PEARSON Education

magnum

Windows Vista Business

MICHAEL KOLBERG

Markt+Technik

kompakt
komplett
kompetent

Jubiläums-ausgabe
€ 24,95 [D]
€ 25,70 [A] / sFr 42,50

Tools und Utilities zu Windows Vista, die das Betriebssystem erheblich aufwerten

+++Jubiläumspreis+++Jubiläumspreis++

3 Die Basissicherheit kontrollieren

Nachdem Sie Windows Vista etwas kennengelernt haben, sollten Sie sich möglichst früh mit der Frage beschäftigen, welche Sicherheiten Ihnen Ihr Rechner bietet. Der normale Anwender möchte ja meist den Computer für produktive Zwecke – welche auch immer – einsetzen und dazu gehören die Fragen der Sicherheit nur bedingt. Da die Welt aber nun einmal schlecht ist, ist er trotzdem gezwungen, sich damit zu beschäftigen. Für ihn ist es wahrscheinlich die beste Strategie, das Aufspüren solcher Lücken den Experten auf diesem Gebiet zu überlassen und möglichst schnell und vollständig von deren Erkenntnissen zu profitieren. Er sollte sich also bezüglich der Informationen zu neu entdeckten Sicherheitslücken immer auf dem neuesten Stand halten und diese anschließend wirksam mit den angebotenen Hilfsmitteln schließen. Dieses Kapitel liefert einen Überblick darüber, was Sie dazu wissen sollten. Einiges davon verlangt einen funktionierenden Zugang zum Internet (→ Kapitel 4).

- Einen guten Einstieg in die Sicherheitseinstellungen Ihres Rechners liefert Ihnen das *Sicherheitscenter* in der *Systemsteuerung* (→ Abschnitt 3.1). Dieses Werkzeug läuft als Hintergrundprozess und überwacht die Einstellungen der wichtigsten Werkzeuge zur Computersicherheit: *Windows Update*, *Windows Firewall*, *Windows Defender* und *Virenschutz*.
- Nachdem Sie das *Sicherheitscenter* kennengelernt haben, sollten Sie sich mit seinen einzelnen Bestandteilen beschäftigen. Auf jeden Fall sollten Sie *Benutzerkonten* einrichten (→ Abschnitt 3.2). Das gilt besonders dann, wenn mehrere Personen den Computer verwenden. Bereits bei der Installation wurden Sie ja auf dem Einrichtungsbildschirm aufgefordert, ein Konto und ein Kennwort dafür einzurichten.
- In Windows Vista steht Ihnen standardmäßig die Möglichkeit automatischer *Updates* zur Verfügung (→ Abschnitt 3.3). Da auch die Techniken derjenigen, die versuchen, in Ihren Rechner einzubrechen, immer besser werden, sollten Sie diese Verfahrensweise nutzen, um den Computer gegen neue Formen des Angriffs zu schützen. Sie bestimmen dabei aber selbst, auf welche Weise und wann der Computer von Windows aktualisiert wird:
- Eine auf Software basierende *Firewall*, die die Kommunikation zwischen dem Internet und dem Computer oder Netzwerk einschränkt, wird bei der Installation von Vista automatisch eingerichtet und automatisch aktiviert (→ Abschnitt 3.4). Sie sollten die wesentlichen Methoden zur Steuerung dieses Werkzeugs kennen.
- Es ist wichtig, den Computer in regelmäßigen Abständen danach zu untersuchen, ob nicht ein Programm aktiv ist, das Ihre Aktivitäten aufzeichnet und im Hintergrund an jemanden sendet, der Böses damit vorhat. Das leistet der *Windows Defender* (→ Abschnitt 3.5).
- Manchmal muss man sich nicht nur vor externen Angriffen, sondern auch vor eigenen unbedachten Aktionen schützen. Es geschieht zwar

recht selten, aber passieren kann es trotzdem: Sie installieren beispielsweise ein Anwendungsprogramm oder eine Treibersoftware und plötzlich funktioniert überhaupt nichts mehr. Durch Auswahl eines vor dem Änderungsdatum oder -zeitpunkt liegenden *Wiederherstellungspunkts* kann dann ein früherer Zustand des Computers wiederhergestellt werden (→ Abschnitt 3.6).

3.1 Das Sicherheitscenter

Um sich einen ersten Überblick über die Sicherheitseinstellungen Ihres Rechners zu verschaffen, wählen Sie die Ebene *Sicherheitscenter* in der *Systemsteuerung*. Das mit *Windows-Sicherheitscenter* benannte Fenster wird angezeigt (→ Bild 3.1). Sie können dieses Fenster auch anzeigen lassen, indem Sie auf das Symbol *Windows-Sicherheitshinweise* im Infobereich der Taskleiste doppelklicken.

3.1.1 Die Struktur

Nachdem Sie das Sicherheitscenter geöffnet haben, werden darin Statusinformationen von vier Bereichen angezeigt – *Firewall*, *Automatische Updates*, *Schutz vor schädlicher Software* und *Weitere Sicherheitseinstellungen*.

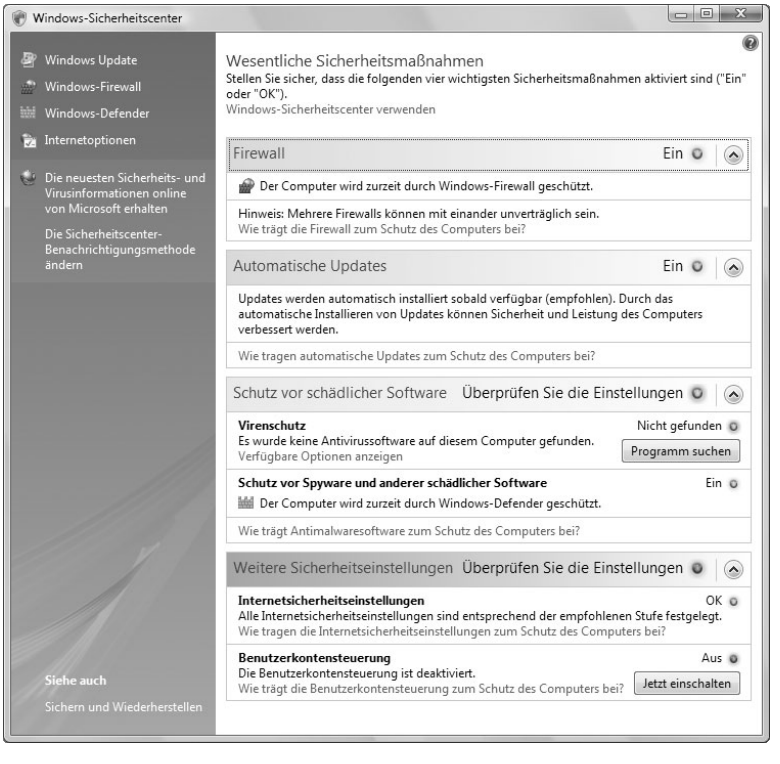


Bild 3.1: Das Windows-Sicherheitscenter

- Um Ihre Aufmerksamkeit zu lenken, wird für die Anzeige ein Farbcode verwendet: Die Farbe *Grün* zeigt an, dass die aktuellen Einstellungen den Computer schützen, *Gelb* signalisiert, dass Aktionen des Anwenders eventuell notwendig sind, und *Rot* kennzeichnet eine potenzielle Gefährdung.

- Die Anzeige der Details zu einem der Elemente des Sicherheitscenters können Sie über die kleinen Schaltflächen mit den Pfeilspitzen an- und abschalten.
- Für einige Probleme gibt es Schaltflächen für eine schnelle Lösung. Wenn beispielsweise die Einstellungen im Bereich *Automatische Updates* bemängelt werden, kümmert sich nach einem Klick auf die Schaltfläche *Jetzt einschalten* Vista ganz ohne Ihr Zutun um seinen aktuellen Stand (→ Bild 3.2). Damit werden generell die von Microsoft empfohlenen Standardeinstellungen hergestellt (→ folgende Abschnitte).

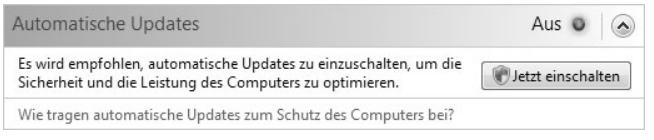


Bild 3.2: Standardeinstellungen können schnell wiederhergestellt werden.

- Da eine Antivirussoftware weiterhin nicht Bestandteil von Windows Vista ist, müssen Sie die Einstellungen des Virenschutzes direkt im jeweiligen Antivirusprogramm ändern, das Sie auf Ihrem Computer installiert haben. Diese Produkte müssen über eine entsprechende Schnittstelle auch dafür sorgen, dass das Sicherheitscenter über die Aktivität des Scanners informiert wird. Das funktioniert zurzeit bei den meisten Scannern, aber nicht bei allen. Sollten Sie noch über keinen Virenscanner verfügen, können Sie auf die Schaltfläche *Programm suchen* in diesem Bereich klicken. Sie werden dann mit einer entsprechenden Website verbunden.
- Für alle Bereiche liefert ein Klick auf den entsprechen Link – beispielsweise *Wie trägt die Firewall zum Schutz des Computers bei?* – recht nützliche Hinweise zur Bedeutung der einzelnen Elemente. Im linken Bereich des Fensters für das *Sicherheitscenter* finden Sie auch Links, über die Sie zu weiteren Seiten wechseln können, die das Thema *Sicherheit* betreffen.

3.1.2 Warnungseinstellungen des Sicherheitscenters ändern

Wenn Ihre im Sicherheitscenter zusammengefassten Einstellungen nicht optimal sind, wird das bereits kurz nach dem Start von Vista durch eine Warnmeldung unten rechts auf dem Desktop gemeldet. Sie können diese Warnungen aber auch ausschalten. Klicken Sie dazu auf den Eintrag *Die Sicherheitscenter-Benachrichtigungsmethode ändern* im linken Bereich des Sicherheitscenters. Das Dialogfeld dazu wird angezeigt (→ Bild 3.3).

- Wir empfehlen Ihnen, es hier bei der Grundeinstellung *Ja, Benachrichtigungen senden und Symbol anzeigen (empfohlen)* zu belassen. Damit werden diese Warnmeldungen angezeigt. Mit *Symbol* ist das kleine Symbol im Infobereich der Taskleiste gemeint. Ändern Sie diese Einstellung nur, wenn Sie einen berechtigten Grund dazu haben. Beispielsweise könnten Sie die Einstellungen zur *Windows Firewall* abschalten, wenn Sie eine externe Firewall benutzen, die Sie separat überwachen.

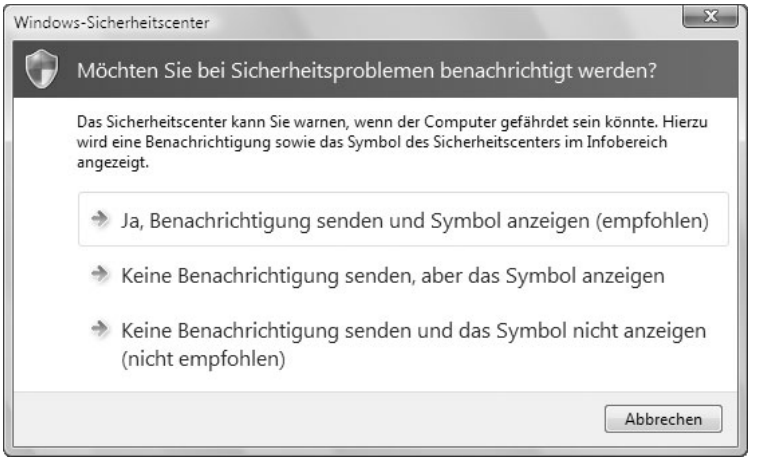


Bild 3.3: Die Warnungseinstellungen konfigurieren

- Wenn Sie eine der beiden darunter angezeigten Optionen wählen, wird der Status von *Firewall*, *Automatische Updates* und *Virenschutz* nach Ausschalten der entsprechenden Warnungen nur noch im Sicherheitscenter selbst angezeigt. Mögliche Probleme führen aber nicht mehr zur Anzeige des Warnhinweises. Durch Ausschalten der Warnungen erhöhen Sie also das Sicherheitsrisiko für Ihren Computer.


TIPP

Vertrauen Sie dem Sicherheitscenter nur im Rahmen gewisser Randbedingungen. Das Werkzeug kann als Dienst deaktiviert werden und der Benutzer merkt nichts davon, da nur dann eine Warnung auftaucht, wenn der Dienst aktiv ist und ein Problem meldet.

3.2 Benutzerkonten einrichten

Durch den ersten Besuch im Sicherheitscenter kennen Sie schon die wesentlichsten Einstellungen zur Basissicherheit. Diese wollen wir jetzt etwas detaillierter durchleuchten. Zunächst sollten Sie sich in diesem Rahmen mit den *Benutzerkonten* beschäftigen. Diese sind besonders dann wichtig, wenn mehrere Personen den Computer verwenden. Beachten Sie die folgenden Grundüberlegungen dazu:

- Wenn Sie für die einzelnen Benutzer des Rechners individuelle Konten erstellen, erhält jeder Benutzer einen eigenen *persönlichen Ordner*, in dem er seine Dokumente ablegen kann, ohne dass diese für andere Benutzer sichtbar werden. Außerdem kann jeder einzelne Benutzer seine Desktopeinstellungen benutzerdefiniert anpassen: Er kann beispielsweise festlegen, wie seine Dateien angezeigt und strukturiert werden sollen, und seine Computereinstellungen und Daten schützen.
- Das direkt bei der Installation des Betriebssystems eingerichtete Konto verfügt automatisch zunächst über Administratorrechte. Wenn Sie weitere Konten definieren, können Sie dafür bestimmte Rechte festlegen. Diese definieren die Aktionen, die ein Benutzer unter Windows ausführen kann. Windows Vista kennt zunächst drei Typen von Benutzerkonten – *Administrator*, *Standardbenutzer* und *Gast*.
- Die Vergabe von individuellen Konten mit bestimmten Rechten für die einzelnen Benutzer eines lokalen Rechners allein liefert nur die eben genannten organisatorischen Vorteile. Ein Mehr an Sicherheit erhalten Sie erst dann, wenn Sie – zumindest für die Konten vom Typ *Administrator* – ein *Kennwort* vergeben. Wenn Sie das nicht tun, können sich auch Benutzer, für die Sie den Kontotyp *Standardbenutzer* vorgesehen hatten, als *Administrator* am Rechner anmelden und dann Dinge tun, die ihnen nicht zustehen. Durch die Vergabe von Kennwörtern für alle Konten – auch die vom Typ *Standardbenutzer* – machen Sie einen ersten Schritt in Richtung einer Erhöhung der Sicherheit gegen unbefugten Zugriff.

Die in diesem Abschnitt gelieferten Hinweise bilden nur den ersten Schritt in Richtung Erhöhung der Sicherheit durch Benutzerkonten und Kennwörter. Mehr zum Thema Sicherheit erfahren Sie auch im folgenden und weiteren Kapiteln dieses Buchs (→ Kapitel 8 und 10).

3.2.1 Kontotypen

Der bei der Installation angegebene Benutzer hat automatisch zunächst die Rechte eines *Administrators*. Das sollten Sie unbedingt beachten, da ein Administrator über alle nur denkbaren Rechte auf dem Computer verfügt. Leider macht Microsoft Sie vielleicht nur ungenügend darauf aufmerksam. Wenn Sie manuell Konten einrichten, haben Sie die Möglichkeit, zwischen den Kontotypen *Administrator* und *Standardbenutzer* zu wählen:

- Das *Administratorkonto* richtet sich an Benutzer, die systemweite Änderungen am Computer vornehmen, Programme installieren und auf alle Dateien auf dem Computer zugreifen dürfen. Der Benutzer eines solchen Kontos kann Benutzerkonten auf dem Computer erstellen und löschen, Kennwörter für andere Benutzerkonten auf dem Computer erstellen oder die Kontonamen, Bilder, Kennwörter und Kontotypen anderer Benutzer ändern. Ein Administrator kann

beispielsweise den Typ eines jeden Kontos hinab- oder heraufstufen. Außerdem kann er den eigenen Kontotyp zu einem *Standardbenutzer*-Konto ändern, sofern mindestens ein weiterer Benutzer mit einem Administratorkonto auf dem Computer vorhanden ist. Dadurch wird sichergestellt, dass immer mindestens ein Benutzer mit einem Administratorkonto auf dem Computer existiert.

- Der Kontotyp *Standardbenutzer* richtet sich an Benutzer, die nicht in der Lage sein sollen, wesentliche Computereinstellungen zu ändern und wichtige Dateien zu löschen. Ein Benutzer mit einem solchen *Standardbenutzer*-Konto kann auf Programme zugreifen, die bereits auf dem Computer installiert sind; er kann jedoch keine Software oder Hardware installieren. Er kann auch das Kontobild erstellen oder ändern sowie sein Kennwort ändern oder löschen. Den Kontonamen oder -typ kann der Benutzer eines *Standardbenutzer*-Kontos hingegen nicht ändern. Diese Art von Änderungen müssen von einem Benutzer mit Administratorrechten ausgeführt werden. Durch Vergabe eines solchen Kontos können Sie also bestimmte Einstellungen des Systems schützen.
- Daneben verfügt Windows Vista über die Möglichkeit, ein *Gastkonto* einzurichten. Ein solches Gastkonto bietet Zugriff auf einen Computer für alle Benutzer, die nicht über ein eigenes Benutzerkonto auf dem Computer verfügen. Das Gastkonto kann nicht mit einem Kennwort belegt werden, sodass sich der Benutzer rasch anmelden kann, um E-Mails zu lesen oder das Internet zu durchsuchen. Ein Gast kann auch auf Programme zugreifen. Ein solches Gastkonto wird standardmäßig eingerichtet, aber nicht aktiviert.

Zum Einrichten oder Ändern von lokalen Benutzerkonten klicken Sie in der *Systemsteuerung* auf *Benutzerkonten*. Anschließend können Sie über die gleichnamige Ebene die wichtigsten Aufgaben ansteuern (→ Bild 3.4). Das im Fenster rechts angezeigte Konto ist das Konto des aktuellen Benutzers.

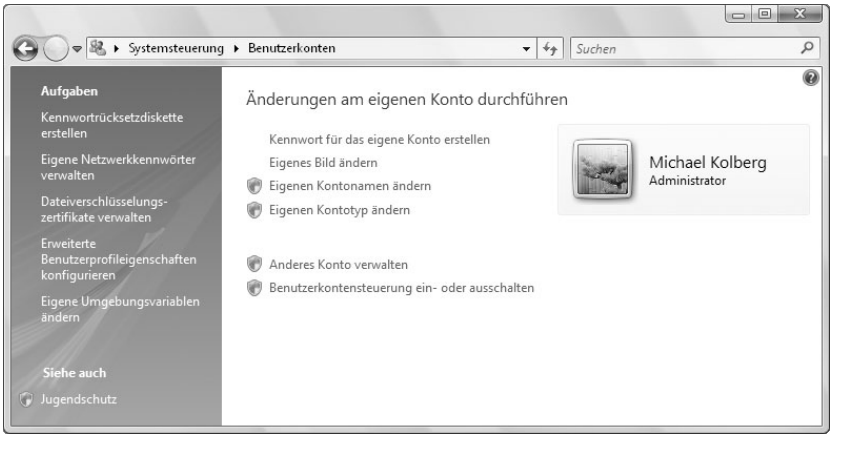


Bild 3.4: Die Benutzerkonten in der Systemsteuerung

3.2.2 Das eigene Konto verwalten

Nach der Installation des Betriebssystems auf dem Rechner ist nur ein Konto vorhanden. Mit den Einstellungen zu diesem Konto sollten Sie sich zuerst beschäftigen. Beachten Sie, dass dieses Konto oft noch nicht geschützt ist. Jeder, der Ihren Computer einschalten kann, kann sich auch unter diesem Namen anmelden und jeden möglichen Unfug mit den Daten treiben.

Ein Kennwort vergeben

Sehr wichtig ist also die Vergabe eines Kennworts für das Konto. Sie fügen dem Computer eine Basisebene für die Sicherheit hinzu. Klicken Sie dazu auf der Ebene *Benutzerkonten* auf *Kennwort für das eigene Konto* erstellen. Die Ebene *Eigenes Kennwort erstellen* wird angezeigt. Darin können Sie ein Kennwort für Ihr Konto festlegen (→ Bild 3.5).

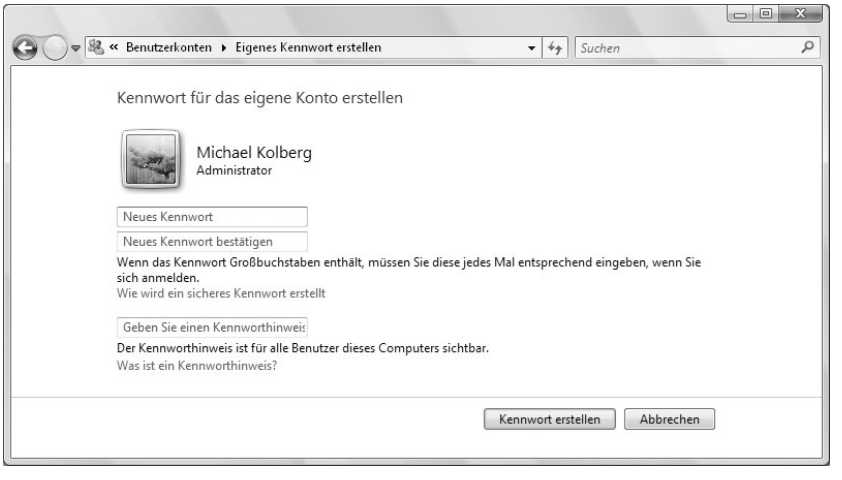


Bild 3.5: Erstellen Sie ein Kennwort für Ihr Konto.

- Das Kennwort muss aus Sicherheitsgründen doppelt eingegeben werden. In der folgenden Eingabezeile müssen Sie das Kennwort also wiederholen. Damit wird die Gefahr eines Tippfehlers bei der Eingabe reduziert.
- Abschließend haben Sie zusätzlich die Möglichkeit, ein Wort oder einen Satz als *Kennworthinweis* einzutragen. Dies dient als eine Art Eselsbrücke, falls das eigentliche Passwort einmal in Vergessenheit gerät. Seien Sie vorsichtig damit: Wenn Sie einen solchen Kennworthinweis erstellen, kann jeder Benutzer des Computers diesen Hinweis auf der Anmeldeseite sehen. Bei einiger Kenntnis der Besonderheiten und Vorlieben der Person kann man durch längeres Ausprobieren das Kennwort meist herausfinden. Eigentlich widerspricht dieser zusätzliche Hinweis der Forderung nach einem sicheren Kennwort.

Bestätigen Sie Ihre Eingaben auf dieser Ebene über *Kennwort erstellen*. Auf der Ebene *Benutzerkonten* wird dann angezeigt, dass das aktuelle Konto *Kennwortgeschützt* ist.

Informationen zu Kennwörtern

Kennwörter stellen im Sicherheitsschema eines Computers oftmals das schwächste Glied dar. Geben Sie hier also nicht einfach ein beliebiges Wort ein, sondern denken Sie sich ein möglichst *sicheres* Kennwort aus. Das ist wichtig, da Werkzeuge zum Knacken von Kennwörtern kontinuierlich weiterentwickelt und auch die dafür verwendeten Computer immer leistungsfähiger werden. Solche Software zum Knacken von Kennwörtern basiert auf einem der folgenden drei Prinzipien: intelligentes Erraten, Wörterbuchangriffe und Automatisierung, durch die alle möglichen Zeichenkombinationen ausprobiert werden. Sofern genügend Zeit zur Verfügung steht, kann durch die letzte Methode jedes Kennwort ermittelt werden. Es kann jedoch immer noch Tage dauern, ein sicheres Kennwort herauszubekommen.

- Ein Kennwort kann Buchstaben, Zahlen und Sonderzeichen (` ~ ! @ # $ % ^ & * ( ) _ + – = { } | [ ] \ : » ; ' < > ? , . oder /) beinhalten. Denken Sie bei der Verwendung von Buchstaben daran, dass Windows Vista bei Kennwörtern die Groß- und Kleinschreibung beachtet. Um die Sicherheit eines Kennworts zu verbessern, sollten mindestens zwei dieser Elemente vorhanden sein: Großbuchstaben, Kleinbuchstaben und Zahlen. Je zufälliger die Reihenfolge der Zeichenkette, desto sicherer ist das Kennwort.
- Das Kennwort kann bis zu 127 Zeichen enthalten. Wenn jedoch in einem Netzwerk auch Computer mit Windows 95 oder Windows 98 eingesetzt werden, sollten Sie Kennwörter verwenden, die nicht mehr als 14 Zeichen umfassen. Anderenfalls kann die Netzwerkanmeldung von diesen Computern aus fehlschlagen.
- Ein sicheres Kennwort umfasst mindestens sieben Zeichen. Aufgrund der Art, in der Kennwörter verschlüsselt werden, umfassen die sichersten Kennwörter bei Windows sieben oder 14 Zeichen. Sichere Kennwörter enthalten Zeichen aus allen drei Gruppen – also Buchstaben (sowohl Groß- und Kleinbuchstaben), numerische Zeichen und Symbole – und es weist mindestens ein Symbolzeichen an zweiter bis sechster Stelle auf. Außerdem sollte es weder Ihren Namen noch Ihren Benutzernamen und auch sonst kein allgemein gebräuchliches Wort oder einen Namen enthalten.
- Komplizierte Kennwörter vergisst man leicht. Ein sinnvoller Trick, dem Gedächtnis etwas nachzuhelfen, besteht in der Verwendung der Anfangsbuchstaben eines Gedichts, Lieds oder anderen Textes. Verwenden Sie sowohl große als auch kleine Buchstaben. Zahlwörter können Sie durch die entsprechenden Ziffern ersetzen, Kommata durch ein Sonderzeichen – beispielsweise *3CmdK/sadSuesw* für *Drei Chinesen mit dem Kontrabass, saßen auf der Straße und erzählten sich was*. Vielleicht finden Sie in dieser Richtung etwas, was Ihnen mehr liegt.

TIPP

Denken Sie daran: Vor einem Einbruch in Ihren Rechner sind Sie nie vollständig sicher. Speichern Sie darum keine Kennwörter in einer Datei auf der Festplatte. Das gilt sowohl für Kennwörter für den Zugang zu Benutzerkonten als auch alle andere Kennwörter. Schreiben Sie sie besser auf ein Stück Papier und verwahren Sie dieses an einem sicheren Ort.

Ein Kennwort ändern

Unter bestimmten Voraussetzungen ist es angebracht, ein vorhandenes Kennwort zu ändern. Wählen Sie dann auf der Ebene *Benutzerkonten* die Option *Eigenes Kennwort ändern*. Das dann angezeigte Dialogfeld entspricht in vielen Punkten dem, das Sie schon vom Erstellen des Kennworts her kennen (→ Bild 3.6 links).

Bild 3.6: Ein Kennwort ändern oder entfernen

Geben Sie im Feld mit der Voreinstellung *Aktuelles Kennwort* das bisher gültige Kennwort ein. In den beiden Zeilen darunter muss das neue Kennwort aus Sicherheitsgründen doppelt eingegeben werden. Beachten Sie die oben genannten Hinweise zu Kennwörtern. Abschließend haben Sie wieder die Möglichkeit, ein Wort oder einen Satz als *Kennworthinweis* einzutragen. Bestätigen Sie durch einen Klick auf *Kennwort ändern*.

Ein Kennwort entfernen

Manchmal werden Sie auch ein Kennwort ganz entfernen wollen – beispielsweise wenn Sie Ihren Rechner verkaufen. Öffnen Sie dazu die Ebene *Benutzerkonten* in der Systemsteuerung und klicken Sie auf *Eigenes Kennwort entfernen*. Geben Sie zunächst das aktuelle Kennwort ein und bestätigen Sie dann mit *Kennwort entfernen* (→ Bild 3.6 rechts). Denken Sie daran, dass das entsprechende Konto danach nicht mehr durch ein Kennwort geschützt ist.

TIPP

Administratoren können die Kennwörter für jedes Konto, andere Benutzer nur die für ihr eigenes Konto löschen.

Eine Kennwortrücksetzdiskette erstellen

Eine *Kennwortrücksetzdiskette* kann auf der Willkommenseite dazu verwendet werden, das Kennwort des eigenen Kontos zurückzusetzen. Dadurch kann der Zugriff auf das eigene Konto wiederhergestellt werden, wenn Sie das Kennwort vergessen haben sollten. Sie müssen als Administrator angemeldet sein, um diese Aufgabe durchführen zu können. Klicken Sie im Fenster für die *Benutzerkonten* unter *Aufgaben* auf der linken Seite des Fensters auf *Kennwortrücksetzdiskette erstellen*. Der *Assistent für vergessene Kennwörter* wird gestartet. Folgen Sie im Assistenten den Anweisungen auf dem Bildschirm:

- Auf der ersten Seite werden Sie begrüßt und über den Zweck des Vorgangs informiert. Beachten Sie: Diese Diskette muss nur einmal erstellt werden und gilt auch dann, wenn Sie das Kennwort später geändert haben. Wenn Sie eine neue Kennwortrücksetzdiskette erstellen, werden die vorher erzeugten ungültig.
- Klicken Sie auf *Weiter*. Sie können dann ein Laufwerk wählen (→ Bild 3.7). In Frage kommen hier nur Diskettenlaufwerke und *USB*-Datenträger.

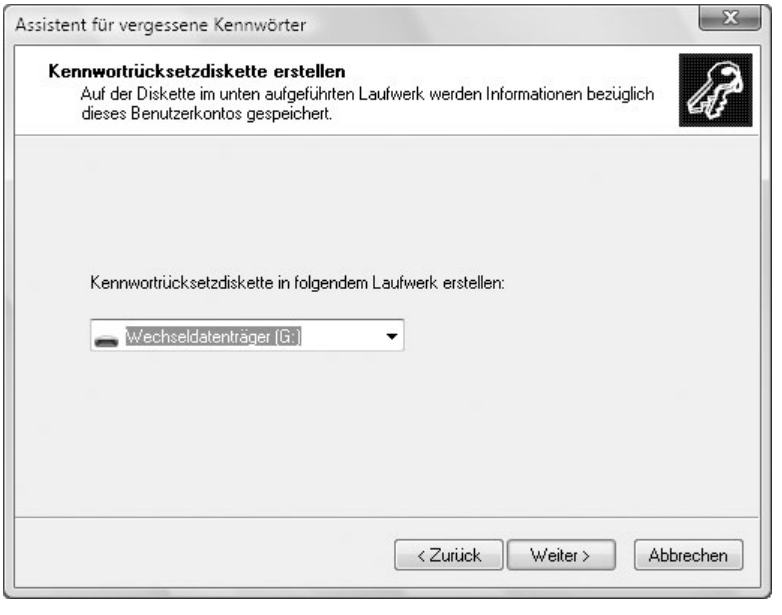


Bild 3.7: Wählen Sie ein Laufwerk.

Zum Einsatz der Kenwortrücksetzdiskette klicken Sie auf der Willkommenseite nach Auswahl Ihres Kontos auf *Haben Sie das Kennwort vergessen?* und folgen Sie den Anweisungen des Kennwortrücksetz-Assistenten, um ein neues Kennwort zu erstellen. Melden Sie sich mithilfe des neuen Kennworts an.

TIPP

Jeder kann die Diskette zum Rücksetzen des Kennworts verwenden und hat damit Zugriff auf das Konto! Nachdem Sie die Diskette erstellt haben, entfernen Sie sie aus dem Laufwerk und bewahren Sie sie an einem sicheren Ort auf.

Den Kontonamen ändern

Wenn Sie den Namen für ein Konto ändern wollen, wählen Sie auf der Ebene *Konto ändern* die Option *Eigenen Kontonamen ändern*. Nach der Zustimmung zur Änderung der Benutzerkonten geben Sie einen neuen Namen ein und bestätigen Sie über *Namen ändern* (→ Bild 3.8 links). Das Konto trägt jetzt den neuen Namen, der bereits auf der Ebene *Benutzerkonten* angezeigt wird.

Das Bild ändern

Unterhalb der Optionen zum Kennwort finden Sie auf der Ebene *Benutzerkonten* noch weitere Optionen, mit denen Sie das verwendete Bild, den Namen des Kontos und seinen Typ ändern können. Nach einem Klick auf *Eigenes Bild ändern* können Sie unter den auf Ihrem System verfügbaren Bilddateien eine auswählen, die dann zusammen mit dem Namen des Kontos auf der Willkommenseite angezeigt wird (→ Bild 3.8 rechts).

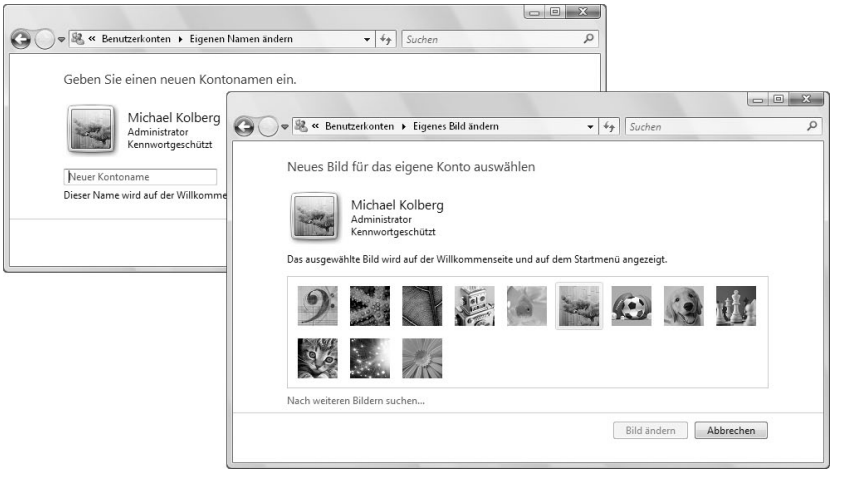


Bild 3.8: Kontonamen und Bild ändern

- Um eines der vorhandenen Standardbilder zu wählen, markieren Sie es. Sie können ein Bild für mehrere Konten verwenden, beispielsweise um nur die unterschiedlichen Kontotypen – *Administrator* und *Standardkonto* – durch verschiedene Bilder zu kennzeichnen.
- Statt eines der Bilder aus der vorgegebenen Auswahl zu verwenden, können Sie auch eine eigene Bilddatei verwenden, die als Grafikdatei auf Ihrem Rechner gespeichert sein muss. Klicken Sie dazu auf die

Schaltfläche *Nach weiteren Bildern suchen*. Der Inhalt des Ordners *Bilder* innerhalb des persönlichen Ordners des aktiven Benutzers wird angezeigt. Sie können auch zu einem anderen Ordner navigieren. An Bildformaten können Sie *.bmp*, *.gif*, *.jpg*, *.png* und *.tif* verwenden. Wählen Sie die zu verwendende Bilddatei und klicken Sie auf *Öffnen*. Das Bild steht danach als weitere Alternative zur Auswahl zur Verfügung.

Klicken Sie nach der Wahl des Bilds auf die Schaltfläche *Bild ändern*.

Den Kontotyp ändern

Eine Option, die Sie wahrscheinlich nie verwenden werden, ist *Eigenen Kontotyp ändern* auf der Ebene *Benutzerkonten*. Sie können sich damit vom Administrator zu einem Standardbenutzer herabstufen (→ Bild 3.9). Dieser Fall tritt wahrscheinlich nur dann ein, wenn Sie von Ihren Angehörigen oder Mitarbeitern entmündigt werden. Beachten Sie gleich, dass mindestens ein Benutzer des Rechners über Administratorrechte verfügen muss.

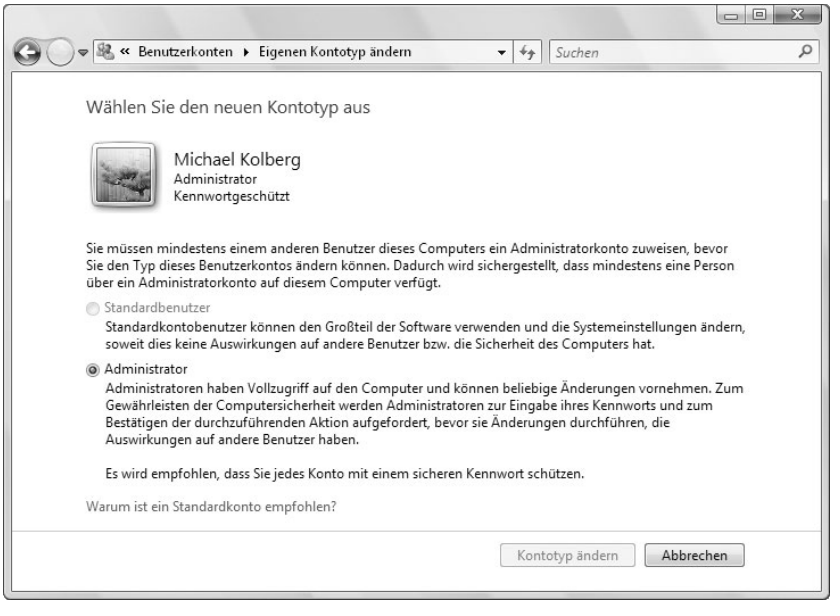


Bild 3.9: Den Typ des Kontos ändern

3.2.3 Weitere Konten

Oben haben wir es schon erwähnt: Wenn mehrere Benutzer einen Computer verwenden, sollten Sie generell für jeden Benutzer ein eigenes Konto einrichten. Damit können zunächst einmal alle Benutzer des Rechners eine komplette eigene Benutzeroberfläche aufbauen. Dadurch stören sie niemand anderen durch Änderungen am Desktop. Außerdem entfallen Überlegungen zur Frage, wo die Dateien der einzelnen Benutzer gespeichert werden sollen, da jeder Benutzer über einen eigenen *persönli-*

chen Ordner verfügt, in dem sowohl seine Dokumente als auch seine Einstellungen für das Betriebssystem und die darunter laufenden Anwendungsprogramme gespeichert werden. Sie sollten daher für jeden Benutzer des Rechners ein eigenes Konto einrichten. Verwenden Sie möglichst generell den Typ *Standardkonto*, der den Benutzern die Installation von Software und die Änderung von Systemeinstellungen ermöglicht, die sich nicht auf andere Benutzer oder die Sicherheit des Computers auswirken. Vergeben Sie nur dann die Rechte eines Administrators, wenn Sie sich über die Eignung des Benutzers für eine solche Aufgabe im Klaren sind.

Auch wenn sich bei Windows Vista durch die Einführung der *Benutzerkontensteuerung* hinsichtlich der Sicherheit einiges getan hat, könnte theoretisch das Arbeiten mit Administratorrechten am Rechner immer noch ein Risiko darstellen. Es empfiehlt sich darum, für eine normale Sitzung am Rechner immer ein Konto des Typs *Standardbenutzer* zu verwenden. Fügen Sie daher auch für sich selbst ein solches Konto hinzu.

Neue Konten erstellen

Um ein neues Benutzerkonto zu erstellen, klicken Sie auf der Ebene *Benutzerkonten* auf die Schaltfläche *Anderes Konto verwalten*. Nach der üblichen Zustimmung wird ein weiteres Dialogfeld angezeigt, in dem Sie oben dem Konto einen Namen geben können (→ Bild 3.10).

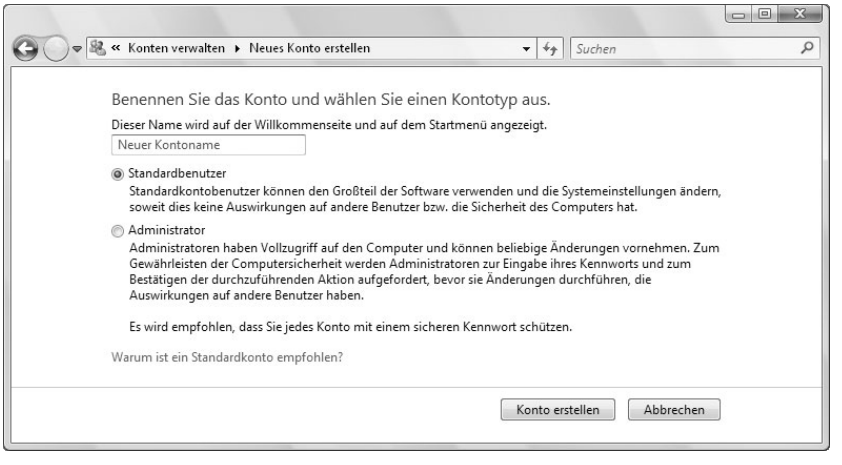


Bild 3.10: Erstellen Sie ein neues Konto

- Im Textfeld mit der Voreinstellung *Neuer Kontoname* geben Sie dem Konto einen Namen. Ein solcher Benutzername darf mit keinem anderen Benutzer- oder Gruppennamen auf dem verwalteten Computer identisch sein. Er kann aus bis zu 20 Klein- oder Großbuchstaben und Zeichen bestehen. Nicht verwendet werden dürfen die folgenden Zeichen: « / \ [ ] : ; | = , + * ? < und >. Außerdem darf ein

Benutzername nicht ausschließlich aus Punkten oder Leerzeichen bestehen. Dieser Name wird später auf der Willkommenseite und – nach der Wahl dieses Kontos – im Startmenü angezeigt

- Darunter können Sie den Typ des neuen Kontos festlegen. Verwenden Sie *Administrator* oder *Standardbenutzer*. Das oben schon angesprochene Konto *Gast* wurde automatisch eingerichtet, muss aber zum Gebrauch noch aktiviert werden.

Klicken Sie nach Eingabe des Namens und der Wahl des Typs auf die Schaltfläche *Konto erstellen*. Das neue Konto wird zusammen mit einem automatisch gewählten Bild auf der Ebene *Konto verwalten* hinzugefügt (→ Bild 3.11). Sie sollten dann gleich noch weitere Einstellungen zu diesem neuen Konto vornehmen – absolut notwendig ist die Vergabe eines Kennworts.

Bild 3.11: Ein neues Konto wurde erstellt.

Nach dem Einrichten eines neuen Kontos und der Anmeldung unter diesem findet der Benutzer dieses Kontos den Windows-Desktop in der Form vor, die Sie noch vom ersten Starten nach der Installation her kennen. Verwendet wird das Standarddesign von Vista: Bis auf den Papierkorb befinden sich auf dem Desktop keine Symbole und die Schnellstartleiste als Element der Taskleiste ist deaktiviert. Die Programme, die vor dem Einrichten des neuen Kontos auf dem vorher vorhandenen Administratorkonto bereits installiert waren, sind im neuen Konto automatisch zugänglich. Es fehlen aber vorher individuell angelegte Verknüpfungen dazu auf dem Desktop. Der Benutzer oder der Administrator muss die gewünschten persönlichen Einstellungen noch vornehmen.

Die Einstellungen für die neuen Konten ändern

Wenn Sie gerade ein neues Konto erstellt haben, können Sie gleich mit den folgenden Schritten fortfahren. Anderenfalls müssen Sie erst wieder die Ebene der *Benutzerkonten* auswählen und dort auf *Anderes Konto verwalten* klicken. Klicken Sie dann in beiden Fällen auf den Namen des Kontos, für das Sie Änderungen durchführen möchten. Die Ebene *Konto ändern* wird angezeigt. Darin müssen Sie festlegen, was am Konto geändert werden soll (→ Bild 3.12). Welche Einstellungen geändert werden können, hängt vom Typ des Kontos des aktuellen Benutzers ab.

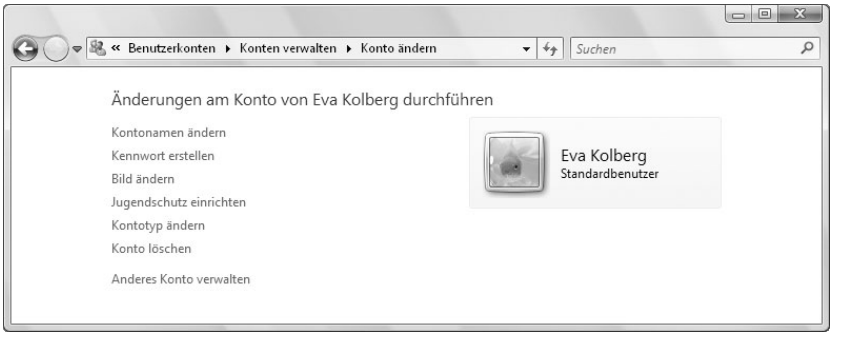


Bild 3.12: Das Konto ändern

Um diese Einstellungen festzulegen, gehen Sie im Prinzip genauso vor, wie oben für die Einstellungen am eigenen Konto beschrieben:

- Wenn Sie den Namen für ein Konto ändern wollen, wählen Sie auf der Ebene *Konto ändern* die Option *Kontonamen ändern*. Geben Sie einen neuen Namen ein und bestätigen Sie über *Namen ändern*. Das Konto trägt jetzt den neuen Namen, der bereits auf der Ebene *Konto ändern* angezeigt wird.
- Nach der Wahl von *Kennwort erstellen* können Sie ein Kennwort für das vorher gewählte Konto festlegen. Administratoren können die Kennwörter für jedes Konto, andere Benutzer nur die für ihr eigenes Konto löschen. Achten Sie dabei wieder darauf, dass das System zwischen Groß- und Kleinbuchstaben unterscheidet. Um die Sicherheit eines Kennworts zu verbessern, sollten Sie dafür einen Mix aus Großbuchstaben, Kleinbuchstaben und Zahlen wählen. Je zufälliger die Reihenfolge der Zeichenkette, desto sicherer ist das Kennwort. Das Kennwort muss aus Sicherheitsgründen doppelt eingegeben werden. Zusätzlich kann ein Kennworthinweis als Gedankenstütze hinzugefügt werden. Es wurde oben schon gesagt: Dieser Hinweis ist für alle Benutzer des Computers auf der Willkommenseite sichtbar. Bestätigen Sie anschließend durch einen Klick auf *Kennwort erstellen*.
- Wenn Sie ein bereits vergebenes Kennwort wieder entfernen wollen, klicken Sie auf *Kennwort entfernen* auf der Ebene *Konto ändern*.

- Nach einem Klick auf *Bild ändern* können Sie unter den auf Ihrem System verfügbaren Bilddateien eine auswählen, die dann zusammen mit dem Namen des Kontos auf der Willkommenseite angezeigt wird. Um eines der vorhandenen Standardbilder zu wählen, markieren Sie es. Statt eines der Bilder aus der vorgegebenen Auswahl zu verwenden, können Sie auch eine eigene Bilddatei verwenden, die als Grafikdatei auf Ihrem Rechner gespeichert sein muss. Klicken Sie nach der Wahl des Bilds auf die Schaltfläche *Bild ändern*.

Den Jugendschutz einrichten

Der Jugendschutz gehört eigentlich nicht zum Programmumfang der Version Business von Windows Vista. Vielleicht sind Sie aber trotzdem daran interessiert. Um eine Einstellung dafür für ein Konto zu wählen, klicken Sie auf der Ebene *Konto ändern* auf die Option *Jugendschutz einrichten*. Damit wechseln Sie zur Ebene *Jugendschutz* innerhalb der Systemsteuerung, die Sie auch direkt über die Systemsteuerung ansprechen können. Nach der Bestätigung müssen Sie wählen, für welches Konto Sie den Jugendschutz einrichten wollen. Klicken Sie dazu auf das gewünschte Konto. Anschließend wird die Ebene *Benutzersteuerungen* zu *Jugendschutz* angezeigt (→ Bild 3.13). Standardmäßig ist der Jugendschutz für alle Konten zunächst ausgeschaltet. Zum Aktivieren für das ausgewählte Konto klicken Sie auf die Option *Ein – Einstellungen erzwingen*. Die restlichen Optionen im Dialogfeld sind dann verfügbar. Ebenfalls ist die Option *Ein – Informationen über Computernutzung sammeln* unter *Aktivitätsberichterstattung* standardmäßig aktiviert.

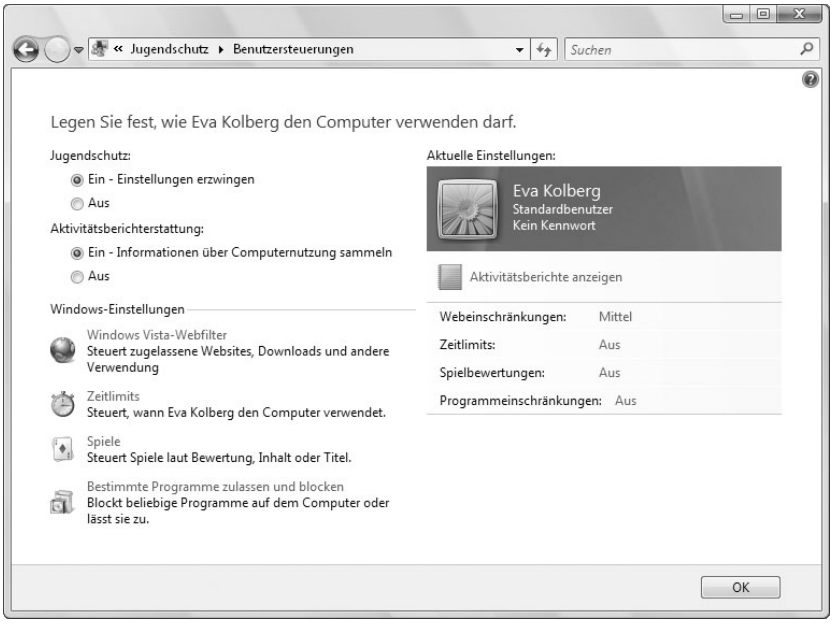


Bild 3.13: Die Einstellungen für den Jugendschutz

Sie müssen anschließend noch die Einstellungen für den *Windows Vista-Webfilter*, die *Zeitlimits*, die erlaubten *Spiele* und die Option *Bestimmte Programme zulassen oder blocken* vornehmen. Beispielsweise wird nach einem Klick auf *Windows Vista-Webfilter* ein Fenster angezeigt, über das Sie regeln können, welche Bereiche im Internet besucht werden dürfen (→ Bild 3.14).

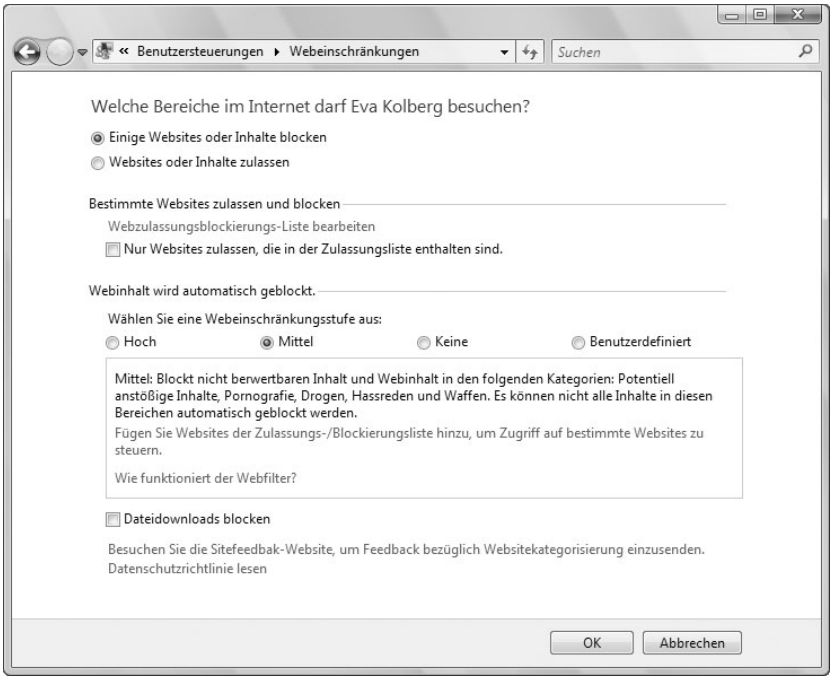


Bild 3.14: Die zugelassenen Bereiche im Internet steuern

- Standardmäßig ist *Einige Websites oder Inhalte blocken* aktiviert. Sie können damit die Einstellungen im unteren Bereich des Fensters benutzen, um die Einschränkungen zu formulieren. Wenn Sie später *Websites oder Inhalte zulassen* einschalten, bleiben die definierten Einschränkungen zwar gespeichert, sie sind aber nicht mehr wirksam.
- Nach einem Klick auf *Webzulassungsblockierungs-Liste bearbeiten* wird ein neues Fenster geöffnet, in dem Sie *Zugelassene Websites* und *Geblockte Websites* eingeben können. Geben Sie dort die Adressen im Feld *Websiteadresse* ein und bestätigen Sie jeweils über *Zulassen* oder *Blocken*. Schließen Sie die Liste abschließend durch einen Klick auf *OK*.
- Wenn Sie die Option *Nur Websites zulassen, die in der Liste enthalten sind* aktivieren, erreichen Sie, dass der Benutzer nur noch die Adressen ansteuern kann, die in der Liste *Zulassen* aufgeführt sind. Ist diese Option nicht aktiviert, können zwar die in der Liste *Blocken* aufgeführten Sites nicht besucht werden, wohl aber alle anderen Adressen im Internet.

- Über die Optionen im Bereich *Webinhalt wird automatisch geblockt* können Sie eine Stufe wählen, die auf Basis der in der Website vorhandenen Inhalte einzelne Seiten vom Besuch ausschließt.

Bestätigen Sie Ihre Einstellungen abschließend durch einen Klick auf *OK*.

Kontotyp ändern

Ein Administrator kann den Typ eines jeden Kontos hinab- oder heraufstufen, auch seines eigenen. Allerdings muss immer mindestens ein Administratorkonto auf dem lokalen System vorhanden sein (→ Bild 3.15).

Bild 3.15: Einen neuen Kontotyp auswählen

Das Konto löschen

Sie müssen beim Löschen eines Kontos entscheiden, ob Sie die vom bisherigen Kontoinhaber erstellten Dateien beibehalten oder löschen wollen. Details zu den in Frage kommenden Dateien finden Sie im Dialogfeld (→ Bild 3.16). Bestätigen Sie dementsprechend.

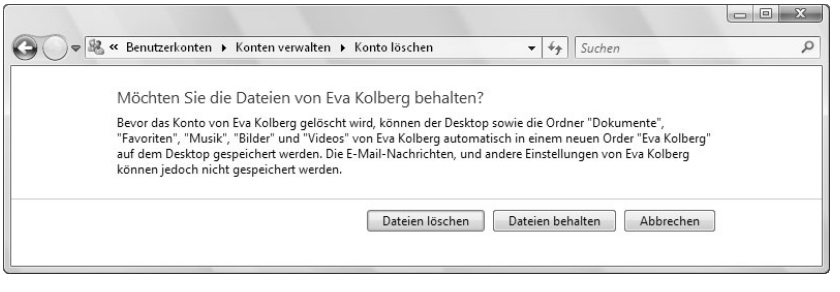


Bild 3.16: Ein Konto löschen

Das Gastkonto aktivieren

Über ein Gastkonto bieten Sie Personen, die über kein eigenes Konto auf dem System verfügen, die Möglichkeit zum Arbeiten auf dem System. Ein Gast kann keine Änderungen an Hard- und Software oder am Kontotyp vornehmen, darf aber das zugeordnete Bild ändern. Für das Gastkonto kann auch kein Kennwort vergeben werden. Standardmäßig ist nach der Installation bereits ein Gastkonto eingerichtet, dieses ist aber nicht aktiviert. Zum Aktivieren dieses Kontos wählen Sie *Benutzerkonten* in der *Systemsteuerung* und *Anderes Konto verwalten*. Klicken Sie auf *Gast*. Bestätigen Sie dann über *Einschalten* (→ Bild 3.17). Auf der Willkommenseite wird ein Symbol für den Zugang als Gast angezeigt.

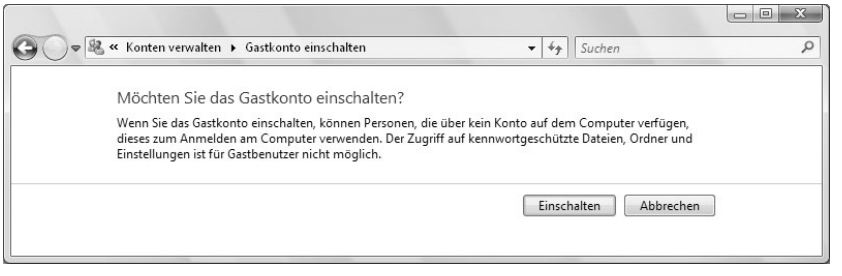


Bild 3.17: Möchten Sie das Gastkonto einschalten?

Zum Ändern oder Löschen des Gastkontos verwenden Sie wiederum die Option *Gast* auf der Ebene *Anderes Konto verwalten*.

3.2.4 Konsequenzen bei der Verwendung von Benutzerkonten

Bevor wir im folgenden Abschnitt noch etwas tiefer in die Arbeit mit Benutzerkonten einsteigen, wollen wir noch einmal kurz zusammenfassen, was Sie durch das Einrichten einzelner Konten bisher erreicht haben:

- Wenn Sie Ihren Rechner einschalten, wird zunächst die *Willkommenseite* angezeigt, auf der die definierten Konten aufgelistet werden. Klicken Sie auf die Schaltfläche für das Konto, unter dem Sie sich anmelden möchten.
- Hatten Sie – hoffentlich – ein Kennwort für dieses Konto vergeben, müssen Sie dieses nach der Wahl des Kontos eingeben und über ↵ oder einen Klick auf die Schaltfläche mit dem Pfeil bestätigen. Bei einem falschen Kennwort wird unterhalb des Felds für das Kennwort der *Kennworthinweis* eingeblendet, der Ihnen helfen kann, sich an das Kennwort zu erinnern.
- Auch die Befehle zum *Benutzer wechseln* und zum *Abmelden* im Menü *Start* sind jetzt vernünftig einsetzbar (→ Kapitel 2). Beide Optionen zeigen die *Willkommenseite* an, auf der sich ein Benutzer erneut am Rechner anmelden kann. Ein neuer Benutzer muss sich gegebenenfalls mit seinem Kennwort anmelden, falls das Konto ein solches verlangt.

- Wenn Sie nach der Anmeldung als Administrator eine administrative Aufgabe ausführen möchten – wie beispielsweise die Installation eines neuen Programms –, werden Sie wie gewohnt von Windows Vista zur Bestätigung aufgefordert. Versucht ein als *Standardbenutzer* angemeldeter Benutzer eine solche administrative Aufgabe auszuführen, wird von ihm die Eingabe eines gültigen Administratorkennworts verlangt. Wenn er über ein solches verfügt, kann er nach der Bestätigung die administrative Aufgabe ausführen.
- Sie können aber auch Programme als Administrator starten, wenn Sie nicht als solcher angemeldet sind, beispielsweise um Verwaltungsaufgaben durchzuführen. Markieren Sie dazu die entsprechende Programmdatei und wählen Sie *Als Administrator ausführen* aus dem Kontextmenü, das Sie durch einen Klick auf die rechte Maustaste anzeigen lassen (→ Bild 3.18). Es muss dann wiederum ein gültiges Administratorkennwort eingegeben und bestätigt werden.

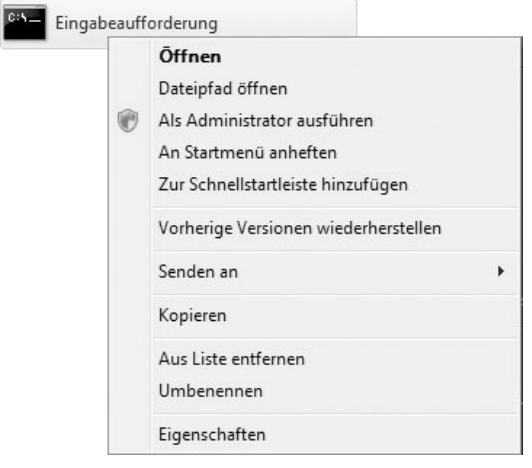


Bild 3.18: Das Kontextmenü erlaubt den Wechsel zu einem Administratorkonto.

3.2.5 Erweiterte Kontokontrolle und -verwaltung

Windows Vista gibt Ihnen die Möglichkeit, die verschiedenen Benutzer mit Zugriff auf die Ressourcen des lokalen Computers zentral anzuzeigen und zu verwalten.

Alle Benutzerkonten anzeigen

Über die Eingabeaufforderung können Sie recht einfach überprüfen, welche Benutzerkonten auf Ihrem Rechner unter Windows Vista eingerichtet wurden. Öffnen Sie das Programm *Alle Programme/Zubehör/Eingabeaufforderung*, geben Sie *net user* ein und bestätigen Sie mit ↵. Es erscheint eine Liste aller Benutzer, die Zugriff auf Ihr System haben könnten (→ Bild 3.19).

Bild 3.19: Die Benutzer werden angezeigt.

Neben den von Ihnen gezielt eingerichteten Konten finden Sie auf allen mit Windows Vista betriebenen Rechnern auch ein nur mit *Administrator* bezeichnetes Konto mit Administratorenrechten. Microsoft hat diese etwas erschwerte Zugangsmöglichkeit geschaffen, um Ihnen auch dann noch den Zugriff auf Ihr System zu ermöglichen, wenn Sie einmal alle Kennwörter vergessen haben sollten. Auch wenn Sie alle offensichtlichen Benutzerkonten durch Kennwörter abgesichert haben, lässt Windows Vista also immer noch eine Hintertür offen, über die sich ein etwas erfahrener Anwender Zugang zum lokalen System verschaffen kann.

Die erweiterte Kontrolle

Für eine erweiterte Kontrolle der Konten können Sie auch ein anderes verstecktes Programm benutzen. Starten Sie wieder die Eingabeaufforderung über *Alle Programme/Zubehör/Eingabeaufforderung*, geben Sie *control userpasswords2* ein und bestätigen Sie mit ↵. Klicken Sie dann auf die blinkende Anzeige *Systemsteuerung* in der Taskleiste. Im Dialogfeld *Benutzerkonten* finden Sie auf der Registerkarte *Benutzer* eine Liste mit (fast) allen definierten Benutzerkonten und die dafür zugewiesenen Rechte (→ Bild 3.20 links).

Sie können auch an dieser Stelle neue Konten hinzufügen und bei bereits vorhandenen die Eigenschaften ändern oder diese löschen:

- Um ein weiteres Konto zu erstellen, klicken Sie auf der Registerkarte *Benutzer* die Schaltfläche *Hinzufügen* an. Die gewünschten Daten geben Sie dann über einen Assistenten ein.
- Nachdem Sie ein Konto in der Liste markiert haben, können Sie durch einen Klick auf die Schaltfläche *Eigenschaften* die dafür gesetzten Parameter anzeigen lassen.
- Interessant ist hier auch die Registerkarte *Gruppenmitgliedschaft*. Zusätzlich zu den weiter vorne in diesem Kapitel genannten Kontotypen *Administrator* und *Standardbenutzer* finden Sie auf der letzten Seite dieses Assistenten noch eine mit *Andere* bezeichnete Liste, aus der Sie einen anderen Kontotyp wählen können.

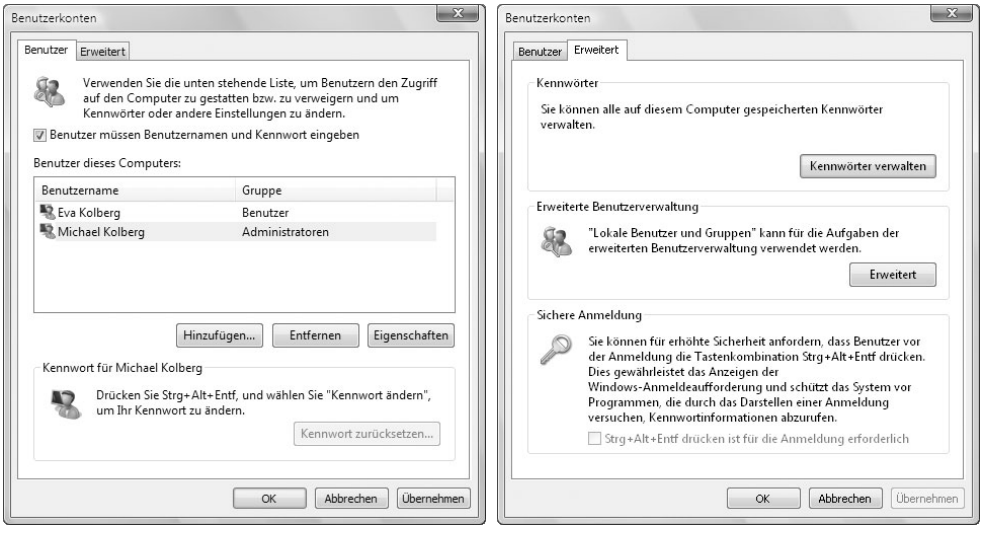


Bild 3.20: Die Konten werden aufgelistet.

Die sichere Anmeldung verwenden

Auf der Registerkarte *Erweitert* des eben angesprochenen Dialogfelds zum Programm *control userpasswords2* finden Sie unter *Sichere Anmeldung* die Option *Strg+Alt+Entf drücken ist für die Anmeldung erforderlich* (→ Bild 3.20 rechts). Wenn Sie diese Option aktivieren, wird der Benutzer in einem separaten Dialogfeld vor der eigentlichen Anmeldung aufgefordert, die Tastenkombination Strg + Alt + Entf zu drücken. Diese Tastenkombination wird nur von Windows anerkannt. Diese *sichere Anmeldung* bietet eine zusätzliche Sicherheitsstufe für den Computer, indem erreicht wird, dass der echte Windows-Anmeldebildschirm angezeigt wird. Dies erhöht die Sicherheit und dient dem Schutz vor trojanischen Pferden, da diese Ihren Benutzernamen und Ihr Kennwort bei der Eingabe nicht mehr abfangen können.

TIPP

Durch einen Klick auf die Schaltfläche *Erweitert* in der Registerkarte *Erweitert* öffnen Sie das Dialogfeld *Lokale Benutzer und Gruppen*. Darin können Sie die Berechtigungen überprüfen und ändern, die die Zugriffsebene bestimmen, über die ein Benutzer für diesen Computer verfügt.

Ein schneller Zugang

Hoch gesetzte Sicherheitsregeln nützen wenig, wenn man sie aus Bequemlichkeit nicht nutzt. Wenn Sie beispielsweise den oben genannten Ratschlag beherzigen, sich neben Ihrem Administratorkonto auch noch ein *Standardbenutzer*-Konto für den alltäglichen Gebrauch anzulegen, ist beim Starten des Rechners die Versuchung groß, gleich das Administratorkonto zu benutzen. Sie können bei mehreren eingerichteten Konten die gesamte Anmeldeprozedur umgehen und sich automatisch mit Standardbenutzerrechten anmelden lassen.

Um eine solche Konfiguration einzurichten, markieren Sie auf der Registerkarte *Benutzer* in der Liste *Benutzer dieses Computers* das Konto, unter dem die automatische Anmeldung erfolgen soll. Deaktivieren Sie dann das Kontrollkästchen *Benutzer müssen Benutzernamen und Kennwort eingeben*. Klicken Sie dann auf *OK*. Anschließend wird der Name des Kontos angezeigt, an dem die Anmeldung automatisch erfolgen soll (→ Bild 3.21). Geben Sie zweimal das erforderliche Kennwort ein und bestätigen Sie dann mit *OK*.

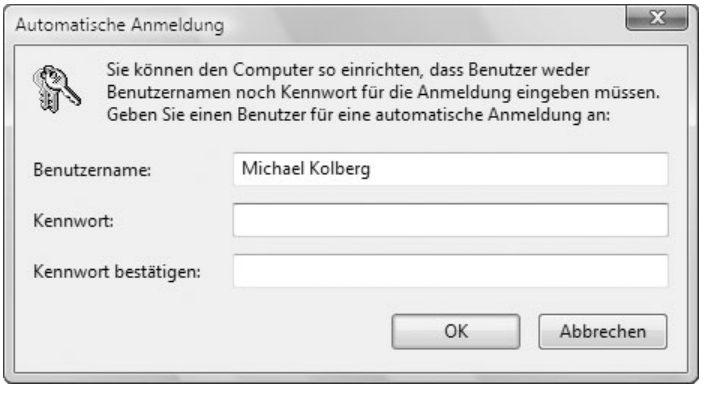


Bild 3.21: Sie können direkt mit einem Standardbenutzerkonto hochfahren.

Wenn Sie dann den Rechner neu starten, wird automatisch das vorher markierte Konto angemeldet. Um von dort aus zu einem anderen Konto zu wechseln, wählen Sie *Abmelden/Benutzer wechseln* im Startmenü oder drücken Sie Win+L.

Um diese Konfiguration wieder abzuschalten, müssen Sie *control userpasswords2* erneut aufrufen und das Kontrollkästchen *Benutzer müssen Benutzernamen und Kennwort eingeben* aktivieren.

Schutz bei kurzer Abwesenheit

Sobald – auch nur theoretisch – mehrere Personen Zugang zum Rechner haben, kann auch eine kurze Abwesenheit – um beispielsweise eine Tasse Kaffee zu holen – zu einem Sicherheitsrisiko führen. Zum Thema *Grundsicherung* gehören deswegen auch einige Hinweise zu den Möglichkeiten, den Rechner bei einer kurzen Abwesenheit vom Arbeitsplatz gegen einen Fremdzugriff über Tastatur und Maus zu sperren:

- Als erste Alternative dafür bietet sich der Bildschirmschoner an. Die Einstellungen erreichen Sie über den Unterpunkt *Bildschirmschoner* im Fenster zum Modul *Anzeige* in der *Systemsteuerung* (→ Kapitel 5). Stellen Sie auf jeden Fall sicher, dass die Option *Anmeldeseite bei Reaktivierung* eingeschaltet ist. Ansonsten wirkt der Bildschirmschoner nicht als Sperre und jeder, der die Maus bewegt oder eine Taste drückt, kann auf das Konto zugreifen. Die Eintragung im Feld *War-*

tezeit ist etwas problematisch: Einerseits sollte der Bildschirmschoner möglichst schnell erscheinen, andererseits kann ein andauerndes Auftauchen während der Arbeit schnell nervig werden.

- Besser ist es, den Rechner auch bei kurzer Abwesenheit zu sperren oder in den Ruhezustand zu versetzen. Der Ruhezustand schafft natürlich keine zusätzliche Sicherheit, erspart Ihnen aber das Speichern und spätere Öffnen der gerade aktiven Dokumente, was einen manchmal von einem Ausschalten des Rechners abhält. Wenn Sie den Computer später wieder starten, stehen alle Programme mit allen Daten in derselben Form wieder zur Verfügung, wie Sie sie vorher geöffnet hatten. Es kann sich lohnen, sich diese Verfahrensweise generell anzugewöhnen.

Die Benutzerkontensteuerung abschalten

Abschließend wollen wir noch auf einen Punkt eingehen, den Sie aber besser gleich wieder vergessen sollten: Sie können die Benutzerkontensteuerung abschalten. Dazu klicken Sie zunächst auf der Ebene *Benutzerkonten* auf die *Benutzerkontensteuerung ein- und ausschalten*. Im dann angezeigten Fenster können Sie die Option *Verwenden Sie die Benutzerkontensteuerung …* deaktivieren (→ Bild 3.22). Wenn Sie das tun, bemerken Sie zunächst einmal nichts von der Änderung. Sie müssen sich weiterhin – auch mit einem Kennwort – anmelden. Die Kontrollfunktion, die es einem nicht als Administrator angemeldeten Benutzer verbietet, bestimmte Änderungen am Rechner durchzuführen, ist aber abgeschaltet! Widerstehen Sie der Versuchung, auf diese Weise die Bedienung von Vista zu vereinfachen.

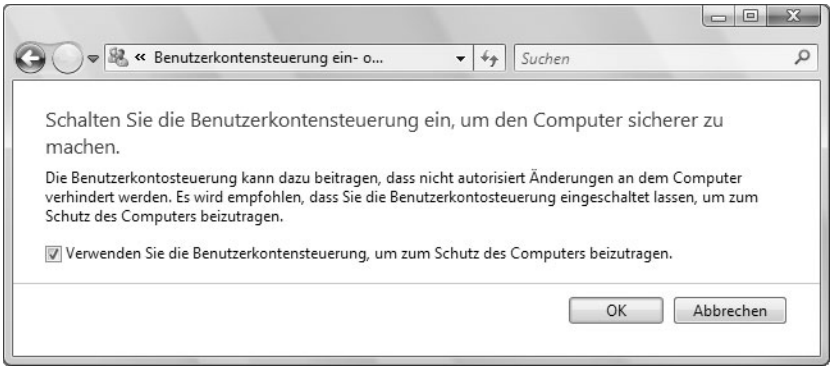


Bild 3.22: Sie können die Benutzerkontensteuerung abschalten.

3.3 Updates regeln

Hinsichtlich des Themas Sicherheit sollten Sie sich auch gleich darüber Gedanken machen, wie Sie es mit den für die Zukunft zu erwartenden Updates halten möchten. Um den Bereich zur Regelung dieser Frage zu betreten, doppelklicken Sie in der *Systemsteuerung* auf *Windows Update*. Sie können auch auf den gleichnamigen Link im linken Bereich

des *Windows-Sicherheitscenters* klicken oder das Programm *Windows Update* im Bereich *Alle Programme* des Startmenüs verwenden. Im dann angezeigten Fenster finden Sie in der Spalte links den Zugang zu mehreren Unterbereichen, über die Sie die gewünschten Einstellungen regeln können (→ Bild 3.23).

Bild 3.23: Der Bereich *Windows Updates* in der Systemsteuerung

- Wenn Sie über keine permanente Verbindung zum Internet verfügen, klicken Sie im linken Bereich auf *Nach Updates suchen* und warten Sie, bis Windows die neuesten Updates für den Computer gefunden hat.
- Falls neue Updates gefunden wurden, klicken Sie auf *Updates installieren*. Wenn Sie aufgefordert werden, ein Administratorkennwort oder eine Bestätigung einzugeben, geben Sie das Kennwort bzw. die Bestätigung ein.


TIPP

Im unteren Bereich finden Sie unter Umständen eine Schaltfläche mit der Bezeichnung *Updates für weitere Produkte*. Ein Klick darauf verbindet Sie zunächst mit der Seite *Microsoft Update* im Internet. Darin stehen Ihnen beispielsweise Downloads für Office und andere Microsoft-Programme zur Verfügung, mit denen Sie den Computer auf dem neuesten Stand halten. Folgen Sie den Anweisungen auf dieser Seite und klicken Sie gegebenenfalls auf *Installieren*. Die Verwendung von Microsoft Update unterliegt den Nutzungsbedingungen. Besuchen Sie außerdem die Website des jeweiligen Herausgebers oder Herstellers, um nach Updates für andere Softwareprogramme und Geräte zu suchen.

3.3.1 Die Einstellungen für Updates festlegen

In Windows Vista steht Ihnen standardmäßig die Möglichkeit automatischer Updates zur Verfügung. Sie bestimmen dabei aber selbst, auf welche Weise und wann der Computer von Windows aktualisiert wird. Um

die Einstellungen für den Erhalt von Updates zu regeln, klicken Sie im linken Bereich des Fensters für *Windows-Update* auf *Einstellungen ändern*. Im dann angezeigten Fenster gleichen Namens finden Sie vier Optionen (→ Bild 3.24).

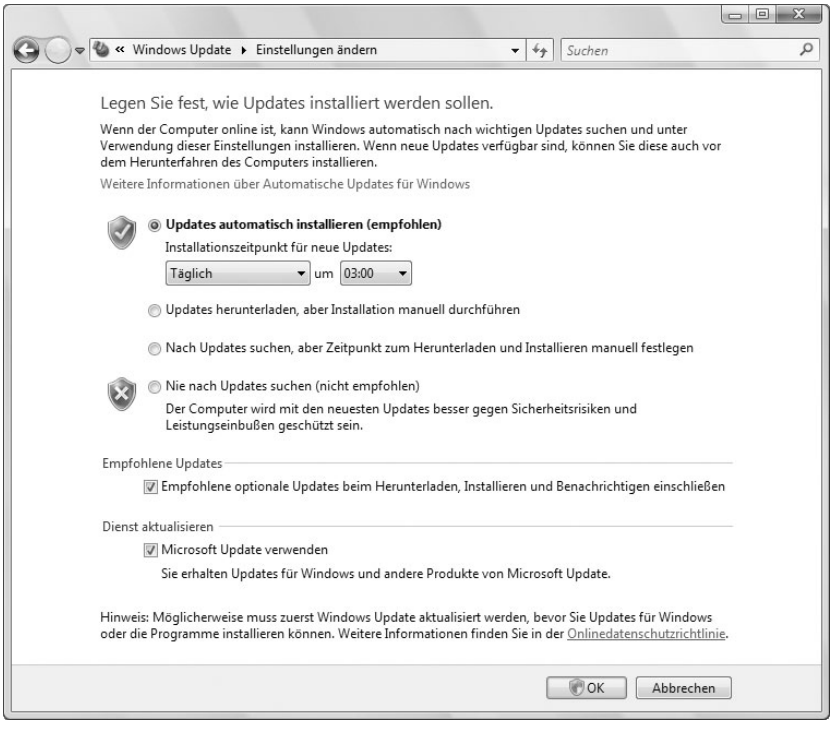


Bild 3.24: Die Einstellungen zu den Updates festlegen

- Bei der Wahl der automatisch eingestellten Option *Updates automatisch installieren (empfohlen)* können Sie den Tag und den Zeitpunkt festlegen, an dem Updates von Windows installiert werden sollen. Wenn Sie diese Option wählen, müssen Sie bei Auswahl des Tages und der Uhrzeit beachten, dass der Computer zum angegebenen Zeitpunkt eingeschaltet ist, damit der Installationsvorgang abgeschlossen werden kann. Die für Ihren Computer geeigneten Updates werden dann gesucht und im Hintergrund heruntergeladen. Hier findet während dieses Vorgangs keine Benachrichtigung statt und Sie werden in Ihrer Arbeit nicht unterbrochen. Nachdem der Download abgeschlossen ist, wird im Infobereich eine Meldung angezeigt, sodass Sie prüfen können, für welche Updates die Installation geplant ist. Wenn Sie sich entschließen, die Installation nicht sofort durchzuführen, startet Windows die Installation gemäß dem von Ihnen festgelegten Zeitplan. Die Installation wird jedoch zum Zeitpunkt der geplanten Installation durchgeführt, unabhängig davon, welcher Benutzer zu dieser Zeit am Computer angemeldet ist.

- Bei Aktivierung von *Updates herunterladen, aber Installation manuell durchführen* werden die für Ihren Computer geeigneten Updates von Windows gesucht und im Hintergrund heruntergeladen. Während dieses Vorgangs findet keine Benachrichtigung statt und Sie werden in Ihrer Arbeit nicht unterbrochen. Nachdem der Download abgeschlossen ist, wird ein Symbol im Infobereich angezeigt und Sie werden in einer Meldung darüber informiert, dass die Updates auf dem Computer installiert werden können. Wenn Sie die verfügbaren Updates anzeigen und installieren möchten, klicken Sie auf das Symbol oder auf die Meldung. Anschließend können Sie die entsprechenden Updates auswählen, die auf dem Computer installiert werden sollen. Wenn Sie sich entschließen, ein bestimmtes heruntergeladenes Update nicht zu installieren, löscht Windows die zugehörigen Dateien vom Computer. Falls Sie Ihre Meinung später ändern, müssen Sie das Update erneut herunterladen. Klicken Sie dazu auf der Registerkarte *Automatische Updates* auf *Abgelehnte Updates*. Wenn die zuvor abgelehnten Updates weiterhin für den Computer geeignet sind, werden sie angezeigt, sobald Windows Sie das nächste Mal über verfügbare Updates informiert.
- Mit der Option *Nach Updates suchen, aber Zeitpunkt zum Herunterladen und Installieren selbst festlegen* bewirken Sie Folgendes: Wenn eine Verbindung zum Internet besteht und Windows für den Computer geeignete Updates findet, wird ein Symbol im Infobereich angezeigt und Sie erhalten eine Meldung darüber, dass die Updates heruntergeladen werden können. Nachdem Sie auf das Symbol oder auf die Meldung geklickt haben, können Sie die Updates auswählen. Anschließend werden die ausgewählten Updates von Windows im Hintergrund auf Ihren Rechner heruntergeladen. Nach Beendigung des Downloads wird das Symbol erneut im Infobereich angezeigt. Diesmal werden Sie jedoch benachrichtigt, dass die Updates jetzt auf dem Computer installiert werden können. Anschließend können Sie die entsprechenden Updates auswählen, die auf dem Computer installiert werden sollen.
- Die letzte Option *Nie nach Updates suchen (nicht empfohlen)* erklärt sich selbst: Auch die Suche nach Updates unterbleibt.

Für einige Updates ist es möglicherweise erforderlich, dass Sie Ihren Computer herunterfahren und erneut starten, um die Installation abzuschließen. Wenn Sie an Ihrem Computer angemeldet sind, benachrichtigt Windows Sie und gibt Ihnen die Möglichkeit, den Neustart zu einem späteren Zeitpunkt durchzuführen. Achten Sie darauf, sonstige Arbeiten vor dem Zeitpunkt der geplanten Installation zu speichern.

Von Microsoft wird empfohlen, die Updates automatisch herunterladen und installieren zu lassen. Hier gilt das schon im vorherigen Kapitel zum Thema Gesagte: Einerseits ist diese Automatik der etwas sicherere Weg, sich gegen neu geschaffene Viren und Würmer zu schützen.

Andererseits besteht der – vielleicht nicht ganz unbegründete – Verdacht, dass Microsoft derartige Prozeduren dazu benutzt, Ihren Rechner auszuspionieren. Solange Sie Ihre Software legal erworben haben, empfiehlt sich die Nutzung der Automatik.

3.3.2 Updateverlauf anzeigen

Wenn Sie sich über den bisherigen Verlauf der Updates informieren möchten, klicken Sie in der linken Spalte des Fensters *Windows-Update* auf den Link *Updateverlauf anzeigen*. Alle durchgeführten Updates werden dann aufgelistet (→ Bild 3.25).

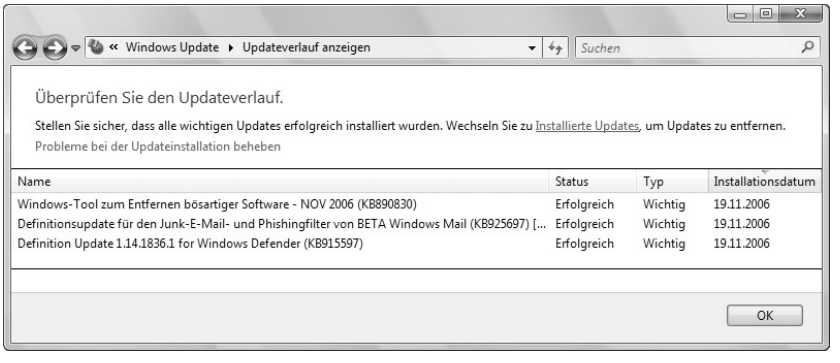


Bild 3.25: Ein Beispiel für den Updateverlauf

Nach einem Klick auf den Link *Installierte Updates* können Sie beispielsweise bereits installierte Updates wieder vom Rechner entfernen (→ Bild 3.26). Markieren Sie das zu entfernende Update und klicken Sie auf den Link *Deinstallieren*.

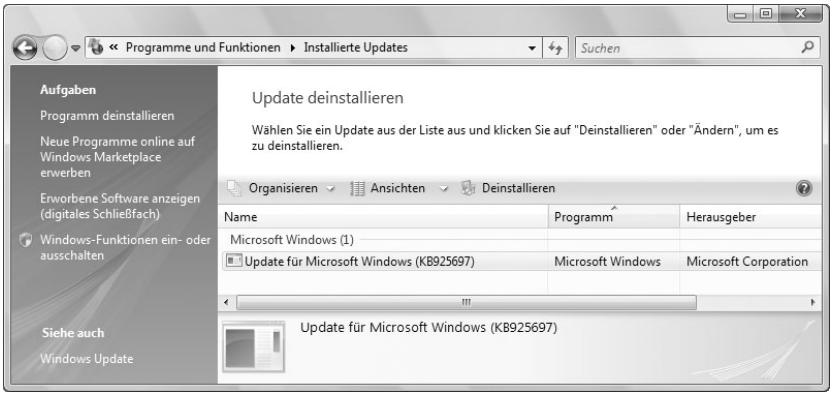


Bild 3.26: Updates können wieder entfernt werden.

3.4 Die Windows-Firewall

Eine auf Software basierende *Firewall*, die die Kommunikation zwischen dem Internet und dem Computer oder Netzwerk einschränkt, wird bei der Installation von Vista automatisch eingerichtet und aktiviert. Um den Computer vor Angriffen zu schützen, filtert diese Firewall eintreffende Datenpakete und erlaubt Verbindungsanforderungen nur über zugelassene Ports. Diese Firewall ist *statusbehaftet*: Sie erlaubt den Eingang von Datenpaketen nur im Zusammenhang mit vorher ausgegangenen Anforderungen. Sendet ein Rechner beispielsweise eine Anfrage an einen Server, erhält er kurze Zeit später von diesem Datenpakete aus dem Internet. Da die Firewall weiß, dass die Anfrage vom Rechner selbst initiiert wurde, lässt sie die Antwort passieren. Anders ist es, wenn ein unaufgefordertes Datenpaket an der Eingangspforte des Rechners eintrifft. Dieses wird zurückgewiesen, es sein denn, es verfügt über bestimmte Charakteristika, die Sie vorher festgelegt haben.

Den Zugriff auf die Einstellungen der Firewall erhalten Sie im *Windows-Sicherheitscenter* nach einem Klick auf den entsprechenden Link im linken Bereich des Fensters. Außerdem kann die *Windows-Firewall* auch über ein eigenes Symbol in der *Systemsteuerung* konfiguriert werden. Das dann angezeigte Fenster zeigt eine Übersicht über die aktuellen Einstellungen an (→ Bild 3.27).

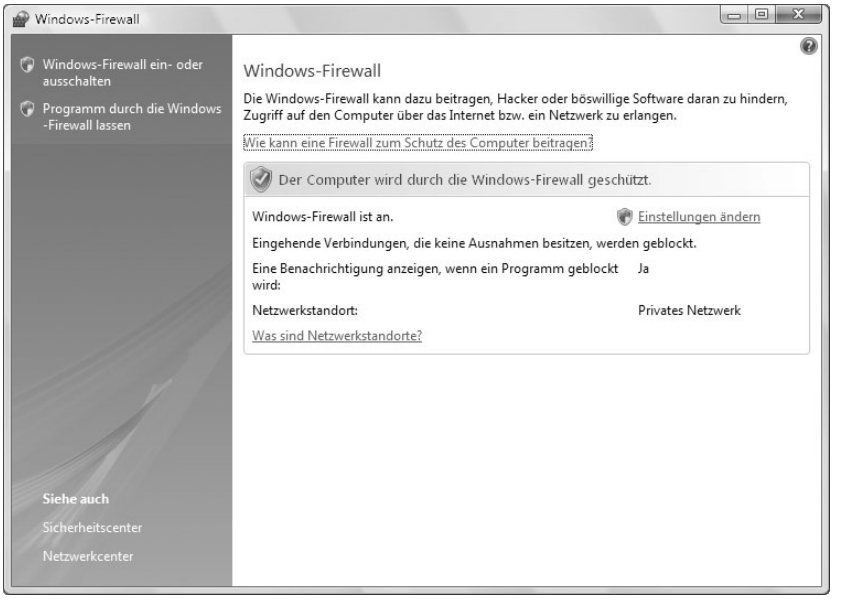


Bild 3.27: Die Übersicht zu den Einstellungen der Firewall

Um die Einstellungen zur Firewall kennenzulernen und gegebenenfalls zu ändern, klicken Sie in der Übersicht zur *Windows-Firewall* auf den Link *Einstellungen ändern*. Sie öffnen damit ein mit drei Registerkarten ausgestattetes Dialogfeld (→Bild 3.28).

Bild 3.28: Die allgemeinen Einstellungen zur Windows-Firewall

- Die Option *Aktiv (empfohlen)* schaltet die Funktion der Firewall ein, *Inaktiv (nicht empfohlen)* schaltet sie aus. Ein Ausschalten empfiehlt sich nur, wenn das lokale System bereits durch eine andere Firewall geschützt ist.
- Wenn Sie *Aktiv (empfohlen)* gewählt haben, gibt es noch die Option *Alle eingehenden Verbindungen blocken*. Damit werden auch die anschließend beschriebenen Ausnahmen unterdrückt – falls Sie solche vorher festgelegt hatten. Diese Option dient dazu, im Problemfall schnell einen maximalen Schutz einschalten zu können, ohne sich um Einzelheiten kümmern zu müssen.


TIPP

Standardmäßig ist *Aktiv (empfohlen)* bereits eingeschaltet. Ändern Sie diese Grundeinstellung nur, wenn Sie einen überzeugenden Grund dafür haben – beispielsweise wenn Sie eine separate Firewall verwenden, deren Einstellungen Sie individuell kontrollieren. Eine separate Firewall wird übrigens nicht benötigt, wenn Ihr Netzwerk bereits über einen Proxyserver verfügt. Dieser fungiert als Hardware-Firewall, überwacht alle gesendeten und empfangenen Kommunikationsaspekte und überprüft die Quell- und Zieladresse jeder verarbeiteten Nachricht. In diesen Fällen können Sie die Windows-Firewall deaktivieren, damit sich beide Programme nicht in die Quere kommen. Nur dazu wählen Sie auf der Registerkarte *Allgemein* des Dialogfelds *Windows-Firewall* die Option *Inaktiv*. Änderungen an den Einstellungen werden nach der Bestätigung sofort wirksam, ein Neustart ist nicht erforderlich.

3.4.1 Ausnahmen

Standardmäßig werden alle von außen her kommenden Versuche zur Verbindungsaufnahme in dem Rechner durch die Firewall blockiert. Alle Ports sind geschlossen. Wenn Sie unter bestimmten Bedingungen den Durchgang zulassen wollen, können Sie dafür Ausnahmen festlegen:

- Sie können den Durchgang für bestimmte Programme und Dienste erlauben – beispielsweise für die Freigabe von Daten oder Druckern oder für den Kommunikationsfluss zwischen den Teilnehmern an bestimmten Computerspielen.
- Die Programme und Dienste, die eine Verbindung zu anderen Rechnern im Internet oder lokalen Netzwerk aufbauen, öffnen für diese Verbindung sogenannte *Ports*. Ein *Port* ist ein Netzwerkbegriff, der den Punkt bezeichnet, an dem eine bestimmte Art von Netzwerkverkehr Ihren Computer erreicht. Welche Ports geöffnet werden, hängt von der Art des Datenverkehrs ab, der gesendet oder empfangen werden soll. Dieser Vorgang wird *Portzuordnung* genannt. Die Ports werden durch Nummern gekennzeichnet. Diese Ports können Sie auch alternativ – also ohne Angabe eines Programms oder Dienstes – individuell öffnen.


ACHTUNG

Wenn Sie eine solche Ausnahme von der Sperrung durch die Firewall definieren, wird diese Ausnahme standardmäßig für alle Computer geöffnet, die mit Ihrem Computer über das Netz verbunden sind. Sie können aber selbst weitere Einschränkungen vornehmen. Denken Sie daran, dass Sie Ihren Computer mit jeder Ausnahme schwächen. Wenn Sie eine Ausnahme zulassen, schaffen Sie ein Loch in der Firewall. Wird die Anzahl der Löcher zu groß, bleibt nicht mehr viel von der Wand der Firewall übrig.

Automatisch generierte Ausnahmen

Wenn Sie ein Programm ausführen, das auf den Empfang von Daten aus dem Internet oder einem Netzwerk angewiesen ist, fragt die Firewall bei Ihnen nach, ob die Anforderung ausgesperrt bleiben oder ob eine Verbindung zu Ihrem Rechner zugelassen werden soll. Das passiert beispielsweise, wenn eine Videokonferenz gestartet wird und die entsprechenden Programme noch nicht in der Liste der Ausnahmen vermerkt sind. Dann wird ein Dialogfeld angezeigt, in dem Sie entscheiden können, was getan werden soll. Voraussetzung für diese Frage ist, dass Sie die Option *Benachrichtigen, wenn ein neues Programm geblockt wird* auf der Registerkarte *Ausnahmen* im Dialogfeld *Windows-Firewall* aktiviert haben (→ folgende Abschnitte).

Sie können dann angeben, ob der Durchgang weiterhin blockiert bleiben oder geöffnet werden soll. Über die Schaltfläche *Weiterhin blockieren* bewirken Sie, dass das Programm auch in Zukunft keine Dateien empfangen kann. Mit *Nicht mehr blockieren* kann das Programm in Zukunft Dateien ohne weitere Nachfrage empfangen. Die Windows-Firewall erstellt daraufhin eine Ausnahme für das Programm (→ folgende Abschnitte).

Erneut nachfragen bewirkt, dass das Programm einmal Dateien empfangen kann, beim nächsten Versuch wird erneut nachgefragt.

Manuell erstellte Ausnahmen

Sie können Programme oder Ports auch manuell zu den Ausnahmen in der Firewall hinzufügen. Dazu verwenden Sie die Registerkarte *Ausnahmen* im Dialogfeld *Windows-Firewall* (→ Bild 3.29). Dort sind im Bereich *Programm oder Port* bereits Ausnahmen definiert, die aber – wie Drucker- und Dateifreigabe – standardmäßig auf das lokale Netz beschränkt sind. Zur Aufnahme weiterer Ausnahmen finden Sie hier zwei Möglichkeiten, die Sie durch einen Klick auf die beiden Schaltflächen *Programm* und *Port* regeln können.

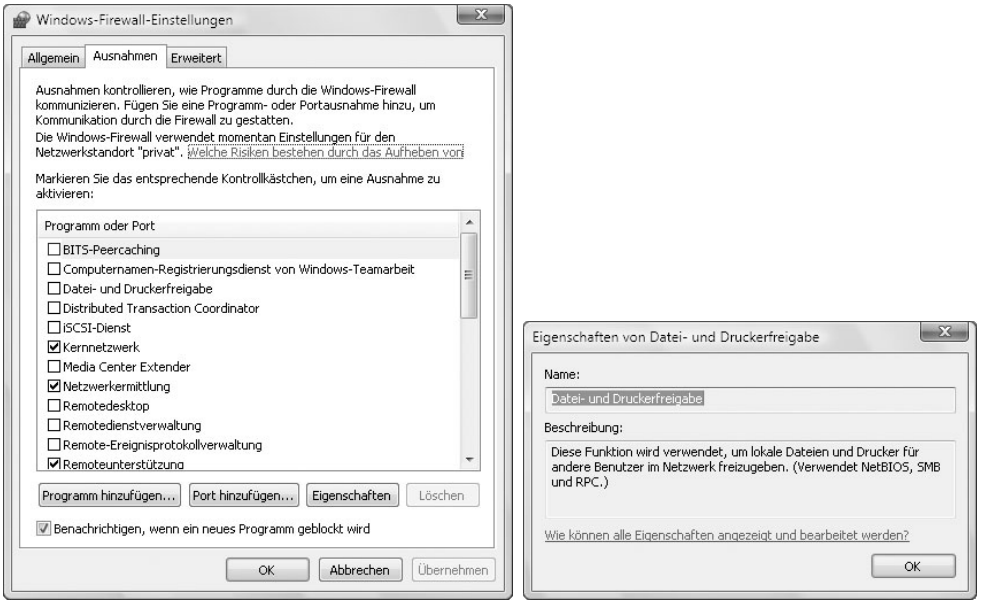


Bild 3.29: Die Ausnahmen zur Firewall

Eine etwas detailliertere Beschreibung zu einer der hier aufgeführten Optionen erhalten Sie, nachdem Sie die entsprechende Zeile markiert haben und auf den Link *Welche Risiken bestehen …* klicken. Weitere Hinweise zur Bedeutung der in der Liste angezeigten Elemente können Sie abrufen, indem Sie das Element markieren und dann auf *Eigenschaften* klicken (→Bild 3.29 rechts).


TIPP

Wenn Ihr Rechner zwar mit dem Internet verbunden, aber nicht an ein sonstiges Netzwerk angeschlossen ist, sollten Sie die Optionen *Datei- und Druckerfreigabe* und *Remoteunterstützung* deaktivieren, da sonst unnötige Sicherheitsrisiken entstehen könnten.

Ausnahmen für Programme

Unter *Programme* können Sie Namen und Pfad von Programmen festlegen, die die Firewall passieren dürfen. Nach einem Klick auf die Schaltfläche *Programm* wird das Dialogfeld *Programm hinzufügen* angezeigt, in dem eine Liste mit allen *bekannten* Programmen wiedergegeben wird (→ Bild 3.30 links). Klicken Sie auf das Programm, das Sie hinzufügen möchten, und anschließend auf *OK*. Das Programm wird ausgewählt und im Bereich *Programme und Dienste* als Ausnahme angezeigt. Sie können es wieder entfernen, indem Sie es dort markieren und auf die Schaltfläche *Löschen* klicken.

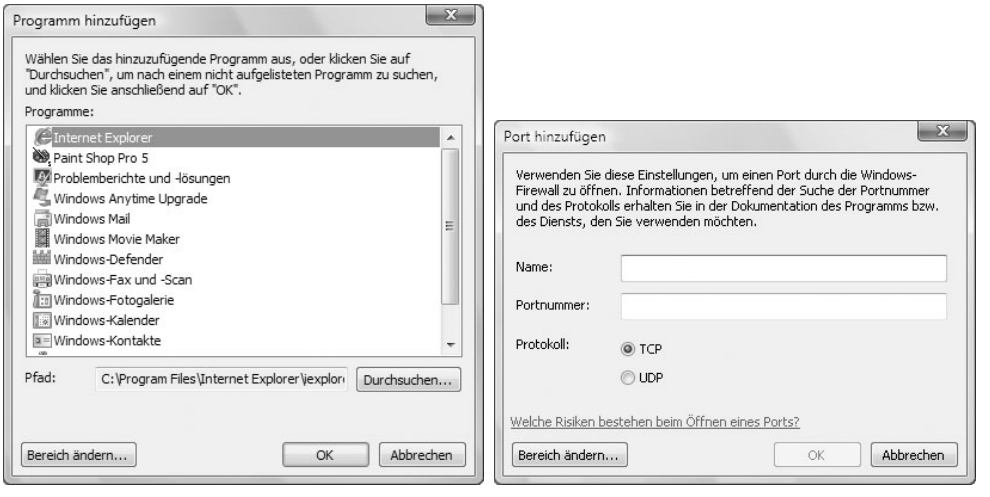


Bild 3.30: Programme und Ports hinzufügen

ACHTUNG

Wenn ein hier festgelegtes Programm seine Arbeit beendet hat, werden die geöffneten Ports automatisch wieder geschlossen. Allerdings können Probleme dann auftauchen, wenn ein solches Programm während seiner Arbeit abstürzt. Ports können dann weiterhin geöffnet bleiben.

Ausnahmen für Ports

Welche Ports ein spezielles Programm benutzen darf, können Sie nicht regeln. Sie können aber nach einem Klick auf die Schaltfläche *Port* auf der Registerkarte *Ausnahmen* einstellen, welche Ports geöffnet gehalten werden sollen (→ Bild 3.30 rechts). Dazu müssen Sie die Nummern der Ports kennen, die Sie öffnen möchten. Diese können dann unabhängig vom Programm genutzt werden, was natürlich einige Sicherheitsrisiken in sich birgt. Dazu klicken Sie auf die Schaltfläche *Port* und geben im Dialogfeld *Port hinzufügen* einen Namen für die Ausnahme und die Nummer des Ports ein.

- Geben Sie unter *Dienstbeschreibung* einen einfach zu merkenden Namen für den Dienst ein, damit Sie den Port identifizieren können, der geöffnet werden soll. Sie können jeden gewünschten Namen verwenden. Unter *Portnummer* geben Sie die Nummer des Ports ein.
- Klicken Sie dann entweder auf *TCP* oder auf *UDP*. Dienste benutzen eines der Transportprotokolle *UDP* und *TCP*, die auf dem Internetprotokoll basieren und es erweitern: *UDP* steht für *user datagram protocol*. Es ist rein nachrichtenorientiert und kümmert sich nicht darum, ob die Daten auch ihr Ziel erreichen. Es bietet also keine sichere Datenübertragung und keine Flusskontrolle. Daher wird *UDP* dann verwendet, wenn es nicht wichtig ist, dass alle Pakete ankommen. Der Vorteil von *UDP* ist eindeutig seine Schnelligkeit. Das *TCP*-Protokoll steht für *Transmission Control Protocol*. Es hat als Ziel, ein zuverlässiges Protokoll zur Datenübermittlung zur Verfügung zu stellen, und schafft dafür eine Verbindung zwischen zwei Systemen zur Übertragung von Datenströmen in beiden Richtungen. Da in einem Netzwerk Daten verloren gehen, in unterschiedlicher Reihenfolge oder mehrfach beim Empfänger ankommen können, übernimmt TCP die Überprüfung der korrekten Datenübertragung. Des Weiteren hat *TCP* Routinen integriert, die eine abgestimmte Datenübertragung mit Flusskontrolle bieten. Der Vorteil von *TCP* liegt in der Sicherheit, dagegen müssen bei der Geschwindigkeit Abstriche in Kauf genommen werden.

Klicken Sie abschließend auf *OK*. Die Ausnahme wird dann im Bereich *Programme und Dienste* angezeigt.


ACHTUNG

Ein Port, der zur Liste der Ausnahmen hinzugefügt wird, ist mit keinem bestimmten Programm verbunden, sondern bleibt permanent geöffnet. Wenn Sie also einen Port öffnen, sollten Sie daran denken, ihn wieder zu schließen, sobald Sie ihn nicht mehr benötigen. Löschen Sie dazu die Ausnahme oder deaktivieren Sie den Eintrag in der Liste, wenn Sie die Ausnahme zu einem späteren Zeitpunkt noch einmal benötigen.

Bereich ändern

Für jede von Ihnen definierte Ausnahme können Sie ferner angeben, aus welchen Netzen Sie den Zugriff erlauben wollen. Sie können hier den Durchgang auf das lokale Netz beschränken oder andere Netze oder *IP*-Adressen zulassen. Standardmäßig werden neu definierte Ausnahmen zunächst für alle Rechner zugelassen. Klicken Sie zum Ändern dieser Grundeinstellung im Dialogfeld *Programm hinzufügen* oder *Port hinzufügen* auf *Bereich ändern* und schränken Sie die Ausnahme auf das gewünschte Netz ein. Wenn Sie beispielsweise ein entsprechendes Spiel innerhalb des lokalen Netzwerks durchführen wollen, bestimmen Sie die dafür notwendigen Ausnahmen und setzen die Option auf *Nur für eigenes Netz*.

TIPP

Um Ihren Computer kurzfristig oder für längere Zeit gegen unverlangte Anforderungen zu sperren, können Sie auf der Registerkarte *Allgemein* des Dialogfelds zu den *Windows-Firewall-Einstellungen* das Kontrollkästchen *Alle eingehenden Verbindungen blocken* aktivieren. Dann werden Anforderungen an Programme und Dienste gesperrt, die auf der Registerkarte ausgewählt sind. Verwenden Sie diese Einstellung, wenn maximaler Schutz für den Computer erforderlich ist, beispielsweise während einer *WLAN*-Verbindung mit einem öffentlichen Drahtlosnetzwerk.

3.4.2 Erweiterte Optionen

Standardmäßig ist die Windows-Firewall für alle Netzwerkverbindungen eingeschaltet, die für Ihren Computer angelegt wurden. Sie können die Firewall gezielt für einzelne Verbindungen ausschalten: Öffnen Sie dazu im Dialogfeld *Windows-Firewall-Einstellungen* die Registerkarte *Erweitert* (→ Bild 3.31).

Bild 3.31: Die Registerkarte *Erweitert* der Firewall

Im Bereich *Netzwerkverbindungseinstellungen* können Sie das Kontrollkästchen vor jeder vorhandenen Verbindung ein- oder ausschalten, um die Firewall für diese wirksam oder unwirksam zu machen. Wenn Sie in

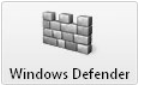
Ihrem Rechner mehrere Netzwerkverbindungen betreiben, die Verbindungen mit dem Internet aufnehmen können, müssen Sie die Firewall für jedes dieser Elemente aktivieren. Das gilt natürlich auch, wenn Sie ein Netzwerk betreiben, in dem mehrere Rechner eine direkte Verbindung zum Internet aufnehmen können. Lassen Sie aber diejenigen Verbindungen, die allein zur Kommunikation der Rechner innerhalb des Netzwerks dienen, zunächst unangetastet. Anderenfalls kommt es zu Störungen bei der Kommunikation zwischen diesem Computer und anderen Computern im Netzwerk und Sie können keine Drucker, Dateien oder Ordner auf den Computern gemeinsam nutzen. Achten Sie abschließend auf die Anzeige im Sicherheitscenter: Wenn Sie die Windows-Firewall für mindestens eine Verbindung deaktiviert haben, wird dort vermerkt, dass die Firewall deaktiviert ist – auch dann, wenn die Firewall für andere Verbindungen weiterhin aktiviert bleibt. Auf der Registerkarte *Allgemein* wird die Firewall jedoch weiterhin als *Aktiv* gekennzeichnet.

3.5 Der Windows Defender

Es ist wichtig den Computern beim Arbeiten in regelmäßigen Abständen danach zu untersuchen, ob nicht ein Programm aktiv ist, das Ihre Aktivitäten aufzeichnet und im Hintergrund an jemanden sendet, der Böses damit vorhat. Solche *Spyware* und andere möglicherweise unerwünschte Software kann sich jederzeit, wenn Sie eine Verbindung mit dem Internet herstellen, selbst auf dem Computer installieren. Diese Art von Software kann den Computer auch infizieren, wenn Sie Programme von einer CD, DVD oder anderen Wechselmedien installieren. Möglicherweise unerwünschte oder bösartige Software kann zudem so programmiert sein, dass sie zu unerwarteten Zeiten und nicht nur zum Zeitpunkt der Installation ausgeführt wird.

Windows Defender bietet drei Möglichkeiten, solche unerwünschte Software davon abzuhalten, den Computer zu infizieren:

- Über den *Echtzeitschutz* gibt *Windows Defender* eine Warnung aus, wenn Spyware oder möglicherweise unerwünschte Software auf dem Computer installiert oder ausgeführt wird. Sie erhalten ebenfalls eine Warnung, wenn Programme versuchen, wichtige Windows-Einstellungen zu ändern.
- Mithilfe der *SpyNet-Community* können Sie sehen, wie andere Personen auf Software reagieren, deren Risiko noch nicht eingestuft wurde. Wenn Sie sehen, ob andere Mitglieder eine Software zulassen, kann dies eine Entscheidungshilfe für Sie darstellen, ob Sie die Software ebenfalls auf Ihrem Computer zulassen. Wenn Sie selbst Bewertungen abgeben, können Sie Ihrerseits anderen Personen helfen, sich für oder gegen eine Software zu entscheiden.
- Über zusätzliche *Überprüfungsoptionen* können Sie überprüfen, ob auf dem Computer Spyware und andere möglicherweise unerwünschte Software installiert ist. Sie können diese Überprüfungen in regelmäßigen Intervallen planen und automatisch jede bösartige Software entfernen lassen, die bei einer Überprüfung erkannt wird.



Den Zugang zu *Windows Defender* erhalten Sie, indem Sie in der klassischen Ansicht der *Systemsteuerung* auf *Windows Defender* doppelklicken. Sie können dazu auch das gleichnamige Programm unter *Alle Programme* im Startmenü ausführen. Das dazu gehörende Fenster wird angezeigt (→ Bild 3.32). Mit etwas Glück wird dort gemeldet, dass auf dem Computer keine unerwünschte oder schädliche Software installiert ist.

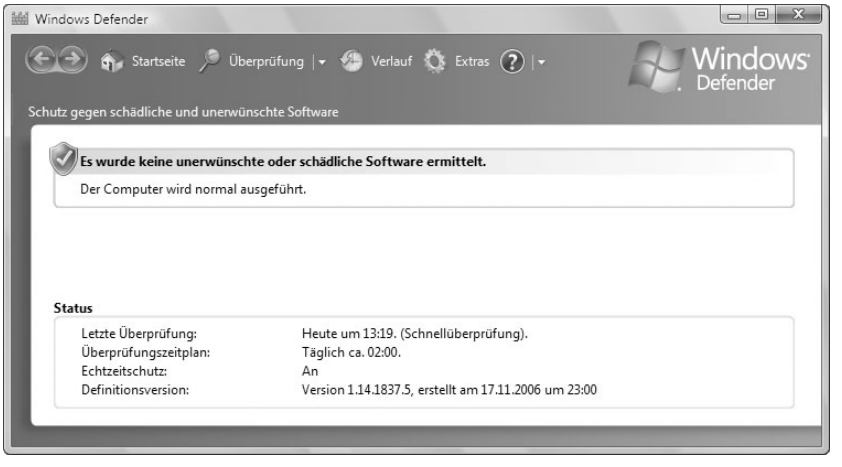


Bild 3.32: Eine positive Meldung

Wenn Sie *Windows Defender* verwenden, sollten Sie stets über aktuelle *Definitionen* verfügen. Definitionen sind Dateien, die als eine ständig wachsende Enzyklopädie potenzieller Softwarebedrohungen verstanden werden können. *Windows Defender* bestimmt anhand von Definitionen, ob es sich bei einer erkannten Software um Spyware oder andere möglicherweise unerwünschte Software handelt, und warnt Sie dann vor potenziellen Risiken. Damit Ihre Definitionen immer dem aktuellen Stand entsprechen, arbeitet *Windows Defender* mit *Windows Update* zusammen, sodass neue Definitionen sofort bei ihrer Freigabe automatisch installiert werden. Sie können *Windows Defender* auch so einrichten, dass vor einer Überprüfung des Computers online nach aktualisierten Definitionen gesucht wird.

Mithilfe der Schaltflächen in der Symbolleiste dieses Fensters können Sie die einzelnen Funktionen dieses Bereichs ansprechen (→ Tabelle 3.1).

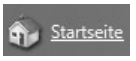
Symbol	Wirkung
	Zeigt nach einem Wechsel zu anderen Seiten des *Windows Defender* wieder die Seite an, mit der dieser Bereich geöffnet wurde.
	Führt eine Überprüfung mit den unter *Extras* vorgenommenen Einstellungen durch. Sie können wählen, ob *Windows Defender* auf dem Computer eine *Schnellüberprüfung* oder eine *vollständige Überprüfung* ausführen soll.
	Hier werden die Aktionen angezeigt, die Sie möglicherweise unerwünschter Software zugeordnet haben, die von *Windows Defender* auf dem Computer erkannt wurde
	Ermöglicht das Festlegen der Einstellungen für Windows Defender. Sie können hierüber bestimmen, wie er ausgeführt werden soll.
	Zeigt die Hilfe zu *Windows Defender* an.

Tabelle 3.1: Die Schaltflächen in der Symbolleiste

3.5.1 Die Optionen festlegen

Es empfiehlt sich, zunächst einmal auf die Schaltfläche *Extras* zu klicken, um sich einen Überblick zu verschaffen. Ein Fenster mit sechs weiteren Schaltflächen wird angezeigt (→ Bild 3.33). Die Einstellungen zu diesem Werkzeug regeln Sie über die oberen beiden Symbole.

Bild 3.33: Die Extras zu *Windows Defender*

Optionen

Klicken Sie zunächst auf *Optionen*. In einer recht langen Liste können Sie diverse Einstellungen für die Überprüfung durch den *Windows Defender* festlegen (→ Bild 3.34).

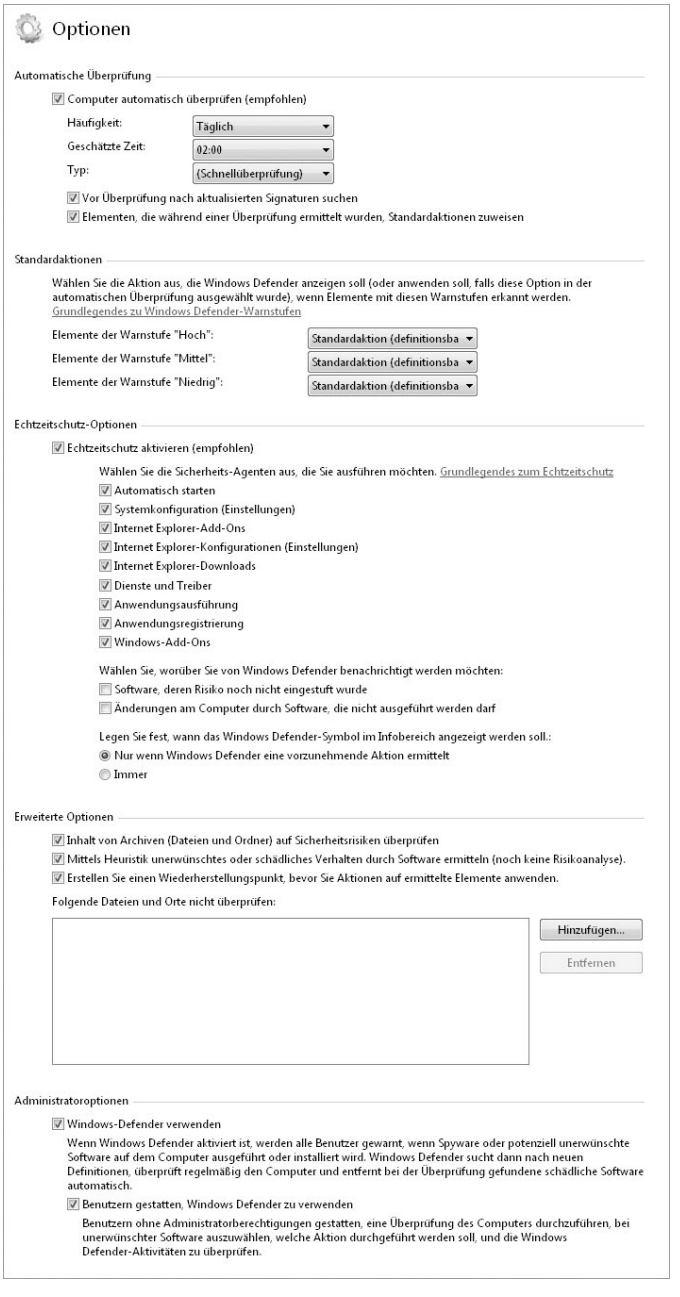


Bild 3.34: Die Optionen zum *Windows Defender*

- Im Bereich unter *Automatische Überprüfung* können Sie festlegen, ob die Prüfung automatisch gestartet werden soll und wann das standardmäßig passieren soll. Wenn Sie zu den Nachtarbeitern gehören, sollten Sie zumindest die Uhrzeit entsprechend anpassen.
- Sie können wählen, ob *Windows Defender* auf dem Computer eine Schnellüberprüfung oder eine vollständige Überprüfung ausführen soll. Bei einer *Schnellüberprüfung* werden die Bereiche auf der Festplatte des Computers überprüft, die am ehesten von Spyware infiziert werden. Bei einer *vollständigen Überprüfung* werden alle Dateien auf der Festplatte und alle derzeit ausgeführten Programme überprüft. Möglicherweise wird jedoch bis zum Abschluss der Überprüfung der Betrieb des Computers verlangsamt. Es wird empfohlen, einmal täglich eine Schnellüberprüfung zu planen. Wenn Sie den Verdacht haben, dass der Computer mit Spyware infiziert worden ist, sollten Sie aber jedes Mal sofort eine vollständige Überprüfung ausführen. Ansonsten scheinen die Einstellungen hier recht vernünftig. Mit dem Kontrollkästchen *Elementen, die während einer Überprüfung ermittelt wurden, Standardaktionen zuweisen* machen Sie die darunter einstellbaren Aktionen wirksam.
- Unter den *Standardaktionen* legen Sie fest, was der Defender tun soll, wenn er auf möglicherweise unerwünschte Software trifft. *Windows Defender* arbeitet mit *Warnstufen*, die einem Programm zugewiesen werden, nachdem es identifiziert wurde (→ Tabelle 3.2). Welche Warnstufe jeweils eingesetzt wird, erfährt *Windows Defender* über das Internet und darin liegt in der Zukunft vielleicht auch ein möglicher Angriffspunkt.

Warnstufe	Bedeutung
Schwerwiegend	Weit verbreitete oder besonders bösartige Programme, ähnlich wie Viren oder Würmer, die den Datenschutz und die Sicherheit des Computers beeinträchtigen und den Computer beschädigen können.
Hoch	Programme, die möglicherweise Ihre persönlichen Informationen sammeln und den Datenschutz beeinträchtigen oder den Computer beschädigen, beispielsweise durch Sammeln von Informationen oder Ändern von Einstellungen, in der Regel, ohne dass Sie davon wissen oder Ihre Zustimmung dazu gegeben haben.
Mittel	Programme, die möglicherweise den Datenschutz beeinträchtigen oder Änderungen am Computer vornehmen, die sich negativ auf Ihre Arbeit am Computer auswirken können, z. B. indem persönliche Informationen gesammelt oder Einstellungen geändert werden.

Tabelle 3.2: Warnstufen und deren Bedeutung

Warnstufe	Bedeutung
Niedrig	Möglicherweise unerwünschte Software, die u. U. Informationen über Sie oder Ihren Computer sammelt oder die Funktionsweise des Computers ändert, die aber in Übereinstimmung mit den bei der Installation der Software angezeigten Lizenzbedingungen ausgeführt wird.
Noch nicht klassifiziert	Diese Programme sind normalerweise harmlos, sofern sie nicht ohne Ihr Wissen auf dem Computer installiert wurden.

Tabelle 3.2: Warnstufen und deren Bedeutung (Forts.)

Für Software der Warnstufe *Schwerwiegend* kann keine Standardaktion ausgewählt werden, da *Windows Defender* diese Software automatisch entfernt oder Sie auffordert, die Software zu entfernen. Bei Software, deren potenzielles Risiko für den Datenschutz oder den Computer noch nicht klassifiziert wurde, müssen Sie Informationen zur Software überprüfen und dann eine Aktion auswählen.

- Mithilfe von Warnstufen können Sie auswählen, wie auf Spyware reagiert werden soll. Auch wenn *Windows Defender* Ihnen empfiehlt, Spyware zu entfernen, ist nicht jede erkannte Software bösartig oder unerwünscht. Anhand der Informationen in der folgenden Tabelle können Sie entscheiden, wie Sie vorgehen, wenn *Windows Defender* möglicherweise unerwünschte Software auf dem Computer erkennt.
- Wenn Sie das Kontrollkästchen *Echtzeitschutz aktivieren (empfohlen)* aktiviert halten, erhalten Sie sofort eine *Warnung*, wenn möglicherweise unerwünschte Software auf dem Computer installiert oder ausgeführt wird. Abhängig von der Warnstufe können Sie dann auf diese Software eine der folgenden Aktionen anwenden:
  - *Ignorieren* lässt zu, dass die Software auf dem Computer installiert oder ausgeführt wird. Wird die Software bei der nächsten Überprüfung immer noch ausgeführt oder versucht die Software, sicherheitsbezogene Einstellungen auf dem Computer zu ändern, gibt *Windows Defender* erneut eine Warnung zu dieser Software aus.
  - Wenn Software von *Windows Defender* unter *Quarantäne* gestellt wird, wird die Software an einen anderen Ort auf dem Computer verschoben und die Ausführung der Software verhindert, bis Sie entscheiden, ob die Software wiederhergestellt oder vom Computer entfernt werden soll.
  - Über *Entfernen* löschen Sie die entsprechende Software dauerhaft vom Computer.
  - Wenn Sie sich für *Immer zulassen* entscheiden, wird die Software der Liste der zugelassenen Elemente von *Windows Defender* hinzugefügt und kann auf dem Computer ausgeführt werden. *Win-*

dows Defender gibt keine Warnungen mehr bezüglich der Risiken aus, die diese Software möglicherweise für den Datenschutz oder den Computer darstellt. Fügen Sie Software nur dann der Liste der zugelassenen Elemente hinzu, wenn Sie der Software und dem Softwareherausgeber vertrauen.

Sie erhalten ebenfalls eine Warnung, wenn eine Software versucht, wichtige Windows-Einstellungen zu ändern. Da die Software bereits auf dem Computer ausgeführt wird, werden Ihnen dann andere Aktionen angeboten: Mit *Zulassen* wird erlaubt, dass die Software sicherheitsbezogene Einstellungen auf dem Computer ändert. Über *Verweigern* wird das verhindert.

- Unter den *Echtzeitschutz-Optionen* finden Sie mehrere Kontrollkästchen. Sie können auswählen, welche Software und welche Einstellungen von *Windows Defender* überwacht werden sollen. Es wird jedoch empfohlen, alle Echtzeitschutzoptionen, die sogenannten *Echtzeitschutz-Agenten*, zu verwenden (→ Tabelle 3.3).

Echtzeitschutz-Agent	Überwacht ...
Automatisch starten	... die Liste der Programme, die beim Starten des Computers automatisch ausgeführt werden dürfen. Da möglicherweise unerwünschte Software meist beim Starten von Windows automatisch ausgeführt wird, ist dieser Aspekt besonders wichtig.
Systemkonfiguration (Einstellungen)	... sicherheitsbezogene Einstellungen in Windows. Bösartige Software ist in der Lage, Hardware- und Softwaresicherheitseinstellungen zu ändern und dann Informationen zu sammeln, mit denen die Sicherheit des Computers noch weiter unterlaufen werden kann.
Internet Explorer-Add-ons	... Programme, die beim Starten von Internet Explorer automatisch ausgeführt werden. Manche Software kann sich als Webbrowser-Add-on tarnen und ohne Ihr Wissen ausgeführt werden.
Internet Explorer-Konfigurationen (Einstellungen)	... Browser-Sicherheitseinstellungen, die die erste Verteidigungslinie gegen bösartige Inhalte aus dem Internet darstellen. Die Software könnte versuchen, diese Einstellungen ohne Ihr Wissen zu ändern.
Internet Explorer-Downloads	... Dateien und Programme, die für die Zusammenarbeit mit dem Internet Explorer entworfen wurden, beispielsweise ActiveX-Steuerelemente und Programme zum Installieren von Software.

Tabelle 3.3: Die Echtzeitschutz-Agenten

Echtzeitschutz-Agent	Überwacht ...
Dienste und Treiber	... Dienste und Treiber bei ihrer Interaktion mit Windows und Ihren Programmen. Da Dienste und Treiber wesentliche Computerfunktionen ausführen, haben sie Zugriff auf wichtige Software im Betriebssystem. Bösartige Software kann sich mithilfe von Diensten und Treibern Zugriff auf den Computer verschaffen.
Anwendungsausführung	... das Starten von Programmen und alle Vorgänge, die von diesen ausgeführt werden. Gewisse Software kann Schwachstellen in installierten Programmen ausnutzen, um ohne Ihr Wissen bösartige oder unerwünschte Software auszuführen.
Anwendungsregistrierung	... Werkzeuge und Dateien im Betriebssystem, wobei Programme so registriert werden können, dass sie jederzeit ausgeführt werden. Unerwünschte Software kann ein Programm so registrieren, dass es beispielsweise jeden Tag zu einer bestimmten Uhrzeit unbemerkt gestartet und ausgeführt wird, oder sich Zugriff auf wichtige Software im Betriebssystem verschaffen.
Windows-Add-ons	... Softwaredienstprogramme für Windows. Diese Art von Programmen dient dazu, Ihnen die Arbeit mit dem Computer in Bereichen wie Sicherheit, Internetsurfen, Produktivität und Multimedia zu erleichtern.

Tabelle 3.3: Die Echtzeitschutz-Agenten (Forts.)

- Legen Sie unter *Wählen Sie, worüber Sie von Windows Defender benachrichtigt werden möchten* die gewünschten Optionen fest.
- Außerdem stehen Ihnen vier *Erweitere Optionen* zur Verfügung:
  - Ein Einschalten von *Inhalt von Archiven … überprüfen* erhöht möglicherweise den Zeitaufwand für eine Überprüfung. Bösartige Software besitzt jedoch die Fähigkeit, sich selbst zu installieren und sich an diesen Speicherorten zu verstecken.
  - Mit der Option *Unerwünschtes … Computerverhalten … mittels Heuristik ermitteln* identifiziert *Windows Defender* Bedrohungen mithilfe von Definitionsdateien. Das Programm ist aber auch in der Lage, potenziell schädliches oder unerwünschtes Verhalten von Software zu erkennen, die noch nicht in einer Definitionsdatei aufgelistet ist, und Sie davor zu warnen.
  - Über *Erstellen Sie einen Wiederherstellungszeitpunkt …* bewirken Sie, dass ein Wiederherstellungszeitpunkt erstellt wird, bevor die festgelegten Aktionen ausgeführt werden. Damit haben Sie die Möglichkeit, Systemeinstellungen wiederherzustellen, falls eine Software entfernt wurde, die Sie verwenden möchten.

- Im Feld *Folgende Dateien und Orte nicht überprüfen* können Sie Dateien und Ordner auswählen, die nicht von *Windows Defender* überprüft werden sollen. Suchen Sie die nicht zu überprüfenden Dateien und Ordner und klicken Sie dann auf *OK*. Wiederholen Sie diesen Schritt für jede Datei und jeden Ordner, die bzw. der nicht überprüft werden soll.
- Klicken Sie nach dem Festlegen der Einstellungen für *Windows Defender* auf *Speichern*. Wenn Sie aufgefordert werden, ein Administratorkennwort oder eine Bestätigung einzugeben, geben Sie das Kennwort bzw. die Bestätigung ein.

Microsoft SpyNet

Wenn Sie der *Microsoft SpyNet-Onlinecommunity* beitreten, können Sie sehen, wie andere Personen auf Software reagieren, deren Risiko noch nicht eingestuft wurde. Dies kann eine Entscheidungshilfe für Sie sein, ob Sie die Software ebenfalls auf Ihrem Computer zulassen sollen. Klicken Sie auf *Microsoft SpyNet* im Fenster *Tools und Einstellungen*, um die Form des Beitritts einzustellen (→ Bild 3.35). Die Besonderheiten werden im Fenster erklärt.

Bild 3.35: Der Beitritt zu Microsoft SpyNet

3.5.2 Die Überwachung durchführen

Nach einem Klick auf *Überprüfung* im Fenster *Windows Defender* wird die Überprüfung mit den vorher definierten Einstellungen durchgeführt. Auch hier können Sie wählen, ob *Windows Defender* auf dem Computer eine *Schnellüberprüfung* oder eine *vollständige Überprüfung* ausführen soll. Klicken Sie auf den nach unten zeigenden Pfeil neben der Schaltfläche *Überprüfen*, um die Form zu wählen. Wenn Sie den Verdacht haben, dass ein bestimmter Bereich des Computers mit Spyware infiziert ist, können Sie hier auch eine *benutzerdefinierte Überprüfung* veranlassen, indem Sie nur die Laufwerke und Ordner auswählen, die Sie überprüfen möchten. Klicken Sie in dem angezeigten Fenster auf *Auswählen* und legen Sie dann fest, welche Laufwerke und Ordner geprüft werden sollen (→ Bild 3.36). Klicken Sie auf *OK*. Wird später unerwünschte oder bösartige Software erkannt, führt *Windows Defender* anschließend eine Schnellüberprüfung aus, damit die erkannten Elemente auch von anderen Bereichen des Computers entfernt werden können.

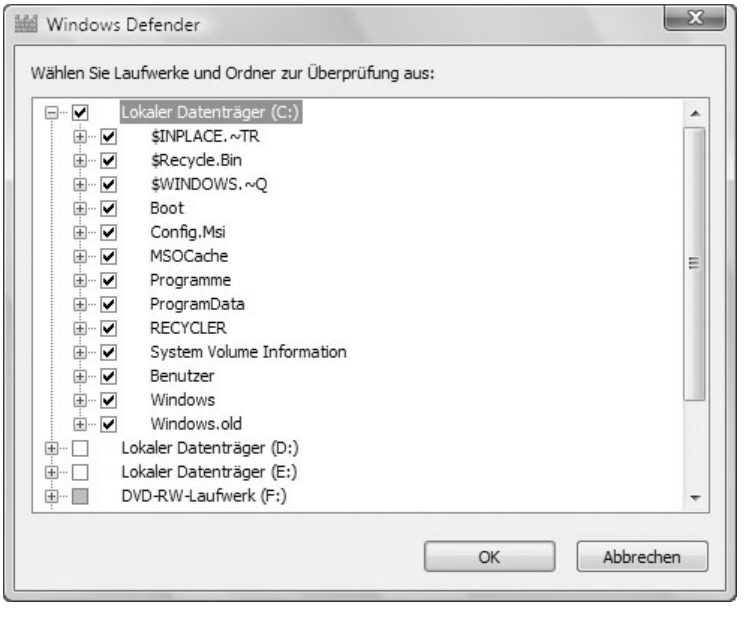


Bild 3.36: Legen Sie Laufwerke und Ordner fest.

Der Verlauf

Nach einem Klick auf *Verlauf* im *Windows Defender* werden die Aktionen angezeigt, die Sie Spyware und anderer möglicherweise unerwünschter Software zugeordnet haben, die von *Windows Defender* auf dem Computer erkannt wurde.

Unter Quarantäne gestellte Elemente

Wenn Software von *Windows Defender* unter Quarantäne gestellt wird, wird die Software an einen anderen Ort auf dem Computer verschoben und die Ausführung der Software verhindert, bis Sie entscheiden, ob die Software wiederhergestellt oder vom Computer entfernt werden soll. Dazu klicken Sie auf *Extras* und dann auf *Unter Quarantäne*. Überprüfen Sie in dem daraufhin angezeigten Fenster jedes Element und klicken Sie jeweils auf *Entfernen* oder *Wiederherstellen*. Sollen alle unter Quarantäne stehenden Elemente vom Computer entfernt werden, klicken Sie auf *Alle entfernen*.

Stellen Sie keine Software wieder her, für die die Warnstufe *Schwerwiegend* oder *Hoch* ausgegeben wurde. Diese Software kann den Datenschutz und die Sicherheit des Computers gefährden.

Zugelassene Elemente

Wenn Sie einer Software vertrauen, die von *Windows Defender* erkannt wurde, können Sie *Windows Defender* so einrichten, dass Sie keine Warnungen mehr zu den Risiken erhalten, die diese Software für den Datenschutz oder den Computer darstellen könnte. Damit keine Warnungen mehr ausgegeben werden, müssen Sie die betreffende Software der Liste der zugelassenen Elemente von *Windows Defender* hinzufügen.

- Wenn von *Windows Defender* das nächste Mal eine Warnung zu der Software ausgegeben wird, klicken Sie im Dialogfeld *Warnung* im Menü *Aktion* auf *Immer zulassen*.

- Wenn Sie ein Element aus der Liste der zugelassenen Elemente entfernen wollen, klicken Sie auf *Extras* und auf *Zugelassene Elemente*. Wählen Sie das Element aus, das wieder überwacht werden soll, und klicken Sie dann auf *Aus Liste entfernen*.

Lassen Sie nicht zu, dass Software, für die die Warnstufe *Schwerwiegend* oder *Hoch* ausgegeben wurde, auf dem Computer ausgeführt wird. Diese Software kann den Datenschutz und die Sicherheit des Computers gefährden.

Der Software-Explorer

Verwenden Sie die Optionen *Software-Explorer* unter den *Extras* zu *Windows Defender*, um detaillierte Informationen zu Software anzuzeigen, die derzeit auf dem Computer ausgeführt wird und den Datenschutz oder die Sicherheit des Computers beeinträchtigen kann (→ Bild 3.37). Sie können hier beispielsweise sehen, welche Programme beim Starten von Windows automatisch ausgeführt werden und wie diese Programme mit wichtigen Windows-Programmen und Diensten interagieren.

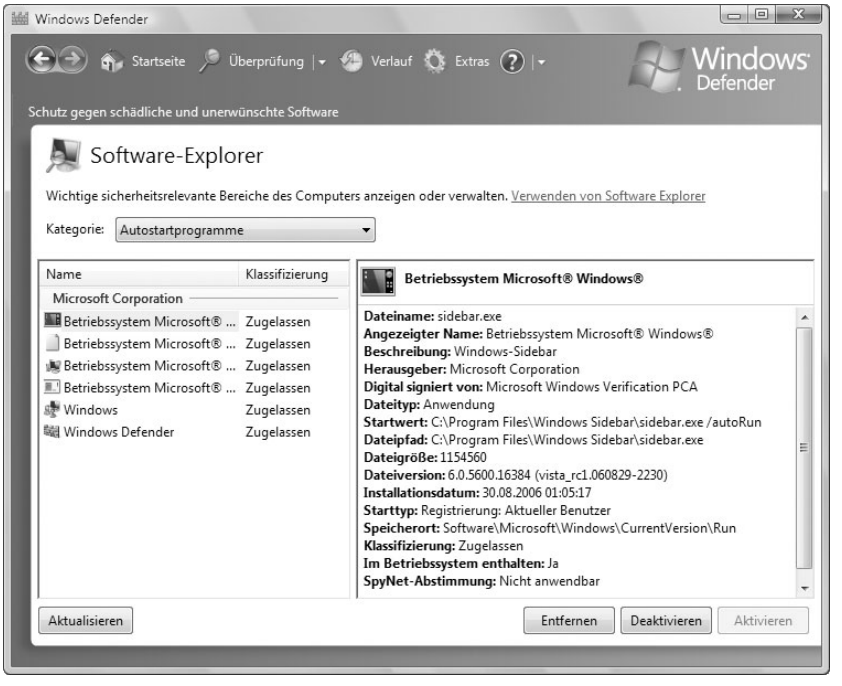


Bild 3.37: Der *Software-Explorer*

Über die Schaltfläche *Kategorie* können Sie die folgenden Elemente überwachen:

- *Autostartprogramme*, die mit oder ohne Ihr Wissen beim Starten von Windows automatisch ausgeführt werden.
- *Derzeit ausgeführte Programme* sind Programme, die derzeit auf dem Bildschirm oder im Hintergrund ausgeführt werden.
- *Mit dem Netzwerk verbundene Programme* sind solche Programme oder Prozesse, die eine Verbindung mit dem Internet oder mit Ihrem Heim- oder Firmennetzwerk herstellen können.
- Mit *Winsock-Dienstanbieter* sind Programme gemeint, die Netzwerk- und Kommunikationsdienste für Windows und Programme unter Windows ausführen. Diese Programme verfügen häufig über Zugriff auf wichtige Bereiche des Betriebssystems.

Der *Software-Explorer* zeigt dann grundlegende Informationen zu Programmen an – beispielsweise den Namen des Programms, den Herausgeber und die Version. Abhängig von der von Ihnen ausgewählten Kategorie werden möglicherweise auch die folgenden wichtigen Informationsarten angezeigt (→ Tabelle 3.4).

Titel	Beschreibung
Automatisch starten	Gibt an, ob das Programm beim Starten von Windows automatisch gestartet wird.
Starttyp	Der Ort, an dem das Programm beim Starten von Windows automatisch gestartet werden soll, z. B. in der Registrierung oder im Startordner *Alle Benutzer*.
Im Betriebssystem enthalten	Gibt an, ob das Programm als Teil von Windows installiert wurde.
Klassifizierung	Gibt an, ob das Programm im Hinblick auf eine Gefährdung des Datenschutzes und der Sicherheit des Computers analysiert wurde.
Digital signiert von	Gibt an, ob die Software signiert ist und, wenn dies zutrifft, ob sie vom aufgelisteten Herausgeber signiert wurde. Wenn dies nicht der Fall ist, sollten Sie den mit der Software bereitgestellten Herausgeberinformationen nicht vertrauen und weitere Details überprüfen, bevor Sie auswählen, ob Sie der Software selbst vertrauen sollen.

Tabelle 3.4: Die Bedeutung einiger zusätzlicher Informationen

3.6 Die Sicherung und Wiederherstellung

Am Anfang diese Kapitels wurde es schon erwähnt: Manchmal muss man sich nicht nur vor externen Angriffen, sondern auch vor eigenen unbedachten Aktionen schützen. Es geschieht zwar recht selten, aber passieren kann es trotzdem: Sie installieren ein Anwendungsprogramm oder eine Treibersoftware und plötzlich wird der Rechner spürbar langsam oder es funktioniert überhaupt nichts mehr. Durch Auswahl eines vor dem Änderungsdatum oder -zeitpunkt liegenden *Wiederherstellungspunkts* kann dann ein früherer Zustand des Computers wiederhergestellt werden. Um diese Möglichkeit zu gewährleisten, überwacht die Systemwiederherstellung Änderungen am System und an bestimmten Anwendungen und erstellt automatisch bestimmte *Wiederherstellungspunkte*.

Diese Systemwiederherstellung ist nicht dafür gedacht, persönliche Dateien zu sichern. Sie können daher damit keine persönliche Datei wiederherstellen, die gelöscht oder beschädigt wurde. Beispielsweise werden Textdokumente damit nicht in den Zustand zurückversetzt, den sie vor der Wiederherstellung hatten. Sie sollten Ihre persönlichen Dateien und wichtige Daten aber auf jeden Fall regelmäßig mit einem Sicherungsprogramm sichern. Darauf gehen wir in Kapitel 10 ein.

Den Zugang zu den Werkzeugen zur Sicherung und Wiederherstellung finden Sie im Fenster *Sicherheitscenter* unter dem Link *Sichern und Wiederherstellen* unten links im Aufgabenbereich. Sie können auch direkt die Ebene *Sicherung und Wiederherstellung* der Systemsteuerung ansprechen. Das gleich benannte Fenster wird geöffnet (→ Bild 3.38).

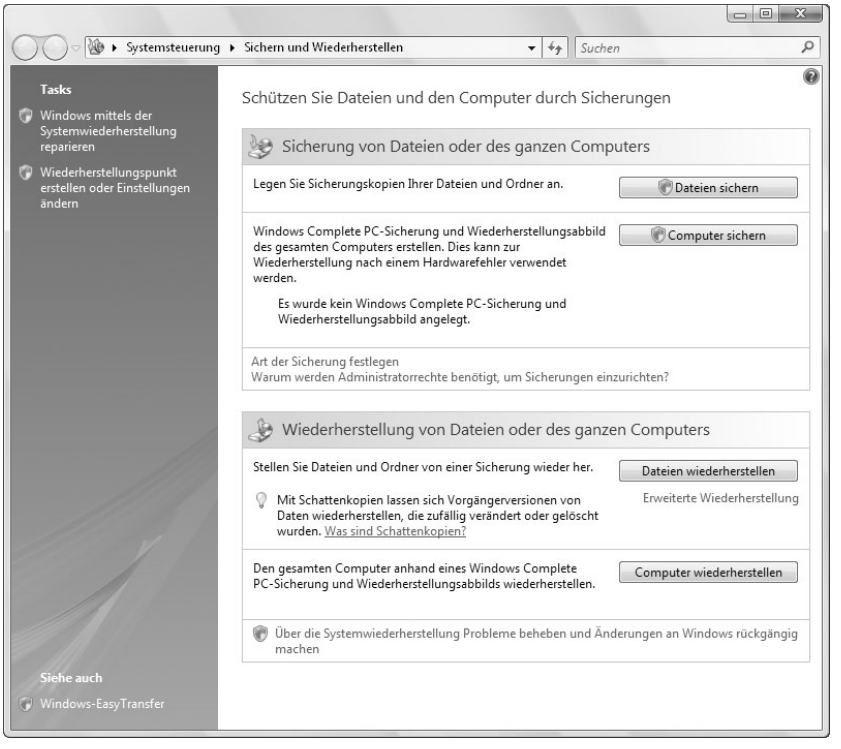


Bild 3.38: Die Ebene *Sichern und Wiederherstellen* der *Systemsteuerung*

3.6.1 Wiederherstellungszeitpunkte

Klicken Sie auf den Link *Wiederherstellungszeitpunkt erstellen oder Einstellungen ändern* im Bereich *Aufgaben* links im Fenster. Die Registerkarte *Computerschutz* des Dialogfelds *Systemeigenschaften* wird angezeigt (→ Bild 3.39).

Die Grundeinstellung kontrollieren

Im Listenfeld unten werden die auf dem Rechner vorhandenen Festplattenlaufwerke angezeigt. Stellen Sie hier sicher, dass das Kontrollkästchen vor dem zusätzlich mit *(System)* gekennzeichneten Laufwerk eingeschaltet ist. Damit garantieren Sie, dass die Funktion für dieses wichtige Laufwerk generell aktiviert ist. Wenn die Systemwiederherstellung auf einer Partition oder einem Laufwerk deaktiviert wird, werden alle auf dieser Partition oder auf diesem Laufwerk gespeicherten Wiederherstellungspunkte gelöscht.

Die Wiederherstellungszeitpunkte der Systemwiederherstellung werden automatisch in bestimmten Abständen und bei Änderungen am Computer erstellt (→ Tabelle 3.5).

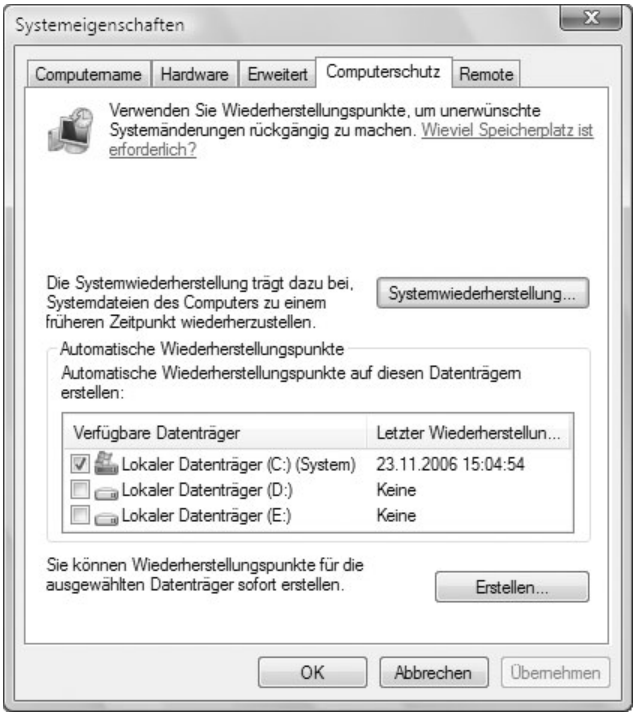


Bild 3.39: Der Computerschutz

Prüfpunkt	Beschreibung
Erster Systemprüfpunkt	Wird nach dem ersten Starten eines Computers nach der Aktualisierung zu Windows Vista oder nach dem ersten Starten eines neuen Computers erstellt.
Weitere Systemprüfpunkte	Wird in regelmäßigen Abständen erstellt, auch wenn keine Änderungen am System vorgenommen wurden. Standardmäßig werden diese Punkte alle 24 Stunden automatisch erstellt. War der Computer länger als 24 Stunden ausgeschaltet, erstellt die Systemwiederherstellung beim nächsten Starten des Computers einen Wiederherstellungspunkt.
Programminstallation	Wenn Sie ein Programm mithilfe der neuesten Installationsprogramme – beispielsweise *InstallShield* oder *Windows-Installer* – installieren, wird von diesem ein Wiederherstellungspunkt angelegt.
Windows Vista-Updates	Wenn Sie automatische Windows Vista-Updates für das Downloaden von Aktualisierungen verwenden, erstellt die Systemwiederherstellung einen Wiederherstellungspunkt vor dem Installieren der Aktualisierungssoftware.

Tabelle 3.5: Wiederherstellungszeitpunkte werden automatisch erzeugt.

Prüfpunkt	Beschreibung
Wiederherstellungsvorgang	Die Systemwiederherstellung erstellt selbst Wiederherstellungspunkte für Wiederherstellungsvorgänge, um die Änderung und die Wiederherstellung zu verfolgen.
Unsignierte Gerätetreiber	Wenn auf dem Computer ein Treiber installiert wird, der nicht von Microsoft signiert oder zertifiziert wurde, wird sofort ein Wiederherstellungspunkt erstellt.
Microsoft-Sicherungsprogramm	Auch wenn Sie eine Wiederherstellung mithilfe des Sicherungsprogramms ausführen, wird ein Wiederherstellungspunkt erzeugt. Sie können damit den Zustand vor der Wiederherstellung wiederherstellen (→ Kapitel 10).

Tabelle 3.5: Wiederherstellungszeitpunkte werden automatisch erzeugt. (Forts.)

Wenn das Betriebssystem die Systemwiederherstellung auf dem Computer installiert, werden standardmäßig etwa 12% des verfügbaren Speicherplatzes für die Systemwiederherstellung zur Archivierung von Wiederherstellungspunkten zugewiesen, es sei denn, es stehen weniger als 200 MB freier Speicherplatz auf der Festplatte zur Verfügung. Die Systemwiederherstellung benötigt mindestens 200 MB Speicherplatz auf der Festplatte. Sobald Sie den Platz auf der Platte für andere Zwecke nutzen und nicht mehr genügend Speicherplatz verfügbar ist, wird die Systemwiederherstellung automatisch deaktiviert. Nach der Freigabe von ausreichend Speicherplatz wird die Systemwiederherstellung automatisch wieder aktiviert, die zuvor angelegten Wiederherstellungspunkte gehen jedoch verloren. Falls alle alten Wiederherstellungspunkte von der Systemwiederherstellung entfernt werden müssen, wird ein neuer Wiederherstellungspunkt erstellt und die Erstellung regulärer Wiederherstellungspunkte wird von diesem Punkt an fortgesetzt.

Einen Wiederherstellungszeitpunkt manuell erstellen

Ist das eben angesprochene Kontrollkästchen eingeschaltet, werden Wiederherstellungspunkte automatisch täglich erstellt sowie unmittelbar vor wesentlichen Systemereignissen, wie beispielsweise der Installation eines Programms oder eines Gerätetreibers. Wiederherstellungspunkte können aber auch manuell erstellt werden. Sie können beispielsweise einen Wiederherstellungspunkt erstellen, wenn Sie mit der Funktionsweise des Computers zufrieden sind oder bevor Sie Änderungen auf dem Computer vornehmen – etwa bevor Sie Programme installieren, die die Funktionsweise des Computers möglicherweise verändern. Es ist sehr empfehlenswert, einen solchen Prozess vor allen tiefer greifenden Änderungen am System durchzuführen. Dazu markieren Sie auf der Registerkarte *Computerschutz* das entsprechende Laufwerk und klicken auf die Schaltfläche *Erstellen*. Geben Sie im Dialogfeld *Wiederherstellungspunkt erstellen* eine Beschreibung ein und klicken Sie dann auf *Erstellen* (→ Bild 3.40). Das Datum und die Uhrzeit werden automatisch hinzugefügt. Nach der

Bestätigung werden die zum Zeitpunkt notwendigen Daten auf die Festplatte geschrieben.

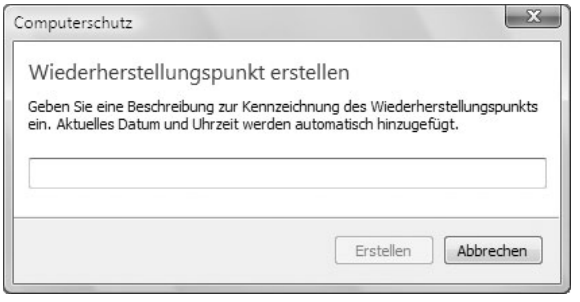


Bild 3.40: Einen Wiederherstellungszeitpunkt manuell erstellen

3.6.2 Wiederherstellen

Um das System in einen Zustand zurückzuversetzen, den es vor einem Wiederherstellungszeitpunkt innehatte, klicken Sie auf der Registerkarte *Computerschutz* auf die Schaltfläche *Systemwiederherstellung*. Ein Fenster wird angezeigt, in dem Ihnen ein empfohlener Wiederherstellungszeitpunkt angegeben wird (→ Bild 3.41).

- Im Allgemeinen sollten Sie diesen empfohlenen Zeitpunkt verwenden, wenn Probleme mit dem Rechner erst vor sehr kurzer Zeit aufgetreten sind. Lassen Sie dafür die Option *Empfohlene Wiederherstellung* aktiviert und klicken Sie auf *Weiter*.

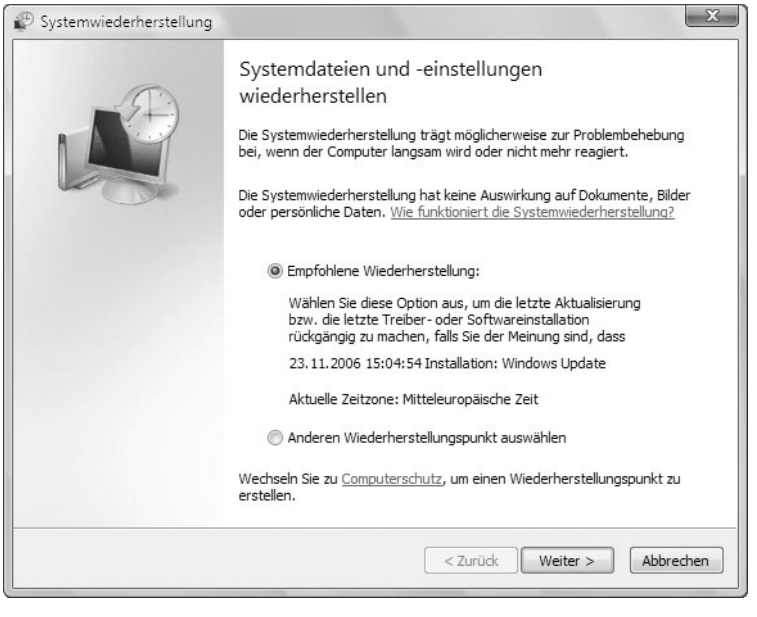


Bild 3.41: Wählen Sie einen Wiederherstellungszeitpunkt aus.

- Sie können aber auch einen anderen Zeitpunkt benutzen. Wenn Sie beispielsweise vermuten, dass die Störungen auf die Installation eines Programms zurückzuführen sind, das keines der unter Vista üblichen Installationsprogramme verwendet, wählen Sie den unmittelbar vor der Installation des Programms liegenden Wiederherstellungspunkt aus. Dazu aktivieren Sie die Option *Anderen Wiederherstellungszeitpunkt auswählen* und klicken Sie dann auf *Weiter* (→ Bild 3.42). Markieren Sie zuerst das gewünschte Datum und anschließend – falls dafür mehrere Zeitpunkte erfasst worden sind – auf der rechten Seite auf den gewünschten Zeitpunkt. Klicken Sie dann auf die Schaltfläche *Weiter*.

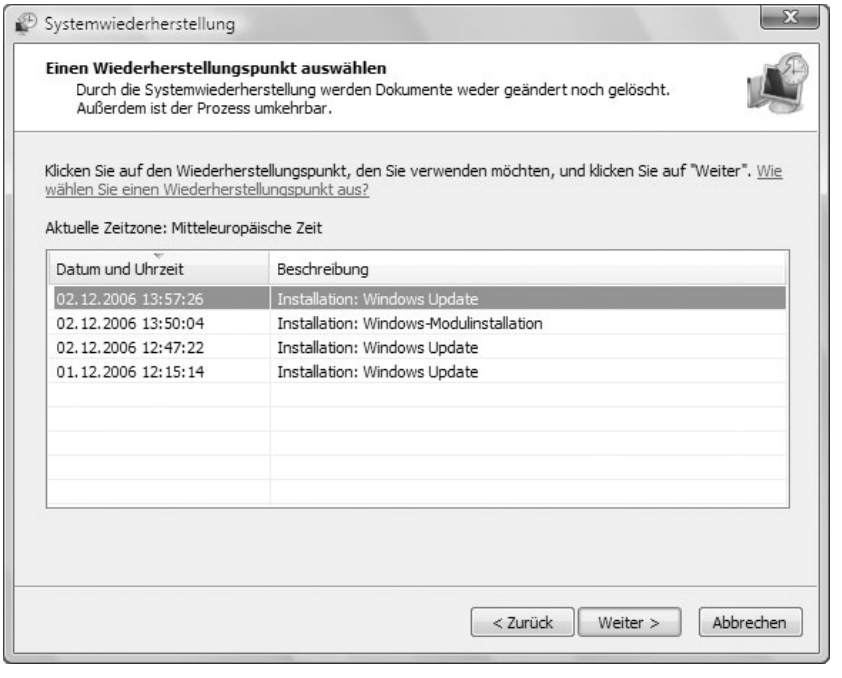


Bild 3.42: Sie können einen Zeitpunkt manuell wählen.

- Lesen Sie die angezeigte Zusammenfassung der bevorstehenden Aktion und klicken Sie nochmals auf *Weiter*. Der Rechner wird mit der Konfiguration zum gewählten Zeitpunkt neu gestartet.

3.6.3 Wenn der Computer nicht gestartet werden kann

Der wahrscheinlich schlimmste Fall besteht darin, dass nach einer Änderung der Computer nicht mehr gestartet werden kann, der Anmeldebildschirm also nicht angezeigt wird. Hatten Sie die Systemwiederherstellung aktiviert, ist aber auch das oft kein größeres Problem.

Die letzte Konfiguration verwenden

Sie können zunächst versuchen, die letzte als funktionierend bekannte Konfiguration wiederherzustellen. Dabei werden einige der Registrierungseinstellungen und Treiber wiederhergestellt, die beim letzten erfolgreichen Start des Computers wirksam waren. Schalten Sie den Computer ein. Sobald die Meldung *Wählen Sie das zu startende Betriebssystem* angezeigt wird, drücken Sie [F8]. Markieren Sie dann mit den Pfeiltasten *Letzte als funktionierend bekannte Konfiguration* und bestätigen Sie mit der Taste [↵]. Die Taste [Num ⇳] muss meist separat deaktiviert sein, damit die Pfeiltasten der Zehnertastatur verwendet werden können.

Abgesicherter Modus und Systemanalyse

Wenn die eben beschriebene Funktion *Letzte als funktionierend bekannte Konfiguration* nicht zum gewünschten Ergebnis führt, können Sie versuchen, das System im abgesicherten Modus zu starten. Dabei wird der Rechner nur mit den wichtigsten Dateien und Treibern – Maus, Bildschirm, Tastatur, Massenspeicher, Grundeinstellungen für Grafik, Standardsystemdienste usw. – hochgefahren. Wenn Sie in diesem Modus in der Lage sind, das System zu starten, können Sie anschließend die Systemwiederherstellung verwenden, um alle Einstellungen wiederherzustellen, die zu einem Zeitpunkt wirksam waren, als das System noch funktionsfähig war.

Schalten Sie den Computer ein. Sobald die Meldung *Wählen Sie das zu startende Betriebssystem* angezeigt wird, drücken Sie [F8]. Markieren Sie dann über die Pfeiltasten die geeignete Option für den abgesicherten Modus: Sie können die Option *Abgesicherter Modus mit Netzwerktreibern* auswählen, wenn außer den oben genannten Dateien und Treibern auch die wichtigsten Dienste und Treiber für das Arbeiten im Netzwerk geladen werden sollen. Oder Sie haben die Möglichkeit, die Option *Abgesicherter Modus mit Eingabeaufforderung* auszuwählen, die dem abgesicherten Modus entspricht, abgesehen davon, dass eine Eingabeaufforderung anstelle der grafischen Benutzeroberfläche gestartet wird. Bestätigen Sie mit der Taste [↵].

Im abgesicherten Modus können Sie Probleme diagnostizieren. Wenn ein Symptom nach dem Starten im abgesicherten Modus nicht mehr auftritt, können die Standardeinstellungen und die Basisgerätetreiber als mögliche Ursache ausgeschlossen werden. Wenn ein neu hinzugefügtes Gerät oder ein geänderter Treiber Probleme verursacht, haben Sie im abgesicherten Modus die Möglichkeit, das Gerät zu entfernen oder eine zuvor durchgeführte Änderung rückgängig zu machen.

Die Computerreparaturoptionen

Unter bestimmten Umständen kann auch der abgesicherte Modus nicht zur Problembehandlung verwendet werden. Dies ist beispielsweise der Fall, wenn Windows-Systemdateien, die zum Starten des Systems erforderlich sind, fehlerhaft oder beschädigt sind. In diesem Fall können Sie meist die Wiederherstellungskonsole zur Reparatur verwenden. Diese Methode wird aber nur für fortgeschrittene Benutzer empfohlen.

Legen Sie die Windows Vista-DVD, die Sie zur Installation verwendet haben, in ein Laufwerk und starten Sie den Computer neu. Die *Bootreihenfolge* muss dabei im BIOS so eingestellt sein, dass zuerst das CD/DVD-Laufwerk abgefragt wird (→ Kapitel 1). Wenn Sie dazu aufgefordert werden, eine Taste zu drücken, um den Computer von der DVD zu starten, drücken Sie beispielsweise [↵]. Wenn Sie zum Starten der Installation aufgefordert werden, wählen Sie *Computerreparaturoptionen* oder drücken Sie [C]. Von dieser Konsole aus können Sie auf die Laufwerke des Computers zugreifen. Sie können dann Dienste aktivieren und deaktivieren, Laufwerke formatieren, Daten auf einem lokalen Laufwerk lesen und schreiben und zahlreiche weitere Verwaltungsaufgaben ausführen. Beispielsweise können Sie auch wichtige Dateien kopieren, um sie zu retten. Die Konsole bietet neben Befehlen für einfache Aufgaben, wie das Wechseln zu einem anderen Verzeichnis oder das Anzeigen eines Verzeichnisses, auch Befehle für komplexere Aufgaben, beispielsweise das Reparieren des Bootsektors.

Die Windows-Installations-DVD

Als allerletzte Möglichkeit bietet es sich an, das Betriebssystem neu zu installieren. Ein solcher letzter Ausweg ist nur notwendig, wenn Sie den Computer nicht im abgesicherten Modus starten können, weder die Funktion *Letzte als funktionierend bekannte Konfiguration* noch die Verwendung der Wiederherstellungskonsole erfolgreich ist und Sie keine *Sicherungskopie für die automatische Systemwiederherstellung* besitzen. Dabei gehen Ihre auf dem Systemlaufwerk vorhandenen Datendateien verloren. Es empfiehlt sich also, diese Datendateien möglichst oft zu sichern. Dann können Sie sie mithilfe von Sicherungskopien wiederherstellen.

Sie können aber eine vollständige Neuinstallation des Betriebssystems umgehen, indem Sie eine vollständige Sicherung des Rechners durchführen – eine *Windows Complete PC-Sicherung* (→ Kapitel 10). Eine solche Sicherung ist mit einem Abbild – auch *Snapshot* genannt – der Programme, Systemeinstellungen und Dateien auf dem Computer vergleichbar. Bei einem Ausfall des Computers können Sie dann auf die Sicherung zurückgreifen. Sie sollten darüber hinaus alle sechs Monate eine neue *Windows Complete PC-Sicherung* erstellen.