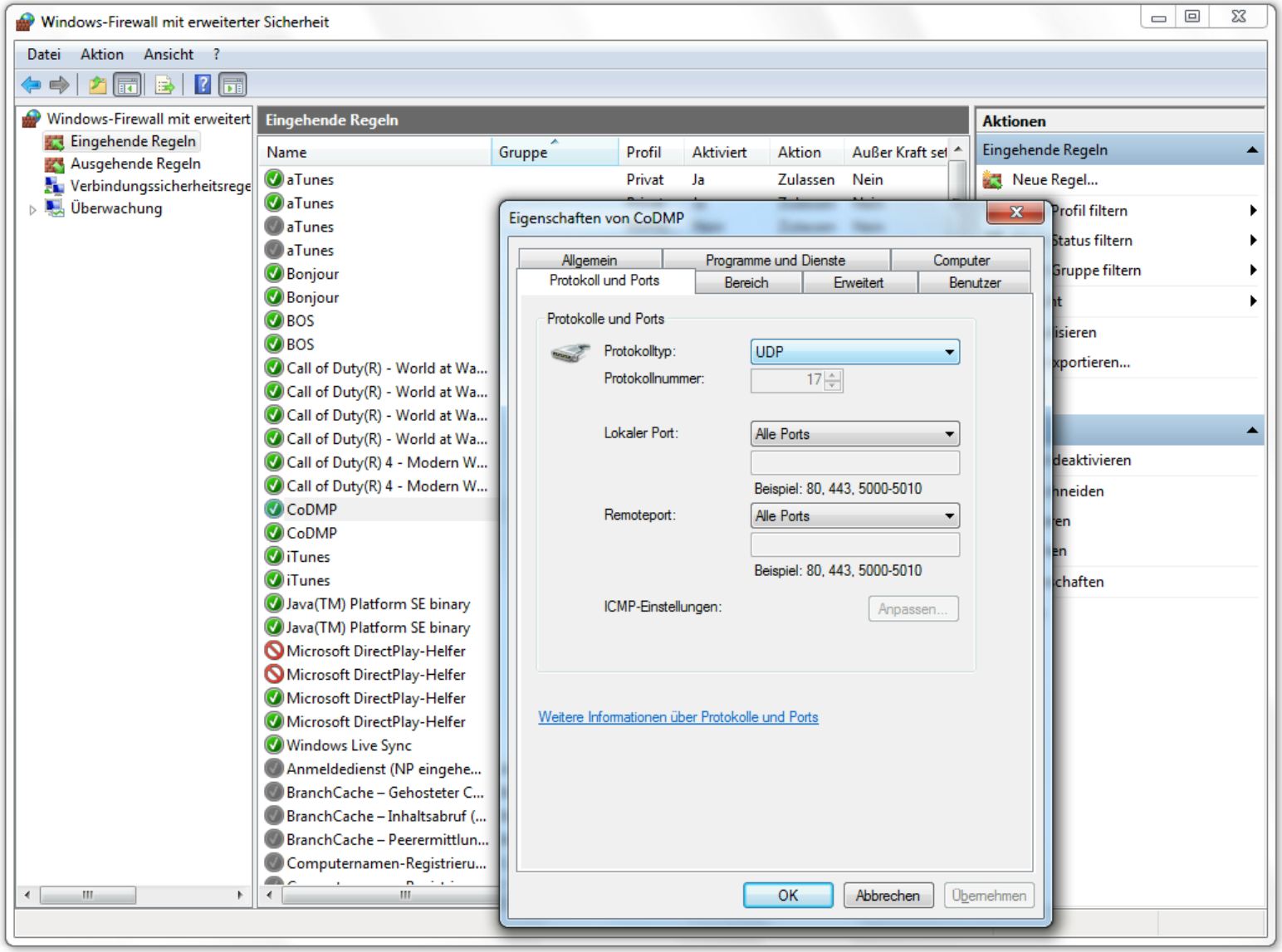
nicht kennt, erscheint ein Warnhinweis. Die Windows-Firewall macht Sie darauf aufmerksam, dass ein neues Programm versucht, an der Firewall vorbei zu kommen. Das ist ein gutes Zeichen – es zeigt, dass die Firewall funktioniert und nicht einfach jeden Zugriff auf das Internet zulässt.

Firewall-Einstellungen für Profis

Einmal eingeschaltet, sorgt die Windows-Firewall automatisch für einen optimalen Schutz vor Angriffen. Dank der einfachen Bedienung kommen auch Laien mit der Firewall schnell zurecht. Für Profis gibt es einen erweiterten Modus, mit dem sie die Firewalleinstellungen bis ins kleinste Detail ändern können.



1. Den Profi-Modus erreichen Sie per Klick auf Erweiterte Einstellungen.
2. Im folgenden Fenster sind alle Regeln für den ein- und ausgehenden Datenverkehr aufgeführt. Um weitere Details einzublenden, klicken Sie zum Beispiel auf Eingehende Regeln und dann doppelt auf einen Programmeintrag.
3. Im nächsten Fenster finden Sie die Details der Firewallregel. Änderungen sollten hier nur Windows-Anwender vornehmen, die Erfahrungen mit Fachbegriffen wie Ports und Protokollen haben.
4. Im Register Protokoll und Ports können Sie beispielsweise festlegen, durch welche Ports (Schnittstellen) das Programm kommunizieren darf. Das ist für einige Onlinespiele oder Chatprogramme wichtig, die nur funktionieren, wenn bestimmte Ports und Protokolle in der Firewall freigegeben sind. Welche das sind,



erfahren Sie meist auf den Support-Seiten des Programmanbieters.

5. Falls Sie nur einen Blick in die Regel werfen, aber nichts verändern möchten, sollten Sie das Dialogfenster mit Abbrechen wieder verlassen. Um die Änderungen zu übernehmen, klicken Sie auf OK.

Alternative Schutzprogramme

Es muss nicht immer die Windows-Firewall sein. Sie können auch eine andere Firewall-Software einsetzen, zum Beispiel das kostenlose Schutzprogramm Zone-Alarm Free Firewall (http://www.zonelabs.com). Windows erkennt automatisch, dass Sie eine eigene Firewall-Lösung einsetzen und schaltet die Windows-Firewall aus. Im Zweifelsfall entscheiden Sie im Wartungscenter einfach selbst, welcher Firewall Sie den Vorzug geben.

Automatische Updates sorgen für Sicherheit

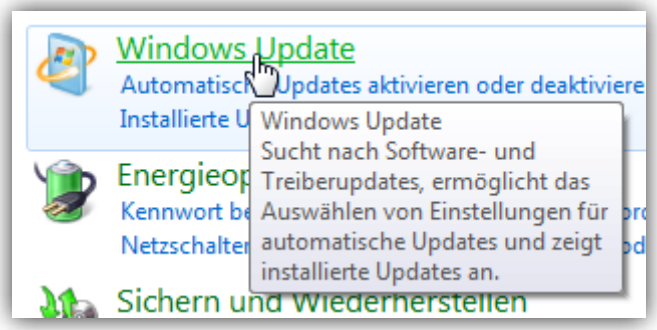
Ist mein PC sicher? Sind alle Sicherheitsupdates installiert? Diese und ähnliche Fragen stellen sich viele PC-Benutzer. Insbesondere, wenn in Fachzeitschriften oder Radio und Fernsehen über neue Sicherheitslöcher berichtet wird. Damit die Fragen gar nicht erst aufkommen, hat Windows ein nützliches Werkzeug an Bord: das automatische Update.

Wie der Name bereits verrät, heilt sich Windows 7 damit selbst. Es überprüft automatisch, ob es zurzeit neue Aktualisierungen oder Verbesserungen für das Betriebssystem gibt, und installiert diese von alleine. Windows bleibt so stets auf dem neuesten Stand. Das ist ungefähr so praktisch, als würde Ihr Auto selbständig zu Inspektionen und TÜV-Untersuchungen fahren und sich ohne Ihr Zu-

tun selbst reparieren oder neue Reifen und Bremsen einbauen.

Daher gilt für jeden Windows-PC: Die automatische Update-Funktion sollte auf jeden Fall eingeschaltet sein. Nur so stellen Sie sicher, dass Ihnen kein Sicherheitsupdate entgeht und Ihr PC bestmöglich vor Angriffen geschützt ist. Ob auf Ihrem PC das automatische Update aktiviert ist, können Sie selbst überprüfen:

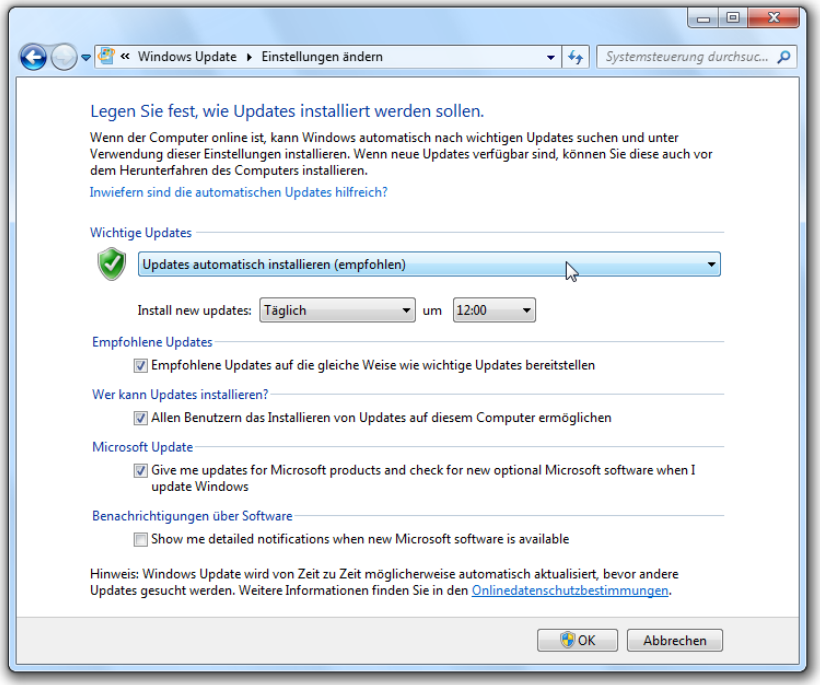
1. Klicken Sie auf das Start-Symbol, und rufen Sie den Befehl Systemsteuerung auf.



2. Klicken Sie auf System und Sicherheit und dann auf Windows Update.
3. Anschließend klicken Sie auf Einstellungen ändern.
4. Um alle verfügbaren Updates für Windows 7 automatisch herunterzuladen und zu installieren, sollte die Option Updates automatisch installieren (empfohlen) aktiviert sein. Damit können Sie – bildlich gesprochen – die Füße hochlegen und müssen nur noch darauf warten, dass Windows von den Microsoft-Servern automatisch die aktuellsten Sicherungen herunterlädt und installiert.
5. Wann genau Windows nachschauen soll, bestimmen Sie in den Feldern für den Tag und die Uhrzeit. Idealerweise wählen Sie einen Zeitpunkt, an dem der Computer eingeschaltet ist, aber nur wenig benutzt wird. Falls der Computer zum gewählten Zeitpunkt nicht eingeschaltet

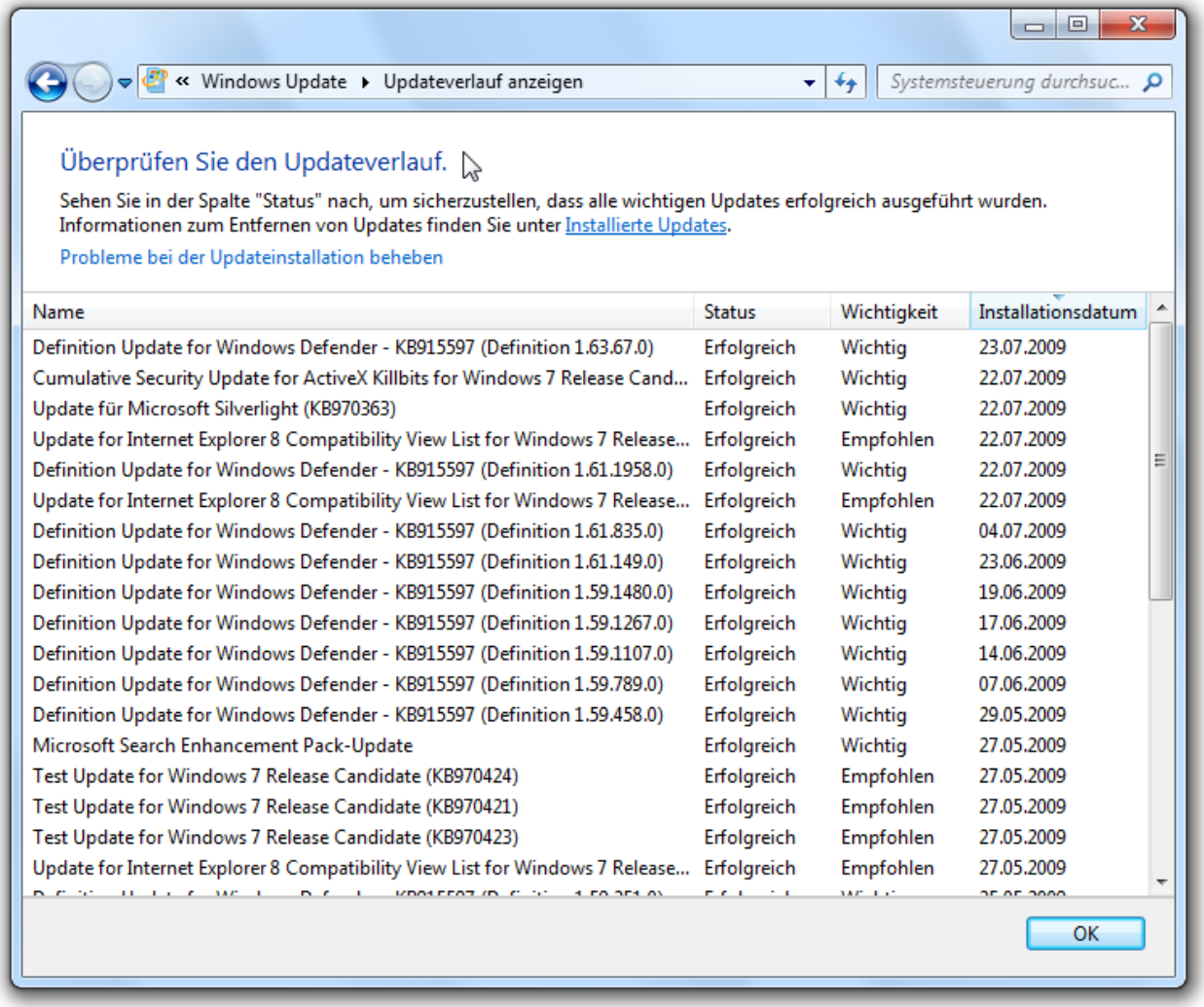
sein soll, ist das nicht weiter tragisch. Beim nächsten Einschalten holt Windows die „versäumten" Updatezeiten nach.

6. Ebenfalls empfehlenswert: Kreuzen Sie das Kontrollkästchen Empfohlene Updates an, um nicht nur die sicherheitsrelevanten, sondern auch alle von Microsoft empfohlenen Aktualisierungen zu installieren. Meist handelt es sich um neue oder verbesserte Windows-Funktionen.
7. Um die Änderungen zu übernehmen, schließen Sie das Fenster mit OK.



So sollte die Update-Funktion konfiguriert sein, damit Windows 7 immer auf dem neuesten Stand bleibt.

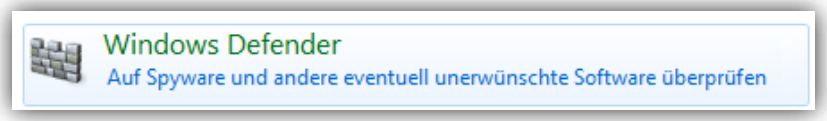
Auf Wunsch können Sie genau nachverfolgen, wann Windows welche Updates installiert hat. Klicken Sie hierzu auf Updateverlauf anzeigen. Im nachfolgenden Fenster erscheint das „Logbuch" der Update-Funktion. Jedes Update ist mit Datum und Grad der Wichtigkeit aufgeführt.



Im Updateverlauf verrät Windows, wann welches Update installiert wurde.

Keine Chance für Spyware, Malware und andere Schädlinge

Ein großes Ärgernis ist sogenannte Malware – frei übersetzt: Schad-Software. Weit verbreitet sind zum Beispiel Spyware-Spionageprogramme. Das Ärgerliche: Zahlreiche Freeware- und Shareware-Programme installieren still und heimlich SpyWare auf Ihrem PC. Der Name ist gut gewählt: Wie ein feindlicher Spion nistet sich die SpyWare heimlich im PC ein und spioniert Sie aus: Welche Programme Sie wann aufrufen, zu welchem Zeitpunkt Sie ins Internet gehen oder welche Webseiten Sie besuchen. Die Informationen übermittelt die SpyWare dann unbemerkt im Hintergrund an ihre Programmierer. Das ist nicht nur störend und lästig, sondern macht Ihren PC auch noch langsamer. Schlimmstenfalls spioniert der Eindringling sogar Kennwörter oder PIN- und TAN-Nummern aus.



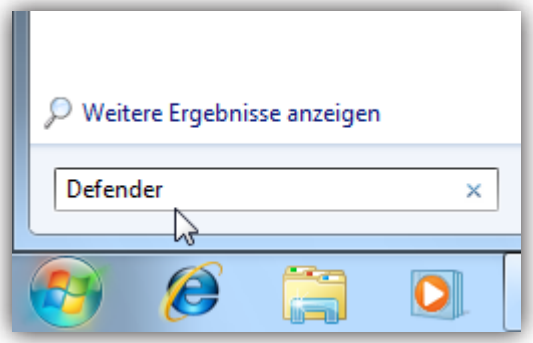
Mit dem in Windows 7 integrierten Anti-Spyware-Tool namens Windows Defender geht es SpyWare und anderen Schädlingen an den Kragen. Windows Defender durchforstet im Hintergrund alle Festplattenlaufwerke – auch USB-Sticks, Digitalkameras und andere Wechseldatenträger – nach verdächtigen Programmen. Auch der Arbeitsspeicher und die Registrierdatenbank von Windows werden laufend gründlich durchleuchtet. Wird Windows Defender fündig, schlägt es Alarm, und Sie können auf Knopfdruck die schädliche Software wieder loswerden.

Das Schöne an Windows Defender: Sie müssen nichts tun. Das Tool wird beim Windows-Start aktiviert und überwacht Ihren Computer automatisch. Eine gute Maßnahme, um Spy-

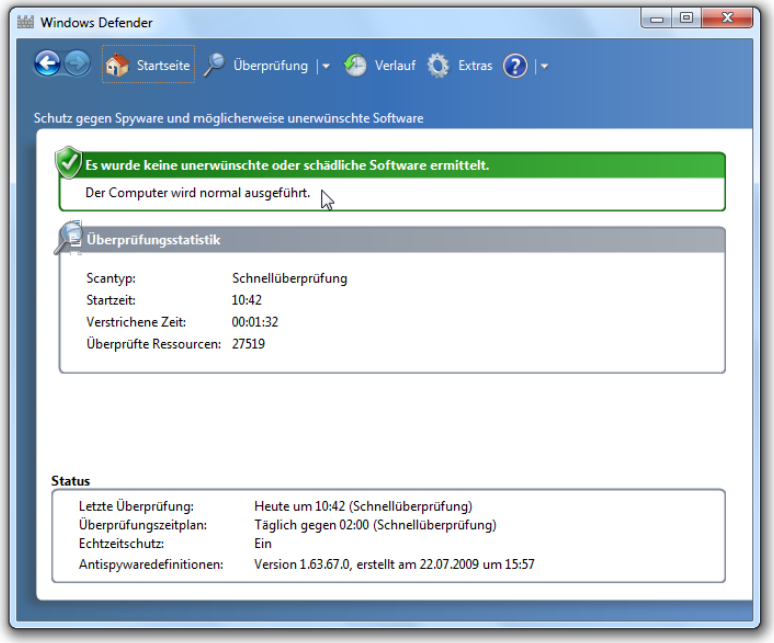
ware und andere Schädlinge erst gar nicht rein zu lassen.

Windows Defender konfigurieren

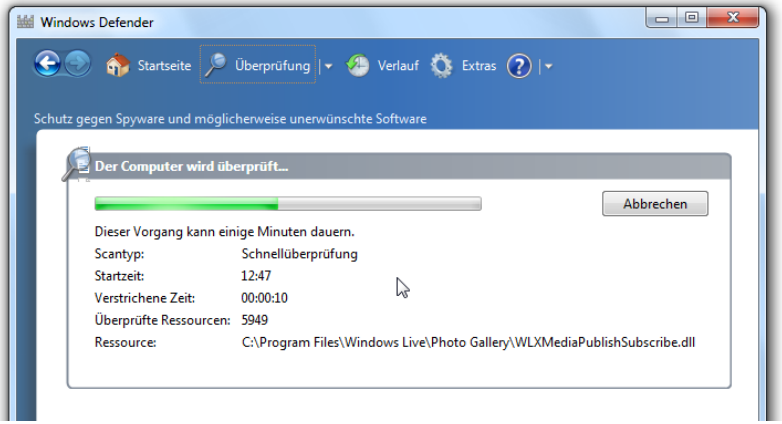
Eigentlich müssen Sie sich um Windows Defender nicht weiter kümmern. Es bleibt unauffällig im Hintergrund und wacht darüber, dass keine schädliche Software eindringt. Auf Wunsch können Sie Defender unter die Motorhaube schauen und genau festlegen, wie weit der Schutz gehen soll:



1. Klicken Sie auf das Start-Symbol und geben Sie in das Suchfeld Defender ein.
2. Anschließend klicken Sie in der Startmenüliste auf Windows Defender.
3. Im nachfolgenden Fenster berichtet Defender über den aktuellen Stand an der „Front". Ist alles in Ordnung, erscheint in grüner Schrift die Meldung Es wurde keine unerwünschte oder schädliche Software ermittelt sowie Der Computer wird normal ausgeführt.

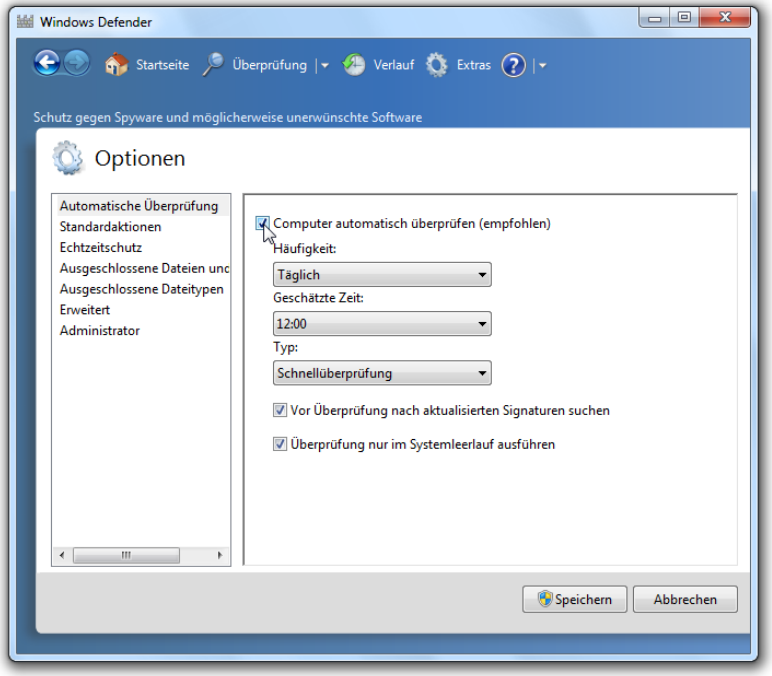


4. Wer möchte, kann Windows Defender noch einmal auf die Suche nach verdächtiger Software schicken. Klicken Sie hierzu auf Jetzt überprüfen. Windows Defender legt dann eine Extraschicht ein und untersucht noch einmal das Betriebssystem selbst und alle Festplatten. Das dauert in der Regel nur wenige Minuten.



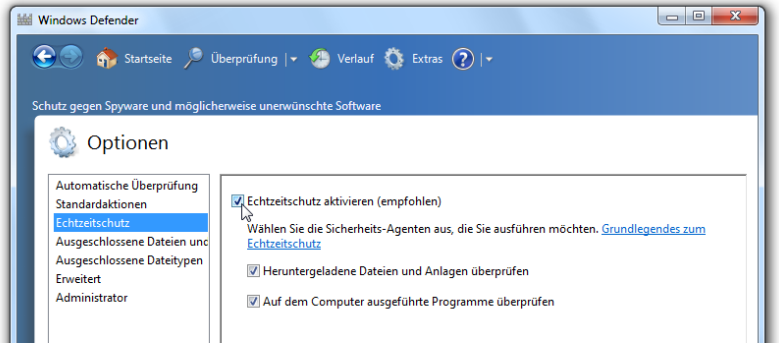
5. Wenn Sie wissen möchten, was Windows Defender in den letzten Tagen gefunden hat, klicken Sie auf Verlauf. Hier sehen Sie genau, wann Defender welche Aktionen durchgeführt hat.

6. Um festzulegen, wann und wie intensiv Windows Defender Ausschau halten soll, genügt ein Mausklick auf Extras sowie Optionen. Im nachfolgenden Dialogfenster bestimmen Sie, ob und wann



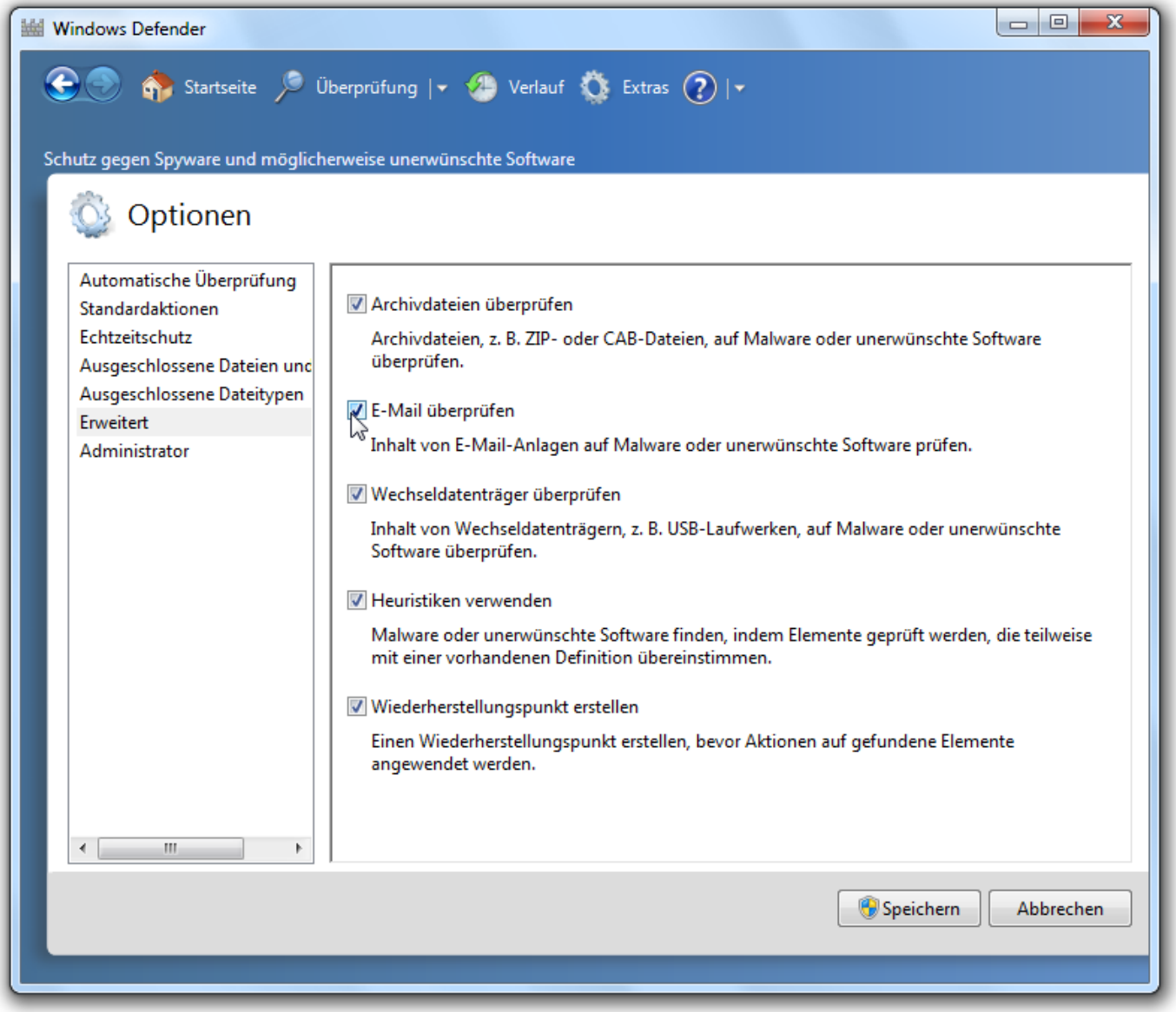
Windows Defender den Computer untersuchen soll. Optimal ist eine täglich stattfindende automatische Überprüfung vom Typ Schnellüberprüfung.

7. Damit Ihr Computer optimal geschützt ist, sollte im Bereich Echtzeitschutz das Kontrollkästchen Echtzeitschutz aktivieren eingeschaltet sein. Dann hat Defender nicht nur zu den zuvor festgelegten Prüfzeitpunkten, sondern praktisch rund um die Uhr ein Auge auf Ihren Computer. Das Tool überprüft dann jede Aktivität am PC: das Ändern von Systemkonfigurationen, das Herunterladen von Dateien oder das Installieren und Starten von Programmen. Kommt Windows Defender zum Beispiel beim Starten eines heruntergeladenen Programms etwas verdächtig vor, schlägt es sofort Alarm und lässt den Start erst gar nicht zu.



Wie genau Windows Defender den PC überwacht, können Sie selbst bestimmen. Wichtig ist der Echtzeitschutz, der rund um die Uhr für Sicherheit sorgt.

8. Ebenfalls empfehlenswert: Aktivieren Sie im Bereich Erweitert die Kontrollkästchen E-Mail überprüfen sowie Wechseldatenträger überprüfen, damit Windows Defender auch ein Auge auf den E-Mail-Verkehr und angestöpselte USB-Laufwerke sowie Speicherkarten wirft.
9. Schließen Sie das Fenster per Klick auf Speichern.



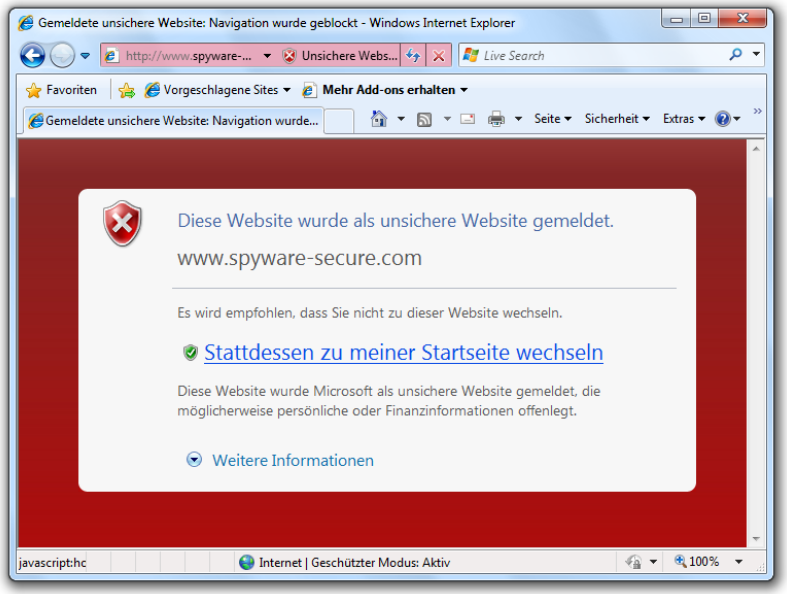
Internetsicherheit inklusive Schutz vor Phishing, Datenklau und gefährlichen Downloads

Ganz schön gemein: Findige Hacker schaffen es immer wieder, durch gefälschte E-Mails und Webseiten sensible Daten wie Kennwörter oder PIN und TAN fürs Homebanking zu ergaunern. Mit wenigen Mausklicks ist man die die Falle getappt. Die Gauner verschicken E-Mails, die exakt genau so aussehen wie z.B. E-Mails Ihrer Hausbank. Sogar als Absender erscheint die Hausbank. Alles gefälscht. Sowohl der Absender als auch der Inhalt sind falsch. Wer den manipulierten Link in der Mail anklickt, landet dann aber nicht bei der Hausbank, sondern bei der manipulierten Webseite des Angreifers – die natürlich so aussieht wie die der Bank. Wer jetzt leichtgläubig seine PIN und TAN eingibt, ist in die Falle getappt. Fachleute sprechen hier vom Phishing, dem Fischen nach persönlichen Informationen.

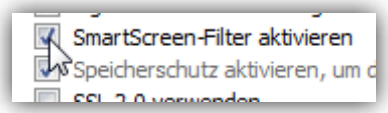
Ebenfalls gefährlich: Über manipulierte Webseite versuchen Hacker, Schadprogramme auf den Rechner zu schleusen. Neben direkten Angriffen mit Methoden wie Clickjacking und Cross-Site-Scripting (XSS) droht Gefahr von vermeintlich harmlosen Downloads, hinter denen sich schädliche Programme verbergen.

Zum Glück ist gegen Phishing, manipulierte Webseiten und gefährliche Downloads ein Kraut gewachsen: der SmartScreen-Filter des Internet Explorers überwacht alle Aktivitäten im Netz. Bevor der Browser eine Seite darstellt, schickt er die Webadresse zuerst zu Microsofts Sicherheits-Servern, die über eine Liste bekannter Phishing- und Hacker-Seiten sowie gefährlicher Downloadanbieter verfügen. Erst wenn die Adresse „sauber" ist und

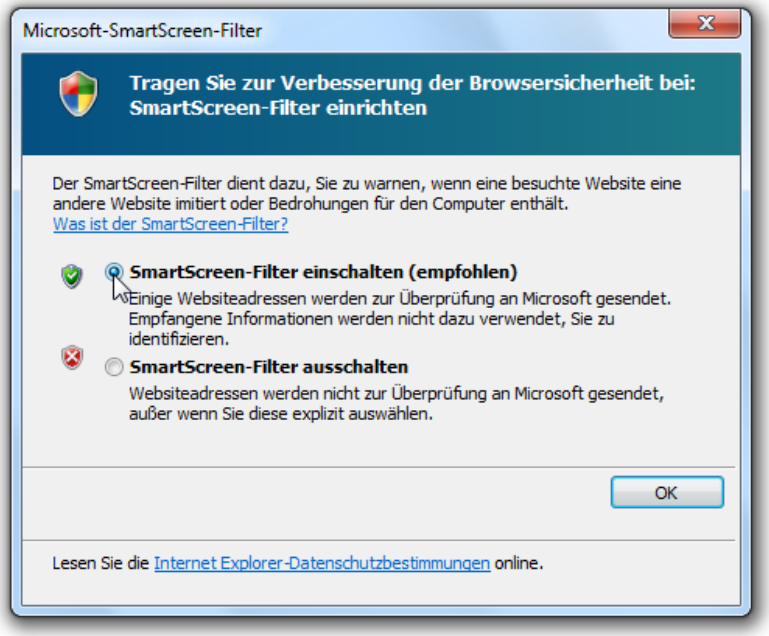
nicht auf der schwarzen Liste steht, zeigt der Internet Explorer die Webseite an. Kommt Windows 7 die Adresse hingegen suspekt vor, erscheint ein Warnhinweis. Sie können dann selbst entscheiden, ob Sie die Seite tatsächlich besuchen möchten oder nicht.



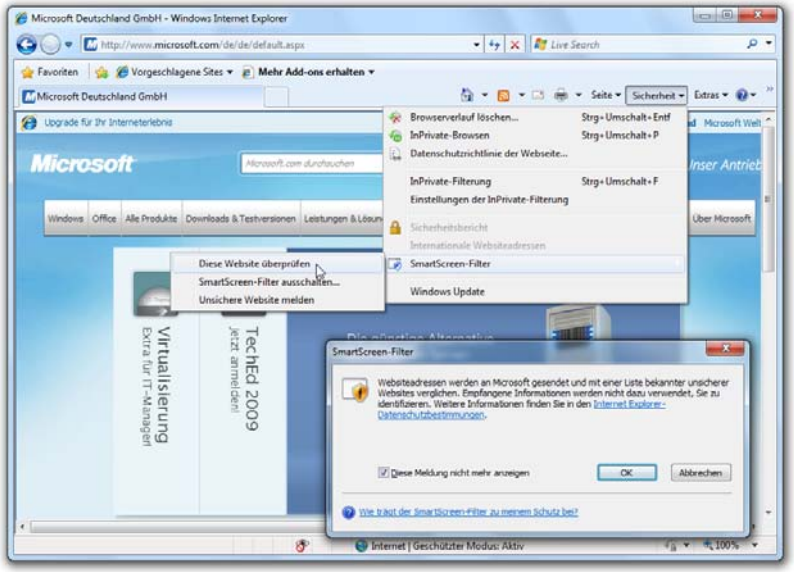
Erwischt: Der SmartScreen-Filter des Internet Explorers hat eine gefährliche Webseite entdeckt und den Zugriff blockiert.



Ob der SmartScreen-Filter eingeschaltet und richtig konfiguriert ist, können Sie leicht nachprüfen. Rufen Sie im Internet Explorer den Befehl Extras | Internetoptionen auf, und wechseln Sie ins Register Erweitert. Hier sollte im Bereich Sicherheit das Kontrollkästchen SmartScreen-Filter aktivieren angekreuzt sein.Sie können den Filter auch aktivieren, indem Sie den Menübefehl Sicherheit | SmartScreen-Filter | SmartScreen-Filter aufrufen, im nächsten Fenster die Option SmartScreen-Filter einschalten (empfohlen) aktivieren und mit OK bestätigen.



Mit aktiviertem SmartScreen-Filter überprüft der Internet Explorer die Seiten automatisch. Sie können Webseiten auch manuell inspizieren. Hierzu wählen Sie im Menü Sicherheit | SmartScreen-Filter den Befehl Diese Website überprüfen. Der Internet Explorer nimmt die Seite dann noch einmal unter die Lupe und teilt das Ergebnis mit.

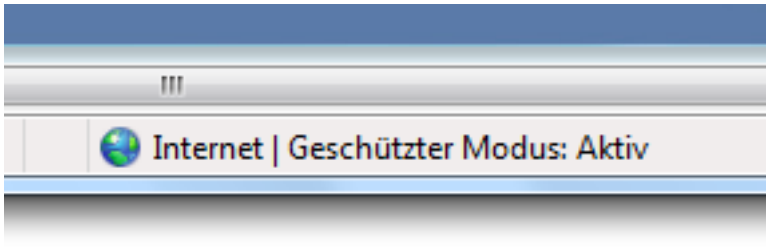


Wer auf Nummer sicher gehen möchte, kann mit dem Befehl Diese Website überprüfen jede Adresse noch einmal manuell inspizieren.

Optimale Sicherheit durch geschützten Modus

Der Internet Explorer von Windows 7 arbeitet standardmäßig im geschützten Modus. Der Name ist Programm: Im geschützten Modus wird verhindert, dass manipulierte Webseiten

heimlich Daten ausspähen oder Konfigurationsänderungen vornehmen.



Ob der Internet Explorer im geschützten Modus arbeitet, erkennen Sie anhand der Statusleiste am unteren Rand des Internet-Explorer-Fensters. Taucht dort der Hinweis Geschützter Modus: Aktiv auf, sind Sie beim Surfen durch das Internet sicher vor manipulierten Webseiten.

Im geschützten Modus arbeitet der Internet Explorer isoliert von anderen Programmen oder dem Betriebssystem selbst. Wie in einem Käfig. Angriffe von manipulierten Webseiten haben im geschützten Modus keine Chance, außerhalb des Käfigs Schaden anzurichten. Die Schreibzugriffe beschränken sich auf den Ordner Temporäre Internetdateien – mehr ist nicht erlaubt.

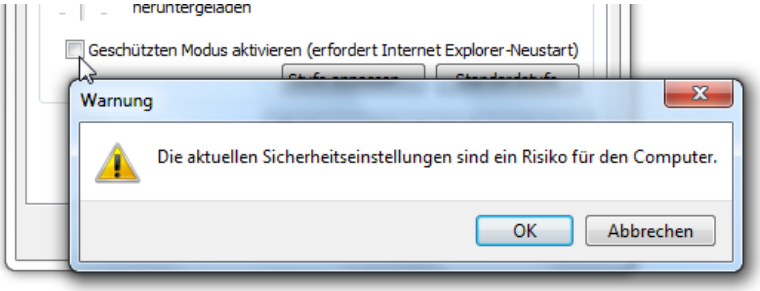
Und falls doch einmal eine bösartige Software versucht, aus dem Käfig auszubrechen, erscheint eine Warnmeldung. Erst wenn Sie die Warnmeldung bestätigen und Ihre Zustimmung für den „Ausbruchsversuch" geben, gewährt der Internet Explorer den erweiterten Zugriff. Das kann zum Beispiel sinnvoll sein bei Programmen oder Webseiten, denen Sie vertrauen – beispielsweise der Microsoft-Webseite.

Standardmäßig sind Sie mit dem Internet Explorer stets im geschützten Modus unterwegs. Auf Wunsch können Sie den geschützten Modus aber auch deaktivieren. Das ist allerdings

nur sinnvoll, wenn Sie wiederholt Webseiten besuchen, denen Sie vertrauen und die einen erweiterten Zugriff benötigen. Das kann zum Beispiel in internen Firmennetzwerken (Intranets) notwendig sein.

Um den geschützten Modus zu deaktivieren, gehen Sie folgendermaßen vor:

1. Klicken Sie im Internet Explorer auf Extras, und wählen Sie den Befehl Internetoptionen.
2. Wechseln Sie in das Register Sicherheit.
3. Hier können Sie das Kontrollkästchen Geschützten Modus aktivieren ausschalten.



stop

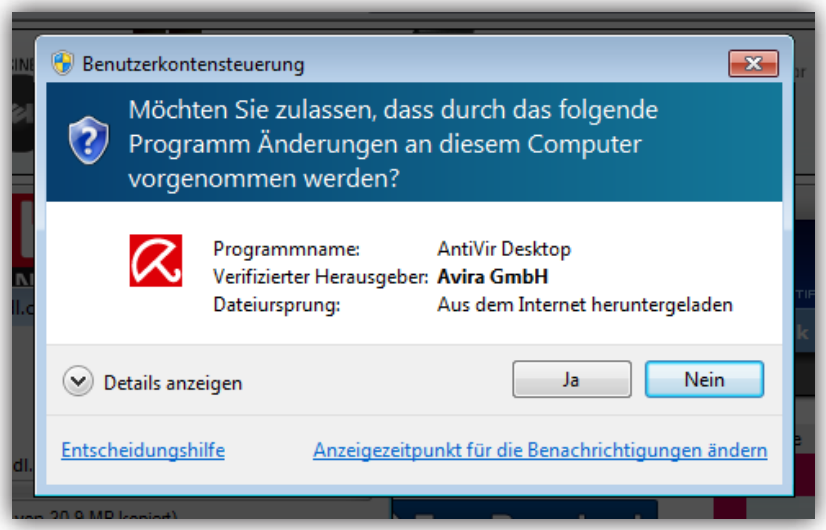
Den geschützten Modus sollten Sie nur in Ausnahmefällen deaktivieren – etwa um eine Software zu installieren, der Sie vertrauen. Das Surfen mit dem Internet Explorer ist ohne den geschützten Modus wesentlich unsicherer. Schalten Sie den geschützten Modus sofort wieder ein, sobald der Ausnahmefall erledigt ist.

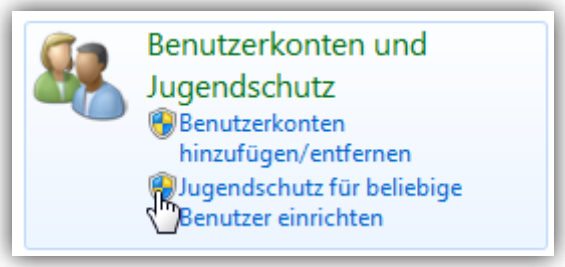
Die Benutzerkontensteuerung

Damit wichtige Systemeinstellungen nicht unbemerkt verändert werden können, schiebt die sogenannte Benutzerkontensteuerung unerwünschten Änderungen einen Riegel vor. In der Praxis funktioniert das so: Sobald ein Programm eine Aktion durchführen möchten, die Windows 7 als potenziell gefährlichen Eingriff in das System ansieht, erscheint ein Warnhinweis.

Im Vergleich zum Vorgänger Vista werden Sie beim neuen Windows 7 aber wesentlich seltener von Warnhinweisen unterbrochen. Wenn Sie selbst eine Änderung durchführen – etwa eine Anpassungen der Firewall-Regeln – gibt es keine Unterbrechungen. Alle eigenen Änderungen werden sofort umgesetzt. Erst wenn im Hintergrund ein Programm heimlich versucht, sicherheitsrelevante Einstellungen zu ändern (oder wenn Sie nicht als Administrator eingeloggt sind), erscheint die Benutzerkontensteuerung. Die bedenkliche Aktion – etwa das Deaktivieren der Firewall – wird erst nach Bestätigung oder der Eingabe eines Administratorkennworts durchgeführt.

Alle geschützten Bereiche sind mit einem bunten Schutzschild-Symbol gekennzeichnet, beispielsweise in der Systemsteuerung. Versucht ein Programm, hier unbemerkt Änderungen vorzunehmen, erscheint eine Warnmeldung.



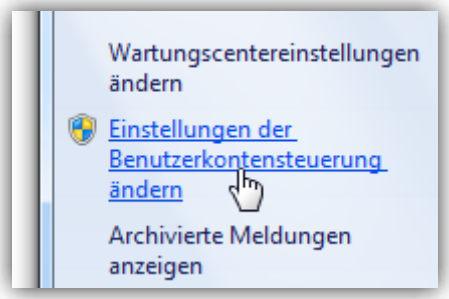


Als Standardbenutzer besonders sicher arbeiten

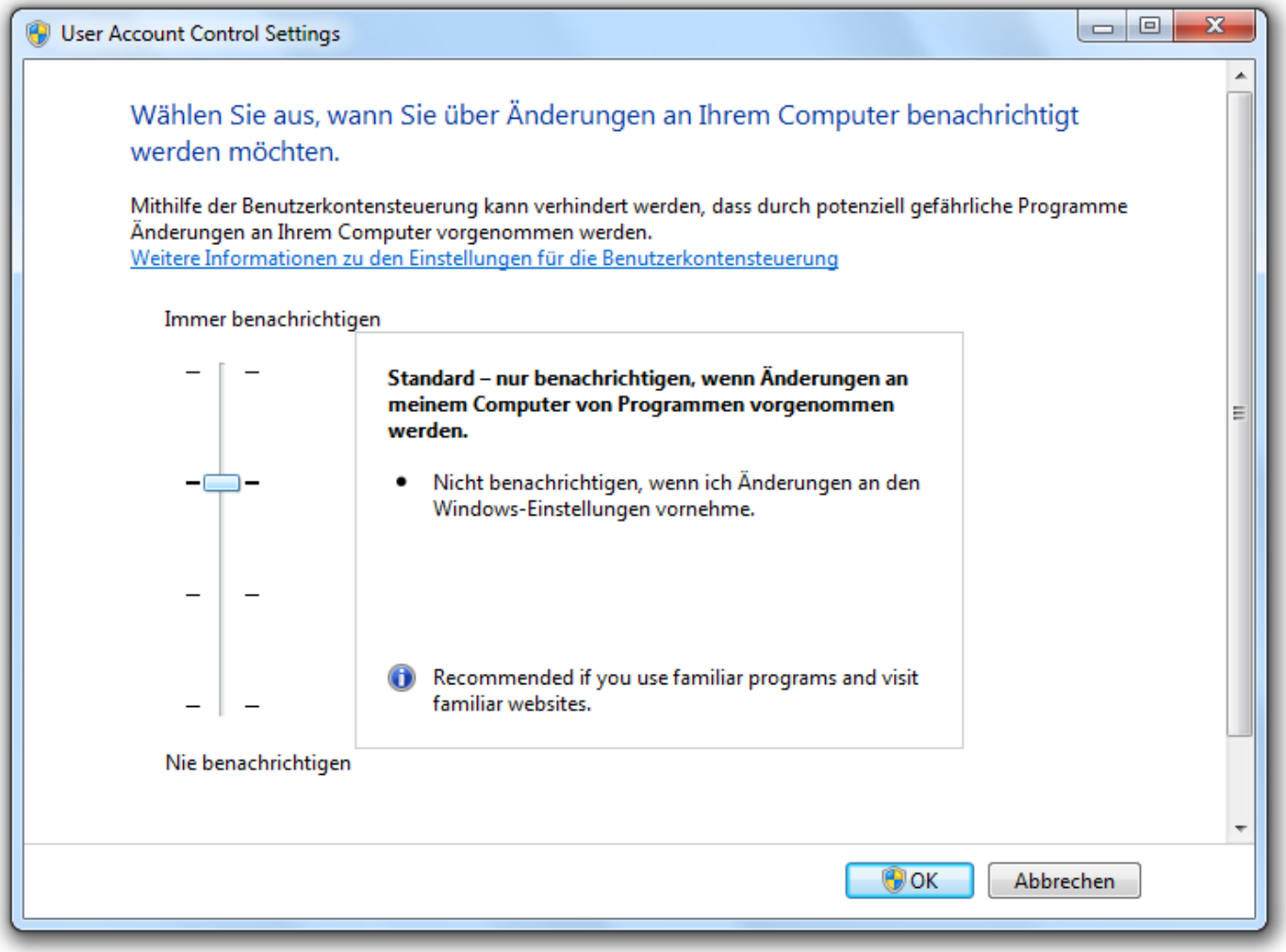
Unser Tipp für größtmögliche Sicherheit: Verwenden Sie für die tägliche Arbeit mit Windows 7 nicht das Administrator-, sondern ein Standardbenutzerkonto. Das Standardkonto ist mit weniger Rechten ausgestattet und schützt den PC noch besser vor versehentlichen oder mutwilligen Eingriffen. Trotz der Einschränkung können Sie alle Windows-Funktionen nutzen. Sobald Sie Sicherheitseinstellungen ändern möchten, muss lediglich das Kennwort eines Administratorkontos eingegeben werden. Wie's funktioniert, steht weiter unten im Abschnitt Sicher arbeiten als Standardbenutzer.

Sie können übrigens selbst festlegen, wie „scharf" die Benutzerkontensteuerung eingestellt ist. Für die meisten Anwender sind die Standardeinstellungen optimal. Warnmeldungen erscheinen dann nur, wenn Änderungen von Programmen vorgenommen werden. Wer mehr Sicherheit wünscht, kann die Benutzerkontensteuerung schärfer einstellen und zum Beispiel auch auf Konfigurationsänderungen des Benutzers eine Auge werfen. So geht's:

1. Öffnen Sie die Systemsteuerung (Start | Systemsteuerung), und klicken Sie auf System und Sicherheit sowie Wartungscenter.



2. Klicken Sie auf Einstellungen der Benutzerkontensteuerung ändern.
3. Im folgenden Fenster haben Sie die Wahl zwischen vier Einstellungen:
   - Immer benachrichtigen: Die Benutzerkontensteuerung greift ein, wenn andere Programme oder Sie selbst Änderungen an geschützten Bereichen vornehmen. Diese Einstellung entspricht der Benutzerkontensteuerung des Vorgängers Windows Vista.
   - Standard: Das ist die empfohlene Standardeinstellung. Die Benutzerkontensteuerung greift nur noch ein, wenn andere Programme sicherheitsrelevante Einstellungen verändern möchten. Sie selbst können ungehindert Änderungen vornehmen und werden nicht mehr so oft bei der Arbeit unterbrochen wie beim Vorgänger Windows Vista.
   - Nur benachrichtigen, wenn…: Ähnliche wie Standard, allerdings wird der Bildschirm nicht mehr verdunkelt, sobald das Warnfenster erscheint.
   - Nie benachrichtigen: Mit dieser Option verzichten Sie völlig auf den Schutz durch die Benutzerkontensteuerung. Jeder (Sie selbst oder andere Programme) können ungehindert sicherheitsrelevante Einstellungen verändern. Diese Einstellung sollten Sie nur in Ausnahmefällen verwenden, falls sich beispielsweise alte Programme sonst nicht nutzen oder installieren lassen. Danach sollten Sie wieder die Standardeinstellung verwenden.

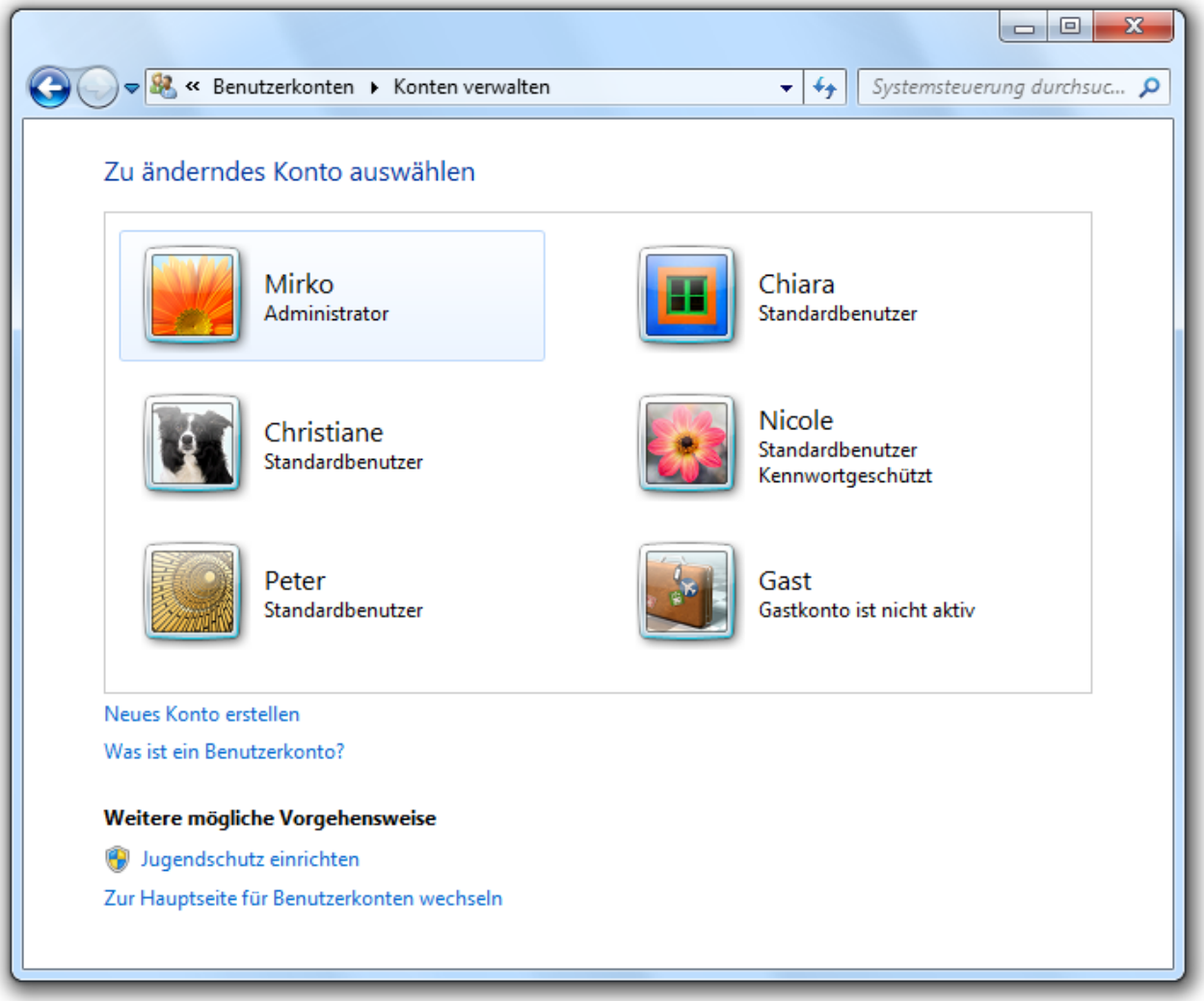


In der Systemsteuerung legen Sie selbst fest, wie genau die Benutzerkontensteuerung ein Auge auf Systemänderungen wirft. Die Standardeinstellung ist ein guter Kompromiss zwischen Sicherheit und flüssigem Arbeiten ohne störende Unterbrechungen.

Sicher arbeiten als Standardbenutzer

Sicher ist ein Betriebssystem erst dann, wenn möglichst viel verboten ist. Es ist zwar praktisch, wenn man an seinem eigenen PC alles und jedes verändern kann. So viel Freiheit hat aber seinen Preis. Mitunter werden wichtige Systemeinstellungen – oft unabsichtlich – verändert. Oder findige Hacker nutzen die Freizügigkeit und nehmen tiefgreifende Änderungen vor – ohne, dass Sie selbst etwas davon bemerken. Der PC wird dann langsamer, oder schlimmstenfalls spionieren Hacker Ihren Computer aus.

Dem „Jeder darf alles"-Problem begegnet Windows 7 mit Benutzerkonten. Die gab es auch schon bei Windows XP und Vista, mit Windows 7 sind sie aber noch ausgeklügelter geworden. Und es funktioniert: Jeder, der regelmäßig mit dem PC arbeitet, erhält ein eigenes Benutzerkonto. Ganz wichtig: Das Benutzerkonto ist nur mit eingeschränkten Rechten versehen. Und zwar mit genau so vielen, dass jeder mit „seinen" Programmen wie gewohnt arbeiten, aber keinesfalls Daten und Einstellungen anderer Benutzer verändern oder gar sicherheitsrelevante Veränderungen vornehmen kann. Und wenn doch einmal Einstellungen vorgenommen werden sollen, die einem Standardbenutzer verwehrt bleiben, gibt es noch das Administrator-Konto. Das ist sozusagen der Super-Benutzer, der alles darf. Um systemnahe Veränderungen vorzunehmen, melden Sie sich einfach mit einem Administrator-Konto an, nehmen die gewünschten Einstellungen vor und – ganz wichtig – arbeiten danach als „einfacher" Benutzer weiter. Wer sich konsequent an dieses Konzept hält, macht seinen PC praktisch „bombensicher".

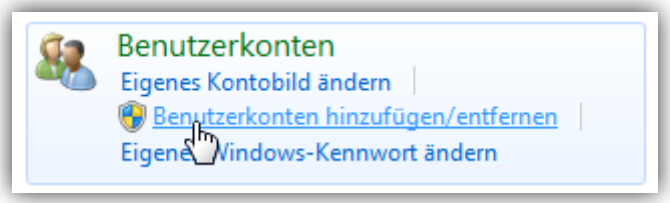


Der beste Schutz vor Manipulationen: Jedes Familienmitglied bekommt ein Standardbenutzerkonto mit eingeschränkten Rechen.

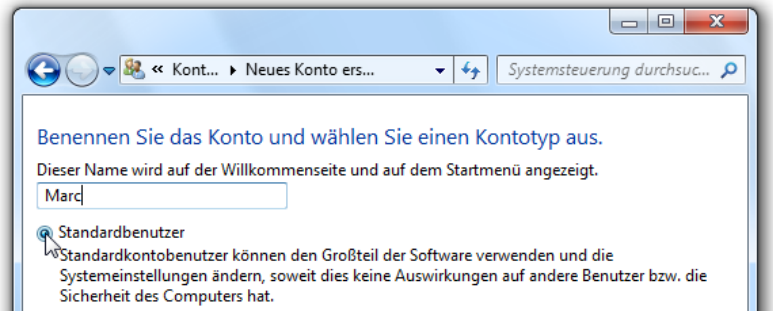
Benutzerkonten einrichten

Idealerweise erhält jedes Familienmitglied ein eigenes Benutzerkonto, in dem es sich nach Herzenslust „austoben" kann. Zum Beispiel eines für den Vater, eines für die Mutter und jeweils eines für Tochter und Sohn. Jedes Konto ist dabei mit einem Kennwort geschützt, damit auch innerhalb der Familie die Privatsphäre gewahrt bleibt. Gehen Sie folgendermaßen vor, um ein neues Benutzerkonto – z.B. für den Sohn – einzurichten:

1. Klicken Sie auf das Start-Symbol, und wählen Sie den Befehl Systemsteuerung.
2. Anschließend klicken Sie auf Benutzerkonten und Jugendschutz sowie Benutzerkonten.



3. Um ein neues Konto einzurichten, klicken Sie auf Benutzerkonten hinzufügen/entfernen und Neues Konto erstellen.



4. Geben Sie den Namen des Benutzers ein – z.B. den Namen Ihres Sohnes –, und wählen Sie die Option Standardbenutzer. Jeder Standardbenutzer darf den PC wie gewohnt bedienen und beispielsweise Programme benutzen oder im Internet surfen. Ein Standardbenutzer darf aber nicht alles: Alle Änderungen, die die Sicherheit des Computers gefährden oder Daten anderer Benutzer verändern, sind nicht möglich. Der Computer

bleibt damit vor unliebsamen Beschädigungen verschont.

5. Klicken Sie auf Konto erstellen.
6. Das Einrichten des neuen Kontos ist damit abgeschlossen.
7. Klicken Sie auf den Namen des neuen Kontos, um weitere Daten zu ergänzen. Wenn mehrere Benutzer den PC verwenden und Ihnen die Wahrung der Privatsphäre wichtig ist, können Sie das Benutzerkonto mit einem Passwort schützen. Der neue Benutzer muss dann später erst sein Kennwort eingeben, um den PC benutzen zu können. Mit einem Mausklick auf Kennwort erstellen vergeben Sie das Passwort für den neuen Benutzer.

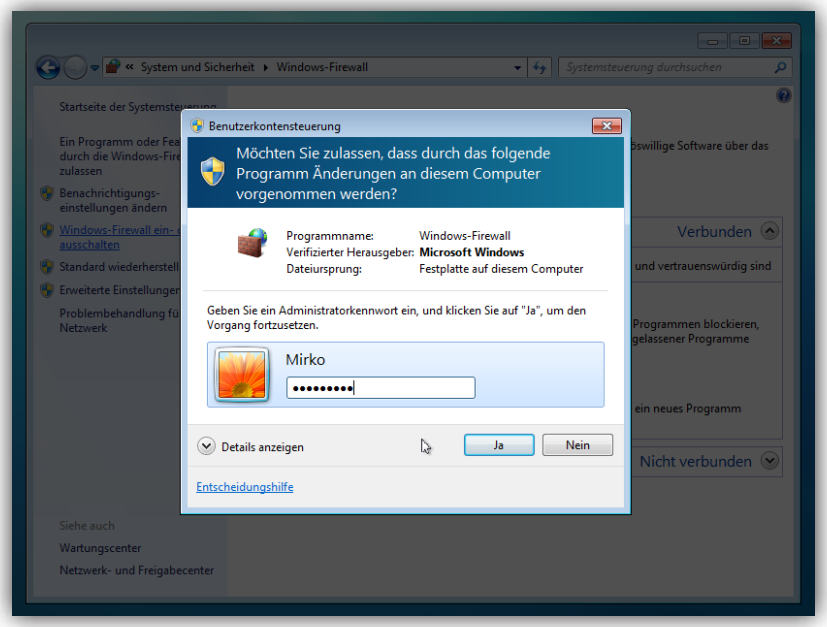
Sie können das Kennwort auch weglassen und ohne Passwortschutz arbeiten. Dann kann der Benutzer des Kontos den PC auch ohne Kennworteingabe bedienen. Der Schutz vor versehentlichen oder mutwilligen Eingriffen in das Betriebssystem bleibt trotzdem bestehen.

Beim nächsten Start von Windows kann sich der neu eingerichtete Benutzer anmelden und mit dem PC arbeiten. Persönliche Änderungen wie die Anordnung oder Farben des Desktops bleiben auf das eigene Konto begrenzt.

Als Standardbenutzer trotzdem Systemänderungen durchführen

Das Schöne an der Benutzerverwaltung: Auch wenn Sie Windows mit einem Standardbenutzerkonto mit beschränkten Rechten verwenden, können Sie dennoch alles machen. Der Trick: Sobald Sie eine Aktion durchführen möchten, für die Ihre Rechte als Standardbenutzer nicht ausreichen, erscheint zunächst eine Warnmeldung.

Sie können die Aktion nur dann ausführen, wenn Sie sich als Administrator ausweisen können. Windows blendet hierzu eine Liste der Konten mit Administratorrechten ein. Erst wenn Sie auf eines der Administratorkonten klicken und das korrekte Kennwort für das Administratorkonto eingeben, führt Windows die Aktion – zum Beispiel das Formatieren einer Festplatte – durch. Wichtig: Die gewährten Administratorrechte gelten nur für diese eine Aktion – danach arbeiten Sie automatisch wieder als Standardbenutzer mit eingeschränkten Rechten.



Bevor Sie als Standardbenutzer wichtige Systemeinstellungen verändern, fragt Windows nach dem Kennwort eines Administrators.

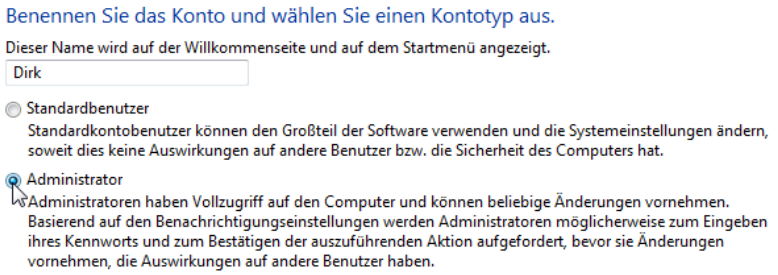
Neben den Standardbenutzern sollte auf jedem PC noch ein gesondertes Konto be-

stehen: das Administrator-Konto. Der Administrator ist praktisch der Super-Benutzer, der alles darf – auch das System beschädigen. Für viele Aktionen rund um die Einrichtung des PCs, z.B. das Formatieren von Festplatten, sind Administratorrechte notwendig.

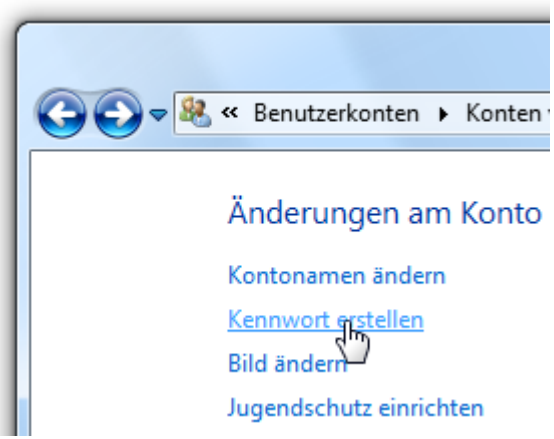
Auch wenn es verlockend ist: Bei der täglichen Arbeit mit dem PC sollten Sie nicht mit dem Administrator-Konto „unterwegs" sein. Damit können Sie zwar alles mit Windows anstellen, die „Ich darf alles"-Berechtigung birgt aber auch die Gefahr, dass versehentlich wichtige Systemeinstellungen verändert werden. Oder dass eingeschleuste Software Ihre Kontoberechtigung missbraucht, um Daten auszuspionieren oder Windows unbrauchbar zu machen. Das Administratorkonto sollte daher immer nur dann zum Einsatz kommen, wenn Sie auch administrative Arbeiten erledigen möchten. Für die tägliche Arbeit reicht ein Standardbenutzerkonto.

Windows vergibt üblicherweise dem ersten Konto, das während der Installation angegeben wird, Administrator-Rechte. Sie können aber jederzeit ein neues Administratorkonto einrichten:

1. Klicken Sie auf das Start-Symbol, und wählen Sie den Befehl Systemsteuerung.
2. Dann klicken Sie auf Benutzerkonten und Jugendschutz sowie Benutzerkonten und Benutzerkonten hinzufügen/entfernen.



3. Klicken Sie auf Neues Konto erstellen, und geben Sie in das nachfolgende Dialogfenster den gewünschten Namen des Administrators ein. Wählen Sie den Kontotyp Administrator.
4. Klicken Sie auf Konto erstellen.



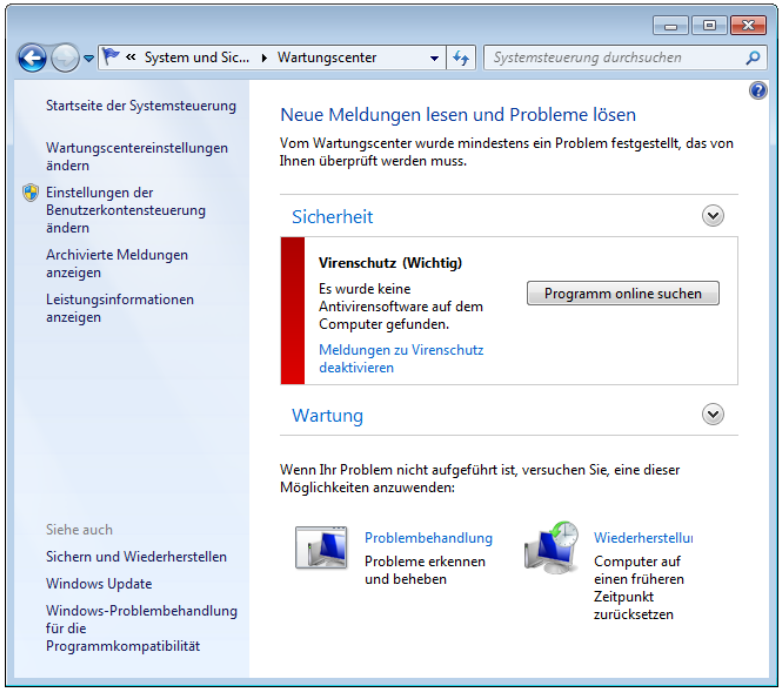
5. Ganz wichtig: Sie sollten für das Administratorkonto unbedingt ein eigenes Kennwort vergeben, damit sich nicht jeder einfach per Mausklick als Administrator ausgeben kann. Klicken Sie hierzu auf den Namen des neu angelegten Kontos und anschließend auf Kennwort erstellen.
6. Tragen Sie im nachfolgenden Fenster zweimal das gewünschte Passwort ein, und bestätigen Sie die Eingabe mit einem Mausklick auf die Schaltfläche Kennwort erstellen.

Unsere Empfehlung: Nutzen Sie das Administrator-Konto nur in Ausnahmefällen. Am sichersten ist es, für die tägliche Arbeit das normale Standardbenutzerkonto zu verwenden. Damit kann am wenigsten passieren. Und falls Sie doch einmal Programme installieren oder Systemeinstellungen ändern möchten, müssen Sie nur im Auswahlfenster der Benutzerkontensteuerung das Konto und Kennwort eines Administratorkontos eingeben.

Was noch fehlt: der Schutz vor Viren

Windows ist mit zahlreichen Schutzmechanismen ausgestattet: Phishing-Filter, Firewall, Anti-Spyware-Software und vieles mehr. Nur eine wichtige Komponente, die eigentlich auf jedem PC installiert sein sollte, fehlt: Ein AntiViren-Programm, dass den PC vor Viren, Würmern und anderer schädlicher Software schützt.

Dass Windows die wichtige Antivirenlösung fehlt, erkennen Sie sofort beim Start des Betriebssystems. In der rechten unteren Ecke taucht regelmäßig ein kleines Fähnchen auf und weist Sie darauf hin, dass keine Antivirenlösung gefunden wurde und der PC eventuell gefährdet ist. Auch im Wartungscenter (Start | Systemsteuerung | Wartungscenter) weist Windows deutlich auf die fehlende Antivirussoftware hin.



Das Wartungscenter macht es deutlich: Windows 7 fehlt eine Antivirussoftware. Das lässt sich schnell ändern.

Eine Antivirussoftware gehört auf jeden PC. Insbesondere wenn Sie viel im Internet surfen oder E-Mails verschicken. Sie sollten daher unbedingt eine Antivirussoftware

nachinstallieren. Sie haben hierzu folgende Möglichkeiten:

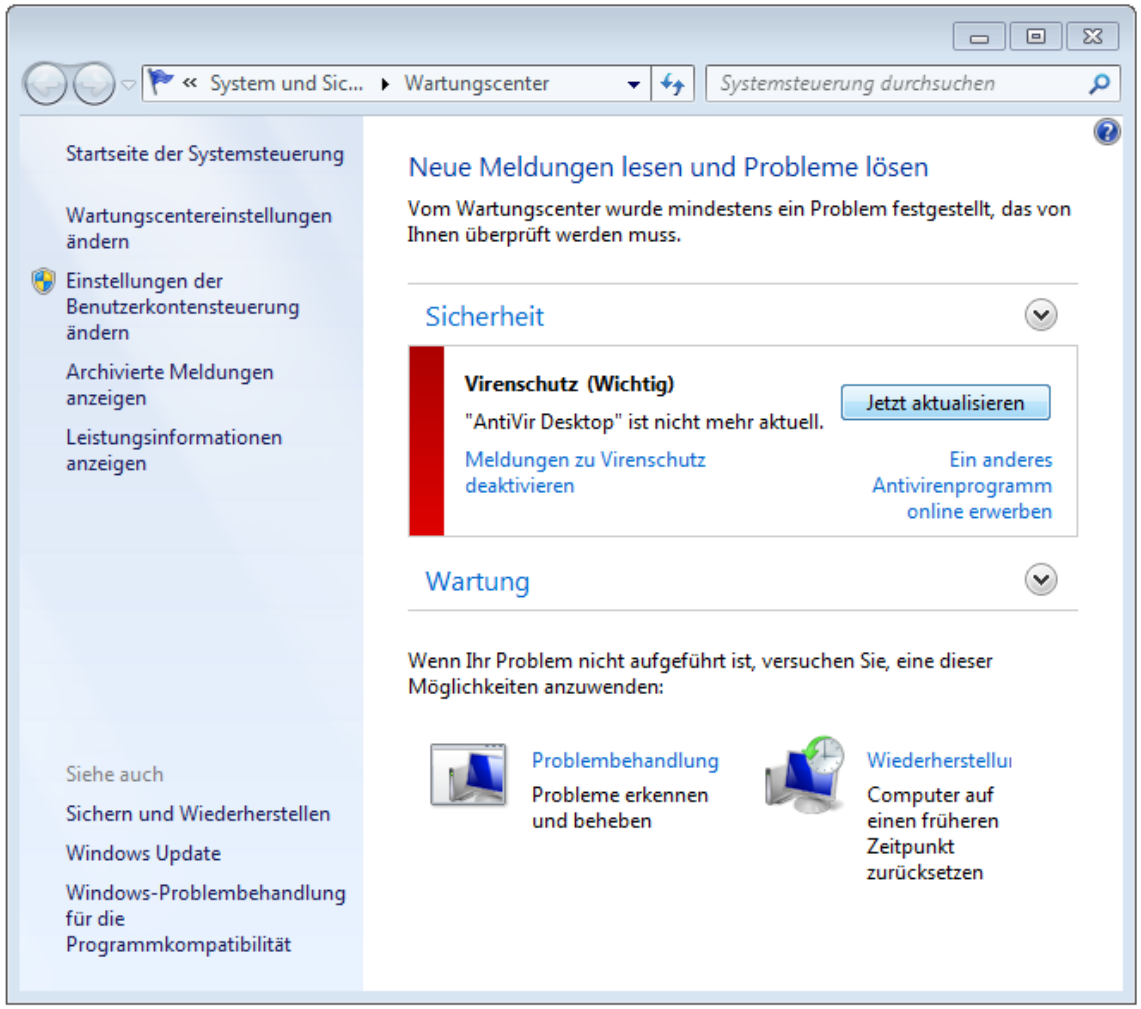
- Antiviruslösung von Microsoft: Microsoft bietet selbst eigene Antivirussoftware namens Microsoft Security Essentials an. Auf der Webseite http://www.microsoft.com/security_essentials können Sie den kostenlosen Virenschutz herunterladen und sind sofort vor gefährlichen Viren und Schädlingen geschützt.
- Kommerzielle Lösungen von Drittherstellern: Viele Softwarehäuser haben sich auf die Bekämpfung von Viren spezialisiert und bieten bereits seit Jahren Antivirussoftware an. Hierzu gehören beispielsweise Symantec (http://www.symantec.de), Kaspersky Labs (http://www.kaspersky.de) oder G-Data (http://www.g-data.de). Hier erhalten Sie für knapp 50 Euro professionelle Antivirensoftware, die Ihren PC „sauber" hält.

Eine Liste aller Antivirus-Partner von Microsoft finden Sie auf der Webseite http://www.microsoft.com/germany/windows/antivirus-partners/windows-7.aspx.

- Kostenlose Virenscanner: Neben kommerziellen Angeboten gibt es gute kostenlose Antiviruslösungen. Die bieten meist zwar weniger Komfortfunktionen, schützen aber genauso zuverlässig vor Viren, Trojanern und ähnlichen Schädlingen. Zu den besten kostenlosen Virenscannern für Windows 7 zählt Avast! Antivirus Home (http://www.avast.de). Auch E-Mails werden bereits während des Empfangs auf Viren geprüft – das können viele andere Gratisscanner nicht. Ebenfalls ein Pluspunkt: Avast Antivirus braucht wenig Systemressourcen. Ideal für ältere Rechner, Netbooks und Notebooks. Ebenfalls empfehlenswert sind die

Gratis-Virenscanner Avira AntiVir Personal (http://www.free-av.de) oder AVG Free (http://free.avg.de).

Für welche Lösung Sie sich auch entscheiden, eines ist allen gemeinsam: Sobald die Antivirussoftware installiert ist, gibt Windows auch für den Schutz vor schädlicher Software grünes Licht. Vorausgesetzt, die installierte Antiviruslösung ist aktuell und mit den neuesten Updates und Antivirus-Signaturen versehen. Sollte das installierte Antivirusprogramm Probleme bereiten, weil es zum Beispiel veraltete Virendatenbanken verwendet, schlägt das Wartungscenter von Windows sofort Alarm; bietet aber auch gleich die passende Lösung an, zum Beispiel das sofortige Aktualisieren der Antivirussoftware.



Falls es in Sachen Virenschutz Probleme gibt, macht das Wartungsfenster darauf aufmerksam. Ist die Virendatenbank zum Beispiel veraltet, können Sie sie per Mausklick auf den neuesten Stand bringen. In der Regel aktualisiert sich das Antivirentool aber selbst.

ratschlag24.com

Das neue Ratgeber-Portal ratschlag24.com liefert Ihnen täglich die besten Ratschläge direkt auf Ihren PC.

Viele bekannte Autoren, Fachredakteure und Experten schreiben täglich zu Themen, die Sie wirklich interessieren und für Sie einen echten Nutzen bieten. Zu den Themen zählen Computer, Software, Internet, Gesundheit und Medizin, Finanzen, Ernährung, Lebenshilfe, Lernen und Weiterbildung, Reisen, Verbrauchertipps und viele mehr. Alle diese Ratschläge sind für Sie garantiert kostenlos. Testen Sie jetzt ratschlag24.com – Auf diese Ratschläge möchten Sie nie wieder verzichten.

ratschlag24.com ist ein kostenloser Ratgeber-Dienst der eload24 AG
www.eload24.com

eload24

Viel guter Rat ab 3 Euro monatlich: Die neuen Flatrate-Modelle von eload24

Das ist ein Wort: Sie bekommen **freien Zugang zu allen eBooks** bei eload24. Sie können alles laden, lesen, ausdrucken, ganz wie es Ihnen beliebt. Eine echte Flatrate eben, ohne Wenn und Aber. Sie werden staunen: Unser Ratgeber-Programm ist groß und wird laufend erweitert.

Der Preisvorteil ist enorm:
24 Monate Flatrate für nur 72,00 € (3,00 € monatlich)
12 Monate Flatrate für nur 48,00 € (4,00 € monatlich)
6 Monate Flatrate für nur 36,00 € (6,00 € monatlich)

Selbst wenn Sie nur zwei eBooks der preiswertesten Kategorie im Monat laden, sparen Sie im Vergleich zum Einzelkauf.

Tausende Kunden haben dieses Angebot schon wahrgenommen, profitieren auch Sie dauerhaft. Wenn Sie nach Ablauf der Flatrate weitermachen wollen, brauchen Sie nichts zu tun: Das Abonnement verlängert sich automatisch. Bis Sie es beenden.

Kaufen Sie jetzt die Flatrate Ihrer Wahl. Schon einige Augenblicke später stehen Ihnen Hunderte toller Ratgeber uneingeschränkt zur Verfügung: Packen Sie mal richtig zu!

www.eload24.com/flatrate